DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN 0945–AA00

HIPAA Privacy Rule: Changes To Support Coordinated Care and Individual Engagement and Reduce Regulatory Burdens

AGENCY: Office for Civil Rights (OCR), Office of the Secretary, Department of Health and Human Services.

ACTION: Final rule.

SUMMARY: The Department of Health and Human Services (HHS or ''Department'') is issuing this final rule to modify the Standards for Privacy of Individually Identifiable Health Information (''Privacy Rule'') under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. These modifications address standards that may impede the nationwide transition to value-based health care by limiting or discouraging individual access or care coordination and case management or posing other unnecessary burdens. The modifications in this final rule promote the essential sharing of individuals' protected health information (PHI) for care coordination and individual engagement while continuing to protect its privacy and security.

DATES:

Effective dates: The final rule is effective on January 19, 2027.

Compliance date: Persons subject to this regulation must comply with the applicable requirements of this final rule by July 19, 2027.

FOR FURTHER INFORMATION CONTACT: Marissa Gordon-Nguyen at (202) 240–3110 or (800) 537–7697 (TDD), or by email at *OCRPrivacy@hhs.gov.*

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Executive Summary
A. Overview
B. Summary of Major Provisions
C. Effective and Compliance Dates
1. 2021 Privacy Rule NPRM
2. Summary of Comments
3. Final Rule
4. Response to Public Comments
D. Severability
II. Statutory and Regulatory Background
A. Statutory Authority and History
1. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
2. The Health Information Technology for Economic and Clinical Health (HITECH) Act
3. Patient Protection and Affordable Care Act
4. Coronavirus Aid, Relief, and Economic Security (CARES) Act
B. Regulatory and Legal History
1. 2000 Privacy Rule
2. 2002 Privacy Rule
3. 2013 Omnibus Rule
4. 2014 Privacy Rule
5. 2016 HIPAA Access Guidance
6. 2018 HIPAA Rules Request for Information
7. Ciox Health, LLC v. Azar
8. 2021 Privacy Rule NPRM
9. 2024 Part 2 Rule
10. 2024 Privacy Rule
III. Justification for This Rulemaking
A. An Effective Health Care System Requires That Individuals Have Access to Their Health Information and That Others Are Able To Use and Disclose Health Information About Individuals
1. Individuals Need To Have Access to Their Own Information for Many Purposes, Including Understanding Their Health Status, Coordinating Their Health Care, and Obtaining Government Benefits
2. Persons Involved in Caring for Individuals Need To Use Their PHI
B. The Health Care Environment Has Changed Since the Privacy Rule's Right of Access and Care Coordination Provisions Were Last Revised
1. Newer Laws Build on HIPAA's Goal of Developing a Nationwide Information Network and Promote the Electronic Exchange of Health Information
2. Technology That Enables the Electronic Exchange of PHI Is More Widely Available Today Than it Was in 2013 When the Omnibus Final Rule Was Published
3. Individuals Benefit When Their PHI Can Be Accessed and Exchanged Electronically
C. To Continue To Improve the Efficiency and Effectiveness of the Health Care System, the Department Must Modify the Privacy Rule To Address Issues That Impede Care Coordination and Individuals' Access to Their PHI
1. The Department Must Ensure That the Privacy Rule Accurately Reflects the Obligations of Regulated Entities and the Rights of Individuals
2. Regulated Entities Misinterpret the Privacy Rule in Ways That Are Inconsistent With an Efficient and Effective Health Care System
3. Regulations That Unnecessarily Impose Real or Perceived Burdens Are Barriers to an Efficient and Effective Health Care System
D. The Department Has Performed the Statutorily Required Consultations
IV. Summary of Final Rule Provisions and Public Comments and Responses
A. Individual Right of Access
1. Adding Definition of ''Electronic Health Record''
2. Adding Definition of ''Personal Health Application''
3. Strengthening the Access Right To Inspect and Obtain Copies of PHI
4. Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access
5. Addressing the Form and Format of Access
6. Addressing the Individual Right of Access to Direct Copies of PHI to a Person Designated by the Individual
7. Adjusting Permitted Fees for Access to PHI and ePHI
8. Notice of Access and Authorization Fees
9. Modifying the General Rules for Required Disclosures of PHI By Business Associates
B. Reducing Identity Verification Burden for Individuals Exercising the Right of Access
1. Issues To Address
2. Proposed Rule
3. Overview of Comments
4. Final Rule
5. Responses to Public Comments
C. Amending the Definition of Health Care Operations To Clarify the Scope of Care Coordination and Case Management
1. Current Rule
2. Proposed Rule
3. Overview of Comments
4. Final Rule
5. Responses to Public Comments
D. Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-Level Care Coordination and Case Management
1. Current Rule
2. Proposed Rule
3. Overview of Comments
4. Final Rule
5. Responses to Public Comments
E. Clarifying the Scope of Covered Entities' Abilities To Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management That Constitutes Treatment or Health Care Operations
1. Current Rule
2. Proposed Rule
3. Overview of Comments
4. Final Rule
5. Responses to Public Comments
F. Encouraging Disclosures of PHI When Needed To Help Individuals Experiencing Substance Use Disorder (Including Opioid Use Disorder), Serious Mental Illness, and in Emergency Circumstances
1. Current Rule
2. Proposed Rule
3. Overview of Comments
4. Final Rule
5. Responses to Public Comments
G. Modifying Notice of Privacy Practices Requirements To Reduce Regulatory Burden and Increase Transparency
1. Current Rule
2. Proposed Rule
3. Overview of Comments
4. Final Rule
5. Responses to Public Comments
H. Permitting Disclosures for Telecommunications Relay Services for People Who Are Deaf, Hard of Hearing, or Deaf-Blind, or Who Have a Speech Disability

1. Current Rule
2. Proposed Rule
3. Overview of Comments
4. Final Rule
5. Responses to Public Comments
I. Expanding the Permission To Use and Disclose the PHI of Armed Forces Personnel To Cover All Uniformed Services Personnel
1. Current Rule
2. Proposed Rule
3. Overview of Comments
4. Final Rule
5. Responses to Public Comments
J. Providing a Transition Period for Business Associate Agreements
1. Current Rule
2. Proposed Rule
3. Overview of Comments
4. Final Rule
5. Responses to Public Comments
K. Other Technical and Conforming Changes
V. Regulatory Impact Analysis
A. E.O. 12866 and E.O. 13563 and Related Executive Orders on Regulatory Review
1. Summary of Costs and Benefits
2. Baseline Conditions
3. Estimated Costs, Cost Savings, and Transfers Arising From Finalized Changes
4. Consideration of Regulatory Alternatives
B. E.O. 14192
C. Regulatory Flexibility Act
D. Unfunded Mandates Reform Act
E. E.O. 13132—Federalism
F. Assessment of Federal Regulation and Policies on Families
G. Paperwork Reduction Act of 1995

BILLING CODE 4153–01–P

Table of Acronyms

Term	Meaning
ACA	Patient Protection and Affordable Care Act.
ADA	Americans with Disabilities Act of 1990.
AHRQ	Agency for Healthcare Research and Quality.
APA	Administrative Procedure Act.
API	Application Programming Interface.
ASL	American Sign Language.
BJS	Bureau of Justice Statistics.
BLS	Bureau of Labor Statistics.
CAH	Critical Access Hospital.
CARES Act	Coronavirus Aid, Relief, and Economic Security (CARES) Act.
CEHRT	Certified EHR Technology.
CLIA	Clinical Laboratory Improvement Amendments of 1988.
CMS	Centers for Medicare & Medicaid Services.
COVID-19	Coronavirus Disease 2019.
Cures Act	21st Century Cures Act.
Department or HHS	U.S. Department of Health and Human Services.
DME	Durable Medical Equipment.
EHI	Electronic Health Information.
EHR	Electronic Health Record.[a]
E.O.	Executive Order.
ePHI	Electronic Protected Health Information.
FAQ	Frequently Asked Question.
GAO	Government Accountability Office.
HCBS	Home and Community Based Services.
Health IT	Health Information Technology.
HIE	Health Information Exchange.
HIN	Health Information Network.
HINTS	Health Information National Trends Survey.
HIPAA	Health Insurance Portability and Accountability Act of 1996.
HITECH Act	Health Information Technology for Economic and Clinical Health Act.
HTI	Health Data, Technology, and Interoperability.
ICR	Information Collection Request.
IIHI	Individually Identifiable Health Information.
IOM	Institute of Medicine.
MACRA	Medicare Access and CHIP Reauthorization Act of 2015.
NAICS	North American Industry Classification System.
NCVHS or Committee	National Committee on Vital and Health Statistics.
NOAA	National Oceanic and Atmospheric Administration.
NPP	Notice of Privacy Practices.
NPRM	Notice of Proposed Rulemaking.
OCR	Office for Civil Rights.
OIG	Office of Inspector General.
OMB	Office of Management and Budget.
ONC	Office of the National Coordinator for Health Information Technology.
PDMP	Prescription Drug Monitoring Program.

PHI	Protected Health Information.
PHSA	Public Health Service Act.
PRA	Paperwork Reduction Act of 1995.
QHIN	Qualified Health Information Network.
RFA	Regulatory Flexibility Act.
RFI	Request for Information.
RIA	Regulatory Impact Analysis.
SBA	Small Business Administration.
SMI	Serious Mental Illness.
SNF	Skilled Nursing Facility.
SSA	Social Security Act of 1935.
SSDI	Social Security Disability Insurance.
SSI	Supplemental Security Income.
SUD	Substance Use Disorder.
TEFCA	Trusted Exchange Framework and Common Agreement.
TPO	Treatment, Payment, and/or Health Care Operations.
TRS	Telecommunications Relay Services.
UMRA	Unfunded Mandates Reform Act of 1995.
U.S.C.	United States Code.
USPHS	U.S. Public Health Service.
VA	U.S. Department of Veterans Affairs.
VDT	View, Download, and Transmit.

[a] For purposes of this final rule, we use the term "EHR" to refer to the commonly understood meaning of the term; *i.e.*, a system that stores electronic health information across different health care settings. We use the term "electronic health record" when referring to the term defined in the HITECH Act and this final rule.

BILLING CODE 4153–01–C

I. Executive Summary

A. Overview

Empowering individuals to take control of their health is critical to delivering on the promise to Make America Healthy Again, which is central to the mission of the Department of Health and Human Services (HHS or ''Department''). Enabling individuals, their personal representatives, their health care providers, and others designated by the individuals to have unfettered access to their information is a necessary first step towards achieving this promise.

Many individuals rely on access to their health information—directly, through their health care providers, through patient or health plan member portals, or through the use of health apps—to monitor their chronic conditions, adhere to their treatment plans, find and address errors in their health records, and track their progress in wellness and disease management programs. This information provides the individual and their care team with insight into the current state of their health and enables them to set goals for improving it. Equally important, the efficient operation of the health care system depends upon the ability of covered entities [1] and their business associates [2] (collectively, ''regulated entities'') to promptly disclose an individual's protected health information [3] (PHI) to other regulated entities and certain others (*e.g.,* non-covered health care providers, social services agencies, family members) to ensure that individuals receive timely and appropriate care. For example, such disclosures enable health care providers to avoid ordering duplicative or unnecessary tests, which reduces waste and the overall cost of health care. They also facilitate the ability of health care providers to provide care promptly by avoiding long waits for approvals of coverage by health plans.

To foster electronic access to health information by individuals and health care providers, the Trump Administration has launched a series of initiatives to break down barriers to information sharing and form the building blocks for a digital ecosystem in which patients can view, manage, use, and share their health information through digital applications and other modern solutions. The goal of this digital ecosystem is to expand access to personalized health guidance for patients to improve prevention and chronic disease management, while maintaining the privacy and security of PHI in the ecosystem. For example, the Centers for Medicare & Medicaid Services (CMS) is taking bold steps to modernize the nation's digital health ecosystem with a focus on empowering Medicare beneficiaries through greater access to innovative health technologies.[4] As another example, the

[1] *See* 45 CFR 160.103 (definition of ''Covered entity'').

[2] *See* 45 CFR 160.103 (definition of ''Business associate'').

[3] *See* 45 CFR 160.103 (definition of ''Protected health information'').

[4] ''Health Technology Ecosystem,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Sept. 16, 2026), *https://www.cms.gov/priorities/health-technology-ecosystem/overview; see also* Press Release, ''White House, Tech Leaders Commit to Create Patient-Centric Healthcare Ecosystem,'' Centers for Medicare & Medicaid Services, U.S. Department of

Continued

Office of the National Coordinator for Health Information Technology [5] (ONC) adopted certification criteria for health information technology (''health IT'') that support real-time verification of an individual's prescription benefits and standardized electronic prior authorization.[6] The Department also has announced an intention to take an active enforcement stance against health care entities that restrict patients' engagement in their care by blocking the access, exchange, and use of certain health information.[7] As explained by then-Acting Inspector General Juliet T. Hodgkins, ''[p]roviders and certain health IT entities have a legal duty to ensure that information flows where and when it's needed.'' [8]

While it is important that individuals have access to their own health information—in a format of their choosing, including through their personal health apps—and covered entities can use and disclose that information for certain purposes, individuals also have an interest in the privacy of this highly personal information, given the potential for harm if it is shared with the wrong person(s). Thus, it is incumbent upon the Department to establish rules that both enable the use and disclosure of an individual's health information for beneficial purposes and protect the privacy (and security) of that information.

Consistent with these goals, this final rule modifies certain provisions of the Standards for Privacy of Individually Identifiable Health Information (''Privacy Rule''), issued pursuant to section 264 of the Administrative Simplification provisions of title II, subtitle F, of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[9] The Privacy Rule [10] is one of several rules, collectively known as the HIPAA Rules,[11] that establish the required protections for the privacy and security of individuals' PHI, which is individually identifiable health information [12] (IIHI) transmitted by or maintained in electronic media or any other form or medium, with certain exceptions.[13] This final rule supports access by individuals to their PHI and the use and disclosure of PHI by regulated entities for care coordination and case management, discussed in detail below. Specifically, this final rule amends provisions of the Privacy Rule that may present barriers to individual engagement and care coordination and case management—or impose other burdens without sufficiently compensating for, or offsetting, such burdens through privacy protections for PHI. These barriers may impede the transformation of the health care system from a system that pays for procedures and services to one that pays for high-quality health care and empowers individuals to take charge of their health. Consistent with the Department's historical approach to the HIPAA Rules, the amendments generally are technology neutral. Where appropriate, we discuss the application of these amendments, and the Privacy Rule as a whole, to current technology in preamble.

B. Summary of Major Provisions

After consideration of the public comments received in response to the 2021 Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement notice of proposed rulemaking (NPRM) (''2021 Privacy Rule NPRM''), the Department is modifying the Privacy Rule to support individual access and improve care coordination and case management by: [14]

- Modifying provisions on the individual's right of access to PHI by doing all of the following:
  - Adding definitions of the terms ''electronic health record'' and ''personal health application'' (''personal health app'').
  - Reducing the amount of time that covered entities have to respond to an access request to no more than 15 calendar days after receipt of the request (reduced from the current 30 days), with the opportunity for an extension of no more than 30 calendar days (retaining the current 30-day extension).
  - Clarifying the form and format required for responding to individuals' requests for PHI.
  - Reducing the burden of identity verification on individuals exercising their access rights.
  - Limiting the individual's right of access to direct the transmission of PHI to a person they designate to electronic copies of PHI in an electronic health record (''right of access to direct''), in accordance with a binding court decision.[15]
  - Requiring covered entities to inform individuals that they retain their

Health and Human Services (July 30, 2025), *https://www.cms.gov/newsroom/press-releases/white-house-tech-leaders-commit-create-patient-centric-healthcare-ecosystem.*

[5] The Assistant Secretary for Technology Policy (ASTP)/ONC is now referred to as ONC. *See* 91 FR 16204 (Apr. 1, 2026). Although at the time of specific references noted herein ONC was either referenced as ASTP/ONC or as ONC, we use ONC throughout this document for clarity, except where ASTP or ASTP/ONC is used in quoted material.

[6] 45 CFR 170.315(b)(4) and 170.315(g)(31)–(33); *see* 90 FR 36536, 36541–42 (Aug. 4, 2025); *see also* Thomas Keane et al., ''ASTP/ONC Rule Creates Prescription Drug Cost Transparency, Eases Administrative Burden, and Speeds Access to Care,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (July 31, 2025), *https://healthit.gov/blog/healthit-certification/astp-onc-rule-creates-prescription-drug-cost-transparency-eases-administrative-burden-and-speeds-access-to-care/;* Testimony of Thomas Keane, M.D., Assistant Secretary for Technology Policy; Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, Hearing on Transforming Health Care with Data: Improving Patient Outcomes Through Next-Generation Care before Senate Health Education, Labor and Pensions Committee (Mar. 5, 2026), *https://www.help.senate.gov/imo/media/doc/0b360ae0-0290-e896-f8f3-1f230eb3dce7/Keane%20Testimony.pdf.*

[7] Press Release, ''HHS Announces Crackdown on Health Data Blocking,'' U.S. Department of Health and Human Services (Sept. 4, 2025), *https://www.hhs.gov/press-room/hhs-crackdown-health-data-blocking.html.*

[8] *Id.*

[9] Subtitle F of title II of HIPAA (Pub. L. 104–191, 110 Stat. 1936 (Aug. 21, 1996)) added a new part C to title XI of the SSA, Public Law 74–271, 49 Stat. 620 (Aug. 14, 1935) (*see* sections 1171–1179 of the SSA (codified at 42 U.S.C. 1320d–1320d–8)), as well as promulgating section 264 of HIPAA (codified at 42 U.S.C. 1320d–2 note), which authorizes the Secretary to promulgate regulations with respect to the privacy of individually identifiable health information. The Privacy Rule has subsequently been amended pursuant to the Genetic Information Nondiscrimination Act of 2008 (GINA), title I, section 105, Public Law 110–233, 122 Stat. 881 (May 21, 2008) (codified at 42 U.S.C. 2000ff), the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Public Law 111–5, 123 Stat. 226 (Feb. 17, 2009) (codified at 42 U.S.C. 1390w–4(O)(2)), and the Coronavirus Aid, Relief, and Economic Security (CARES) Act, Public Law 116–136, 3221(i), 134 Stat. 378 (Mar. 27, 2020) (codified at 42 U.S.C. 290dd–2 note).

[10] 45 CFR part 160 and subparts A and E of part 164. For a history of the Privacy Rule, *see infra* Section II.B., ''Regulatory and Legal History.''

[11] *See also* the HIPAA Security Rule (''Security Rule''), 45 CFR part 160 and subparts A and C of part 164; the HIPAA Breach Notification Rule, 45 CFR part 164, subpart D; and the HIPAA Enforcement Rule, 45 CFR part 160, subparts C, D, and E.

[12] 42 U.S.C. 1320d; *see also* 45 CFR 160.103 (definition of ''Individually identifiable health information'').

[13] At times throughout this final rule, the Department uses the terms ''health information'' or ''individuals' health information'' to refer generically to health information pertaining to an individual or individuals. In contrast, the Department's use of the term ''IIHI'' refers to a category of health information defined in HIPAA, and ''PHI'' is used to refer specifically to a category of IIHI that is defined by, and subject to, the privacy and security standards promulgated in the HIPAA Rules.

[14] Additional revisions are not listed here because they are not considered major. Generally, the proposals being finalized that are not listed here make non-substantive changes. These proposals are reviewable in section IV. and the amendatory language in the last section of the final rule.

[15] Throughout this document, we use ''right of access to direct'' interchangeably with the full description of the right set forth in at new 45 CFR 164.524(d).

right to obtain copies of their PHI or direct electronic copies of PHI in an electronic health record to another person when a summary of PHI is offered in lieu of a copy.

○ Amending the permissible fee structure for responding to requests made pursuant to the right of access, including specifying when electronic PHI [16] (ePHI) must be provided to the individual at no charge.

○ Requiring covered entities to post estimated fee schedules on their websites for copies of PHI obtained under the right of access and with an individual's valid authorization.

• Amending the definition of health care operations to clarify the scope of permitted uses and disclosures for individual-level care coordination and case management that constitute health care operations.

• Clarifying the ability of covered entities to disclose PHI to social services agencies, community-based organizations, home and community-based services (HCBS) providers,[17] and other similar third parties [18] that provide health-related services, to facilitate care coordination and case management for individuals.

• Eliminating the requirement to obtain an individual's written acknowledgment that they have received a copy of a Notice of Privacy Practices (NPP) from a health care provider with whom they have a direct treatment relationship.

• Modifying the content requirements of the NPP to clarify for individuals their rights with respect to their PHI and how to exercise those rights.

• Expressly permitting disclosures to Telecommunications Relay Services (TRS) communications assistants for persons who are deaf, hard of hearing, or deaf-blind, or who have a speech disability, and modifying the definition of business associate to exclude TRS providers.

• Expanding the permission to use or disclose PHI of Armed Forces members in certain circumstances to all Uniformed Services, which then would include the U.S. Public Health Service (USPHS) Commissioned Corps and the National Oceanic and Atmospheric Administration (NOAA) Commissioned Corps.

The Department carefully considered the extent to which each of these modifications would affect privacy protections for health information and the likely benefits of making PHI more available for care coordination or case management. These and other considerations are fully described for each modification throughout this preamble and in detail in the Regulatory Impact Analysis (RIA).

C. Effective and Compliance Dates

1. 2021 Privacy Rule NPRM

In the 2021 Privacy Rule NPRM, the Department proposed an effective date for a final rule that would occur 60 days after publication, and a compliance date 180 days after the effective date.[19] Taken together, the two dates would give entities 240 days after publication to implement compliance measures. In the preamble to the proposed rule, the Department stated that it did not believe that the proposed rule would pose unique implementation challenges that would justify an extended compliance period (*i.e.,* a period longer than the standard 180 days provided in 45 CFR 160.105).[20]

2. Summary of Comments

While some commenters expressed support for our [21] proposed timeline, most urged us to postpone publication of this final rule or to extend the compliance period for a variety of reasons, such as the coronavirus disease 2019 public health emergency (''COVID–19 PHE'') and pending compliance dates for other Department regulations. Many requested that the Department coordinate compliance deadlines across its rulemakings. Several commenters encouraged the Department to delay enforcement of specific provisions of this final rule.

3. Final Rule

The effective date of this final rule is 60 days after publication. Accordingly, the final rule is effective on January 19, 2027.

Regulated entities will have 180 days beyond the effective date of the final rule to comply with its provisions. We understand that some regulated entities are concerned that they may encounter difficulties complying with the modified requirements within an 180-day period. However, we believe that providing a 180-day compliance period best comports with section 1175(b)(2) of the Social Security Act of 1935 (SSA) [22] and the implementing provision at 45 CFR 160.104(c)(1), which require the Secretary to provide at least a 180-day period for covered entities to comply with modifications to standards and implementation specifications in the HIPAA Rules. We also believe that providing a 180-day compliance period best protects individuals' privacy interests in a manner that reflects the importance of the priorities advanced by this final rule and their effects on individuals, regulated entities, and other persons, while minimizing any new burdens on regulated entities for implementing this final rule.

Section 160.104(a) permits the Department to adopt a modification to a standard or implementation specification adopted under the Privacy Rule no more frequently than once every 12 months. As discussed above, we are required to provide a compliance period of at least 180 days for any modification, but we are permitted to provide a longer compliance period based on the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.[23] The Department makes every effort to consider the burden and cost of implementation for regulated entities when determining an appropriate compliance date. While we recognize that regulated entities will need to revise and implement changes to their policies and procedures in response to the modifications in this final rule, we do not believe that these changes are sufficiently significant that they require more than a 180-day compliance period.

Accordingly, we believe that a 180-day compliance period, combined with a 60-day effective date, is sufficient for regulated entities to make the changes needed to comply with the modifications in this final rule, with the exception of the provisions on business associate agreements, discussed separately, below.

To help reduce administrative burdens on regulated entities, the Department is modifying the provision addressing transition periods at 45 CFR 164.532(e) to afford regulated entities a transition period beyond the 180-day compliance period to modify business associate contracts or other written arrangements [24] (referred to, collectively, as ''business associate agreements'') that would qualify for the

[16] 45 CFR 160.103 (definition of ''Electronic protected health information'').

[17] For purposes of this final rule, the Department refers to HCBS providers as they are described and referenced in the context of the Medicaid program. *See, e.g.,* 42 CFR part 441, subparts G, J, K, and M.

[18] In this rule, the term ''third parties'' refers to a person who is not the individual (or the individual's personal representative) and is not part of a category of persons that is limited to regulated entities. For example, we describe social services agencies as third parties because only a subset of social services agencies may meet the definition of a covered entity.

[19] *See* 86 FR 6446, 6448 (Jan. 21, 2021).

[20] *See id.*

[21] In this final rule, ''we'' and ''our'' denote the Department.

[22] 42 U.S.C. 1320d–4.

[23] 45 CFR 160.104(c).

[24] 45 CFR 164.502(e).

longer transition period, as discussed further below.

4. Response to Public Comments

Comment: Many commenters urged the Department to extend the compliance date for this final rule for various reasons, including the need to focus resources on addressing the COVID–19 PHE and implementation of other Federal statutes and regulations, such as the CMS Interoperability and Patient Access Final Rule [25] and ONC's 21st Century Cures Act: [26] Interoperability, Information Blocking, and the ONC Health IT Certification Program (''Cures Act Final Rule'').[27] Some commenters recommended that the Department provide a longer compliance period because of cost and limitations on resources and time for revising policies, implementing technical changes, and training workforce members. Suggested compliance dates generally ranged from 1 to 2 years after the effective date. One commenter suggested that we provide regulated entities with additional time to comply with the modifications to the right of access because they believed that new processes and technological changes would be required to implement some of the proposals.

Response: As discussed above, we do not believe that the modifications required by this final rule generally will take longer than 180 days to implement. Additionally, the COVID–19 PHE officially ended in 2023, more than 2 years ago [28] and the regulations referenced by commenters most frequently had effective dates in 2020, more than 5 years ago. Our assessment of the feasibility of the implementation timeline would not change even if these events were not in the past. Accordingly, we are confident that a compliance date of July 19, 2027 provides regulated entities with sufficient time to comply with this final rule.

Comment: One commenter requested that we provide health plans with additional time for compliance because they are required to provide updated NPPs to their members.

Response: Where a health plan makes a material change to its NPP, 45 CFR 164.520(c)(1)(v) permits a health plan that posts its NPP on its website to provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan if it posts the change or its revised notice on its website by the effective date of the material change to the notice.[29] A health plan that does not post its NPP on its website must provide individuals with the revised notice or information about the material change and how to obtain the revised notice within 60 days of revising the notice.[30] Thus, the Privacy Rule already provides a health plan with additional time to provide individuals with their own copy of the revised NPP where it posts the revised NPP on its website within the allotted time.

Comment: A few commenters requested that the Department provide additional time for regulated entities to revise business associate agreements and other contracts affected by the provisions of this final rule.

Response: We recognize that 240 days may not be sufficient for regulated entities to both implement the modifications that the Department is finalizing as part of this rule and bring their business associate agreements into compliance. While compliant business associate agreements are important for ensuring that covered entities and business associates clearly identify the permissible uses and disclosures of PHI and each party's respective responsibilities,[31] our first priority is to ensure the timely implementation of the policies in this final rule. Accordingly, as discussed below, this final rule revises 45 CFR 164.532(e) to provide regulated entities a transition period for certain business associate agreements to help reduce administrative burdens on regulated entities.

D. Severability

The Department intends that any provisions of the Privacy Rule and its subparts that are unchanged by this final rule shall remain in full force and effect, even if other modified or new provisions in this final rule are held to be invalid or unenforceable, or are stayed pending future judicial or agency action.

The Department also believes that, if a court or further agency action deems invalid or unenforceable any language or section of a provision that is newly finalized or modified in this rulemaking, the remaining provisions that reference the language or section held invalid or unenforceable, but that are not directly related to a covered entity's ability to implement the remaining language or section, will remain in effect and be given the maximum regulatory effect permitted under the law.

The Department is finalizing significant changes related to the individual right of access. We believe these changes are severable such that the individual right of access as a whole or aspects of the right, as they existed until the effective date of this final rule, shall remain in effect should any changes finalized in this rulemaking related to the right as a whole or such aspects of that right be held invalid or unenforceable.

For example, the Department is adopting a new definition at 45 CFR 164.501 for the term ''electronic health record.'' While the Department believes that this new definition will aid in covered entities' and individuals' understanding of the full scope of obligations and rights under the Privacy Rule and the HITECH Act,[32] a covered entity's obligation to implement the right of access to direct [33] is not dependent on the adopted definition of electronic health record. Accordingly, the Department believes that the right of an individual to direct an electronic copy of PHI in an electronic health record to a person designated by the individual, finalized at 45 CFR 164.524(d), remains intact should the new definition be held invalid or unenforceable.

Similarly, the Department believes that the new definition of personal health app is severable from the obligation of a covered entity to provide access to the individual in a timely manner by, among other things, transmitting the requested copy of the PHI through the individual's personal health app, as codified at 45 CFR 164.524(c)(3).[34] Even without the definition of personal health app, covered entities and individuals retain the ability to agree to an acceptable form and format for a requested copy of PHI. Prior to this rulemaking, the Privacy Rule already provided individuals with

[25] 85 FR 25510 (May 1, 2020).

[26] Public Law 114–255, 130 Stat. 1033 (Dec. 13, 2016).

[27] 85 FR 25642 (May 1, 2020).

[28] Press Release, ''HHS Secretary Xavier Becerra Statement on End of the COVID–19 Public Health Emergency,'' U.S. Department of Health and Human Services (May 11, 2023), *https://us.pagefreezer.com/en-US/wa/browse/0a7f82bb-be6e-448a-ae11-373d22c37842?find-by-timestamp=2024-01-02T03:56:59Z&url=https:%2F%2Fwww.hhs.gov%2Fabout%2Fnews%2F2023%2F05%2F11%2Fhhs-secretary-xavier-becerra-statement-on-end-of-the-covid-19-public-health-emergency.html&timestamp=2024-01-02T03:43:14Z.*

[29] 45 CFR 164.520(c)(1)(v)(A).

[30] 45 CFR 164.520(c)(1)(v)(B).

[31] *See* 78 FR 5566, 5601 (Jan. 25, 2013).

[32] Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111–5, 123 Stat. 226 (Feb. 17, 2009) (codified at 42 U.S.C. 201 note).

[33] 42 U.S.C. 17935(e)(1).

[34] *See also* 45 CFR 164.524(c)(2)(ii).

a right to an electronic copy of their PHI that is maintained electronically in the electronic form and format requested by the individual, if it is readily producible, or if not, in a readable electronic form and format as agreed to by the covered entity and the individual. The requirement to provide PHI in the individual's chosen form and format, where readily producible, is a longstanding component of the individual right of access. Thus, the Department believes that individuals should retain the right to request copies of PHI through a personal health app, even if the definition of personal health app is held to be invalid or unenforceable.

We are adopting several provisions that address the fees that covered entities may charge to fulfill an individual's request for access to their PHI. The Department believes that if these new provisions are held to be invalid or unenforceable for any reason, such holdings would not interfere with the ability of covered entities to implement existing provisions related to fees. For example, at 45 CFR 164.524(c)(4)(ii), the Department prohibits a covered entity from charging a fee when the covered entity is unlikely to incur costs for providing the individual with copies of PHI, including when an individual requests—regardless of the manner in which the request is made—that the covered entity provide their PHI through a personal health app or when an individual seeks to exercise the right to inspect their own PHI. Should the new fee prohibitions be held invalid or unenforceable, the existing provisions at 45 CFR 164.524(c)(4) [35] should remain intact. Removing the new fee limitations would not affect a covered entity's ability to continue to implement the current fee requirements or other right of access obligations. Similar considerations apply to the newly finalized requirement at 45 CFR 164.524(c)(2)(iv)(B) that a covered entity inform an individual to whom it offers to provide a summary in lieu of a copy of PHI that the individual retains the right to obtain the copy. To the extent a court invalidates that requirement, the current existing provision permitting the covered entity to provide the summary in lieu of a copy remains.

Certain other new provisions also are wholly severable, including the examples below, which are illustrative and not exhaustive:

- If the new provision that excludes a provider of TRS from the definition of business associate is held to be invalid or unenforceable, the existing definition of business associate at 45 CFR 160.103 remains in effect.
- If the modified provisions that reference Uniformed Services instead of Armed Forces, military, or military services are held to be invalid or unenforceable, the standard permitting uses and disclosures of PHI for specialized government functions in 45 CFR 164.512(k) remains intact.
- If the provision at 45 CFR 164.512(m) that addresses disclosures to TRS is held to be invalid or unenforceable, the other provisions of 45 CFR 164.512 remain intact.
- If the modifications to 45 CFR 164.524(b)(1)(iii) that generally prohibit a covered entity from imposing measures that impede requests for access is held to be invalid or unenforceable, the ability of a covered entity to require an individual to make a request for access to the individual's PHI in writing provided that it informs the individual of the requirement in 45 CFR 164.524(b)(1)(ii) remains in effect.
- If the modifications to the amount of time that a covered entity has to respond to a request for access are held to be invalid or unenforceable, the prior existing requirements that address timeliness of responses to requests for access in 45 CFR 164.524(b)(2) remain in effect.
- If the provision at 45 CFR 164.524(c)(2)(iii) that addresses form and format requirements for requested copies of PHI is held to be invalid or unenforceable, the other paragraphs in 45 CFR 164.524(c)(2) remain intact.
- If the new provision at 45 CFR 164.525 that requires covered entities to provide notice of access and authorization fees is held to be invalid or unenforceable, all existing provisions for the individual right of access at 45 CFR 164.524 remain in effect.

II. Statutory and Regulatory Background

A. Statutory Authority and History

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

In 1996, Congress enacted HIPAA [36] to reform the health care system to ''improve portability and continuity of health insurance coverage in the group and individual markets'' [37] and to support the electronic exchange of health information. To enable health care system reform, Congress included requirements for standards to support the electronic exchange of health information. According to section 261 of HIPAA, ''[i]t is the purpose of this subtitle to improve [. . .] the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.'' [38] Congress applied HIPAA's Administrative Simplification provisions directly to three types of persons referred to in regulation as ''covered entities'': health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with a transaction for which HHS has adopted a standard.[39]

Section 262(a) of HIPAA required the Secretary to adopt uniform standards ''to enable health information to be exchanged electronically.'' [40] Congress also directed the Secretary to adopt standards for, among other things: transactions and data elements relating to health information,[41] the security of that information,[42] and verification of electronic signatures.[43]

Congress recognized that the standardization of certain electronic health care transactions required by HIPAA posed risks to the privacy of confidential health information and viewed individual privacy, confidentiality, and data security as critical for orderly administrative simplification.[44] One Member of

[35] For purposes of this severability discussion, the reference to 45 CFR 164.524(c)(4) refers to the provisions at 45 CFR 164.524(c)(4)(i)-(iv) in effect prior to the amendments adopted in this final rule. This final rule renumbers those provisions as 45 CFR 164.524(c)(4)(A)–(D).

[36] Public Law 104–191, 110 Stat. 1936 (Aug. 21, 1996) (codified at 42 U.S.C. 201 note).

[37] *See* H.R. Rep. No. 104–496, at 66 (1996).

[38] Sec. 261 of Public Law 104–191, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d note); subtitle F of HIPAA also amended related provisions of the SSA.

[39] *See* sec. 262(a) of Public Law 104–191, 110 Stat. 2021, adding sec. 1172 to the SSA (codified at 42 U.S.C. 1320d–1); *see also* sec. 13404 of the American Recovery and Reinvestment Act of 2009, Public Law 111–5, 123 Stat. 115 (Feb. 17, 2009) (codified at 42 U.S.C. 17934) (applying privacy provisions and penalties to business associates of covered entities). The Department codified the term ''covered entity'' and defined it using these three categories of persons. 45 CFR 160.103.

[40] Sec. 262(a) of Public Law 104–191, 110 Stat. 2021, adding sec. 1173(a) (codified at 42 U.S.C. 1320d–2(a)(1)).

[41] 42 U.S.C. 1320d–2(a), (c), and (f).

[42] 42 U.S.C. 1320d–2(d).

[43] 42 U.S.C. 1320d–2(e).

[44] On a resolution waiving points of order against the Conference Report to H.R. 3103, members debated an ''erosion of privacy'' balanced against the administrative simplification provisions. Thus, from HIPAA's inception, privacy has been a central concern to be addressed as legislative changes eased disclosures of PHI. *See* 142 Cong. Rec. H9777 and H9780; *see also* H.R. Rep. No. 104–736, at 264–265 (1996); 142 Cong. Rec. H9780 (daily ed. Aug. 1,

Continued

Congress acknowledged that individuals should have ''control over who actually has access to their medical records.'' [45] According to another Member of Congress, privacy standards would create an additional layer of protection beyond the oath pledged by health care providers to keep information secure and, as described by another Member, would further protect information from being used in a ''malicious or discriminatory manner.'' [46] Moreover, Congress considered that health care reform required an approach that would not compromise privacy as health information became more accessible.[47] Additionally, another Member acknowledged that health plan data was often nonstandard, and the bill ''would facilitate the coordination of benefits between different systems.'' [48]

Section 264(a) of HIPAA directed the Secretary to submit to Congress detailed recommendations for Federal ''standards with respect to the privacy of individually identifiable health information [IIHI]'' within 1 year of HIPAA's enactment.[49] The statute made clear that the Secretary had the authority to promulgate regulations if Congress did not enact legislation covering these matters within 3 years.[50] Congress directed the Secretary to ensure that the regulations promulgated ''address at least'' the following three subjects: (1) the rights that an individual who is a subject of IIHI should have; (2) the procedures that should be established for the exercise of such rights; and (3) the uses and disclosures of such information that should be authorized or required.[51]

Additionally, Congress provided a clear statement that HIPAA's provisions would ''supersede any contrary provision of State law,'' with certain limited exceptions.[52] One exception to this general preemption authority is for state privacy laws that are contrary to and more stringent than the corresponding Federal standard, requirement, or implementation specification.[53] Thus, Congress provided for the Department to create privacy standards to safeguard health information while respecting the ability of states to provide individuals with additional health information privacy protections and rights.

Congress required the Secretary to rely on recommendations of the National Committee on Vital and Health Statistics (NCVHS or ''Committee'') when adopting standards,[54] thereby ensuring that the Secretary's decisions reflected public and expert involvement and advice in carrying out the requirements of section 264.[55] On June 27, 1997, NCVHS sent its initial recommendations to the Secretary. Among its recommendations was that legislation for health privacy should include some specific rights for individuals, including a right to be informed about uses of their health information and a right to request amendment of their records.[56] Additionally, NCVHS recommended that an individual have the right to access their health information.[57] As the Committee explained, a basic element of fair information practices for ''personal records maintained by third party record keepers—is a right of access by the subject of the record.'' [58] NCVHS further asserted that fair information practices for health information would provide secondary users of health information with knowledge about when they could have health information and when they could not, what their obligations would be, and what penalties would result if those obligations were ignored.[59]

NCVHS also supported ''limiting use and disclosure of identifiable information to the minimum amount necessary to accomplish the purpose. The Committee strongly believe[d] that when identifiable health information is made available for non-health uses, patients deserve a strong assurance that the data will not be used to harm them.'' [60] NCVHS also believed that users of health information should be required to justify their need for such information and accept reasonable substantive and procedural limitations on access.[61]

Congress anticipated that the Department's rulemaking under HIPAA would not remain static. Congress built in a mechanism to update or adapt the regulations to address evolving technology and health care practices, directing the Secretary to review and adopt modifications to the Administrative Simplification standards as determined appropriate, but not more frequently than once every 12 months.[62] That statutory directive complements the Secretary's general rulemaking authority to ''make and publish such rules and regulations, not inconsistent with this chapter, as may be necessary to the efficient administration of the functions with which each is charged under [the Social Security Act].'' [63]

As discussed below, Congress did not adopt legislation on the privacy of IIHI within the period of time specified in HIPAA. As a result, it became the Secretary's obligation under HIPAA to adopt regulatory standards for the privacy of health information.

2. The Health Information Technology for Economic and Clinical Health (HITECH) Act

On February 17, 2009, Congress enacted the HITECH Act [64] to promote the nationwide adoption and standardization of health IT. The HITECH Act included additional privacy and security requirements for regulated entities and expanded certain rights of individuals with respect to their PHI. Among other things, the HITECH Act expanded the individual right of access to include the right of an

1996) (statement of Rep. Sawyer); 142 Cong. Rec. H9792 (daily ed. Aug. 1, 1996) (statement of Rep. McDermott); 142 Cong. Rec. S9515–17 (daily ed. Aug. 2, 1996) (statement of Sen. Simon).

[45] *See* statement of Sen. Simon, *supra* note 44.

[46] *See* statement of Rep. Sawyer, *supra* note 44; *see also* statement of Sen. Simon, *supra* note 44.

[47] *See* H.R. Rep. No. 104–496, at 100 (1996).

[48] *See* statement of Rep. Sawyer, *supra* note 44.

[49] Public Law 104–191, 110 Stat. 2021 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d–2 note).

[50] *Id.*

[51] *Id.*

[52] 42 U.S.C. 1320d–7.

[53] 65 FR 82462, 82580 (Dec. 28, 2000) (the exception applies under section 1178(a)(2)(B) of the SSA and section 264(c)(2) of HIPAA); *see also* 42 U.S.C. 1320d–7. Other exceptions to the general preemption authority include: state laws that the Secretary of HHS determines are necessary to prevent fraud and abuse, to ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery or costs, or for other purposes; state laws that address controlled substances; state laws providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention; and state laws requiring a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

[54] NCVHS is HHS' statutory public advisory body on health data, statistics, and national health information policy. *See* ''National Committee on Vital and Health Statistics (NCVHS),'' U.S. Centers for Disease Control and Prevention, U.S. Department of Health and Human Services (June 1, 2026), *https://www.cdc.gov/faca/committees/ncvhs.html; see also* ''NCVHS 60th Anniversary Symposium and History,'' U.S. Department of Health and Human Services, at 28–29 (Feb. 2011), *https://ncvhs.hhs.gov/wp-content/uploads/2014/05/60_years_of_difference.pdf.*

[55] *See* sec. 264(a) and (d) of Public Law 104–191, 110 Stat. 2033 (codified at 42 U.S.C. 1320d–2 note).

[56] *See* 62 FR 39844 (July 24, 1997), *https://www.govinfo.gov/content/pkg/FR-1997-07-24/html/97-19492.htm.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] Sec. 262(a) of Public Law 104–191, 110 Stat. 2021, adding sec. 1174(b)(1) (codified at 42 U.S.C. 1320d–3).

[63] Sec. 1102 of the SSA (codified at 42 U.S.C. 1302).

[64] Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111–5, 123 Stat. 226 (Feb. 17, 2009) (codified at 42 U.S.C. 201 note).

individual to direct a covered entity to transmit an electronic copy of PHI in an electronic health record to a person designated by the individual.[65] The HITECH Act also imposed a limit on fees that a covered entity is permitted to charge for certain requests to disclose PHI.[66] Additionally, the HITECH Act included clarifications to the standard requiring regulated entities to make reasonable efforts to limit most uses, disclosures, and requests for PHI to the minimum amount necessary to accomplish the purpose (''minimum necessary standard'').[67]

When enacting the HITECH Act, Congress understood that privacy and security standards were critical to the development of a connected health IT landscape, which itself was ''a necessary and vital component of health care reform.'' [68] The Purpose statement of an accompanying House of Representatives report [69] on the Energy and Commerce Recovery and Reinvestment Act [70] recognizes that ''[i]n addition to costs, concerns about the security and privacy of health information have also been regarded as an obstacle to the adoption of [health IT].'' The Senate Report for S. 336 [71] similarly acknowledges that ''[i]nformation technology systems linked securely and with strong privacy protections can improve the quality and efficiency of health care while producing significant cost savings.'' [72] The HITECH Act strengthened the privacy and security protections for health information to support Congress' goal of promoting widespread adoption and interoperability of health IT.[73]

In passing the HITECH Act, Congress instructed the Department that any new health IT standards adopted under section 3004 of the Public Health Service Act (PHSA) must take into account the privacy and security requirements of the HIPAA Rules.[74] Congress also affirmed that the existing HIPAA Rules were to remain in effect to the extent that they are consistent with the HITECH Act and directed the Secretary to revise the HIPAA Rules as necessary for consistency with the HITECH Act.[75] Congress confirmed that the new law was not intended to have any effect on authorities already granted under HIPAA to the Department, including section 264 of that statute and the regulations issued under that provision.[76]

3. Patient Protection and Affordable Care Act

On March 23, 2010, Congress enacted the Patient Protection and Affordable Care Act [77] (ACA). While not its primary focus,[78] the ACA amended the Administrative Simplification provisions of HIPAA. Specifically, it modified section 261 of HIPAA to clarify that, in addition to improving the Medicare and Medicaid programs and the efficiency and effectiveness of the health care system, the purpose of the Administrative Simplification provisions is ''to reduce the clerical burden on patients, health care providers, and health plans.'' [79] According to one Member of Congress, enactment of the ACA eliminated ''unnecessary administrative costs in [the] health care system,'' [80] while another Member of Congress asserted that the ACA was ''poised to provide access to quality health insurance for all Americans.'' [81] The ACA also modified section 261 of HIPAA to clarify that the standards for encouraging the development of a health information system are to be ''uniform.'' [82]

4. Coronavirus Aid, Relief, and Economic Security (CARES) Act

On March 27, 2020, Congress enacted the CARES Act.[83] Among other things, the CARES Act directed the Secretary to update the provisions of the Privacy Rule pertaining to the NPP to align with the provisions of the regulations on the Confidentiality of Substance Use Disorder Patient Records that address the required patient notice.[84]

B. Regulatory and Legal History

The Secretary has delegated the authority to administer the HIPAA Rules and to make decisions regarding their implementation, interpretation, and enforcement to the HHS Office for Civil Rights (OCR).[85] The Department exercised its authority to issue the Privacy Rule in 2000 and then to modify it several times—in 2002, 2013, 2014, 2016, and 2024.[86]

1. 2000 Privacy Rule

As directed by HIPAA, the Department provided a set of recommendations to Congress for a potential new law that would address the privacy of IIHI.[87] Congress did not enact legislation governing standards with respect to the privacy of IIHI within its 3-year self-imposed deadline. As a result, the Department published a proposed rule setting forth the required standards on November 3, 1999,[88] and issued the first final rule establishing ''Standards for Privacy of Individually Identifiable Health Information'' (''2000 Privacy Rule'') on December 28, 2000.[89]

The 2000 Privacy Rule set standards to protect the privacy of IIHI to ''begin to address growing public concerns that

[65] *See* 42 U.S.C. 17935(e).

[66] *See* 42 U.S.C. 17935(e)(3).

[67] *See* 42 U.S.C. 17935(b)(2).

[68] C. Stephen Redhead, ''The Health Information Technology for Economic and Clinical Health (HITECH) Act,'' Congressional Research Service, R40161 (2009), *https://crsreports.congress.gov/product/pdf/R/R40161/*9 (''[Health IT], which generally refers to the use of computer applications in medical practice, is widely viewed as a necessary and vital component of health care reform.'').

[69] H.R. Rep. No. 111–7, at 74 (2009), accompanying H.R. 629, 111th Congress (2009).

[70] H.R. 629, Energy and Commerce Recovery and Reinvestment Act of 2009, introduced in the House on January 22, 2009, contained nearly identical provisions to subtitle D of the HITECH Act.

[71] Congress enacted the American Recovery and Reinvestment Act of 2009, which included the HITECH Act, on February 17, 2009. While it was the House version of the bill, H.R. 1, that was enacted, the Senate version, S. 336, contained nearly identical provisions to subtitle D of the HITECH Act. Public Law 111–5, 111 Stat. 115 (2009).

[72] S. Rep. No. 111–3 accompanying S. 336, 111th Congress, at 59 (2009).

[73] Subtitle D of Title XIII of the HITECH Act (codified at 42 U.S.C. 17921, 42 U.S.C. 17931–17940, and 42 U.S.C. 17951–17953).

[74] Sec. 3009(a)(1)(B) of the PHSA, as added by sec. 13101 of the HITECH Act (codified at 42 U.S.C. 300jj–19(a)(1)).

[75] Sec. 13421(b) of the HITECH Act (codified at 42 U.S.C. 17951).

[76] Sec. 3009(a)(1)(A) of the PHSA, as added by sec. 13101 of the HITECH Act (codified at 42 U.S.C. 300jj–19(a)(1)).

[77] Public Law 111–148, 124 Stat. 119 (Mar. 23, 2010).

[78] *See* ''About the Affordable Care Act,'' U.S. Department of Health and Human Services (Mar. 17, 2022), *https://www.hhs.gov/healthcare/about-the-aca/index.html.*

[79] Sec. 1104(a) of Public Law 111–148, 124 Stat. 146 (Mar. 23, 2010) (codified at 42 U.S.C. 1320d note).

[80] 155 Cong. Rec. S11580 (Nov. 19, 2009) (statement of Sen. Cardin).

[81] 156 Cong. Rec. H1856 (daily ed. Mar. 21, 2010) (statement of Sen. Waxman).

[82] Sec. 1104(a) of Public Law 111–148, 124 Stat. 146 (Mar. 23, 2010) (codified at 42 U.S.C. 1320d note).

[83] Public Law 116–136, 134 Stat. 281 (Mar. 27, 2020).

[84] *See* sec. 3221(i)(2) of Public Law 116–136, 134 Stat. 378 (Mar. 27, 2020) (codified at 42 U.S.C. 290dd–2 note).

[85] *See* ''Office for Civil Rights; Statement of Delegation of Authority,'' U.S. Department of Health and Human Services, 65 FR 82381 (Dec. 28, 2000); ''Office for Civil Rights; Delegation of Authority,'' U.S. Department of Health and Human Services, 74 FR 38630 (Aug. 4, 2009).

[86] *See* 78 FR 5566 (Jan. 25, 2013); 79 FR 7290 (Feb. 6, 2014); 81 FR 382 (Jan. 6, 2016); 89 FR 32976 (Apr. 26, 2024).

[87] *See* ''Confidentiality of Individually Identifiable Health Information,'' Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services (Sept. 1997), *https://aspe.hhs.gov/reports/confidentiality-individually-identifiable-health-information.*

[88] 64 FR 59918 (Nov. 3, 1999).

[89] 65 FR 82462 (Dec. 28, 2000).

advances in electronic technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding'' health information.[90] The use of the standards would improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for IIHI.[91]

The 2000 Privacy Rule established ''general rules'' for uses and disclosures of PHI by covered entities, such as the circumstances in which a covered entity was required to limit its requests for PHI, or responses to such requests, to the minimum PHI necessary to accomplish the intended purpose of the use or disclosure.[92] The 2000 Privacy Rule also specified the circumstances in which a covered entity was required to obtain an individual's consent, authorization, or the opportunity for the individual to agree or object.[93] Additionally, it established circumstances for when a covered entity is permitted to use or disclose PHI without an individual's consent, authorization, or opportunity to agree or object; how a covered entity is to determine what constitutes the minimum PHI necessary to accomplish the intended purpose of a requested use or disclosure; and verification of the identity of a person requesting PHI and the authority of such person to have access to PHI under the Privacy Rule.[94] In particular, the 2000 Privacy Rule permitted certain uses and disclosures of PHI, without the individual's authorization, for identified activities such as: public health activities, judicial and administrative proceedings, law enforcement purposes, to avert a serious threat to health or safety, and, in certain circumstances, to ensure the proper execution of the military mission.[95]

The 2000 Privacy Rule also established the rights of individuals with respect to their PHI, including the right to receive adequate notice of a covered entity's privacy practices, the right to request restrictions of uses and disclosures, the right to access (*i.e.,* to inspect and obtain a copy of) their PHI, the right to request an amendment of their PHI, and the right to receive an accounting of disclosures.[96] As part of the right of access, the 2000 Privacy Rule instituted requirements for timely action by covered entities, form and format of copies, the denial of access, and documentation in addition to imposing limitations on the fees a covered entity was permitted to charge for providing an individual with a copy of their PHI.[97]

The 2000 Privacy Rule codified at 45 CFR 160.104(a) the Secretary's statutory authority to modify any standard or implementation specification adopted under the Administrative Simplification provisions.[98] The Secretary first invoked this modification authority to amend the Privacy Rule in 2002 [99] and made additional modifications in 2013,[100] 2014,[101] 2016,[102] and 2024.[103]

2. 2002 Privacy Rule

After publication of the 2000 Privacy Rule, the Department received many inquiries and unsolicited comments about the Privacy Rule's effects and operation. As a result, the Department opened the 2000 Privacy Rule for further comment in February 2001, less than 1 month before the effective date and 25 months before the compliance date for most covered entities.[104] NCVHS' Subcommittee on Privacy, Confidentiality and Security held public hearings about the 2000 Privacy Rule. From those hearings, public comments, meetings requested by industry and other stakeholders, as well as other communications, the Department obtained additional information about concerns related to certain provisions and their potential unintended consequences for health care quality and access.[105] On March 27, 2002, the Department proposed modifications to the 2000 Privacy Rule that maintained strong protections for the privacy of IIHI, while clarifying misinterpretations, addressing the unintended negative effects of the 2000 Privacy Rule on health care quality or access to health care, and relieving unintended administrative burden.[106]

In response to comments on the proposed rule, the Department finalized modifications to the Privacy Rule on August 14, 2002 (''2002 Privacy Rule'').[107] The 2002 Privacy Rule addressed certain workability issues, including by clarifying distinctions between health care operations and marketing, and modified the minimum necessary standard to exclude disclosures authorized by individuals and clarify its operation. Additionally, the Department eliminated the consent requirement for uses and disclosures of PHI for treatment, payment, or health care operations (TPO). The consent changes were balanced by strengthening the NPP provisions to require direct treatment providers to make a good faith effort to obtain a written acknowledgment of receipt of the NPP, thereby preserving an individual's opportunity to raise questions about an entity's privacy policies previously provided in the consent requirements.[108] The Department also included modifications to the provisions permitting the use or disclosure of PHI for public health activities and for research activities without consent, authorization, or an opportunity to agree or object.

3. 2013 Omnibus Rule

Following the enactment of the HITECH Act, the Department proposed modifications to the Privacy, Security, and Enforcement Rules to implement the new statutory requirements and to improve the workability and effectiveness of these rules.[109]

On January 25, 2013, the Department issued the final rule ''Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules'' [110] (''2013 Omnibus Rule''), which implemented many of the new HITECH Act requirements, including strengthening individuals' privacy rights related to their PHI.

The Department also finalized regulatory provisions that were not required by the HITECH Act, but were necessary to address the workability and effectiveness of the Privacy Rule and to increase flexibility for and decrease burden on regulated entities.[111] As the

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *See* 45 CFR 164.520, 164.522, 164.524, 164.526, and 164.528.

[97] 65 FR 82462 (Dec. 28, 2000).

[98] *Id.*

[99] *See* 67 FR 53182 (Aug. 14, 2002).

[100] *See* 78 FR 5566 (Jan. 25, 2013).

[101] *See* 79 FR 7290 (Feb. 6, 2014).

[102] *See* 81 FR 382 (Jan. 6, 2016).

[103] *See* 89 FR 32976 (Apr. 26, 2024).

[104] 66 FR 12738 (Feb. 28, 2001).

[105] 67 FR 53182, 53183 (Aug. 14, 2002).

[106] 67 FR 14775 (Mar. 27, 2002).

[107] 67 FR 53182 (Aug. 14, 2002).

[108] *Id.*

[109] 75 FR 40868 (July 14, 2010).

[110] 78 FR 5566 (Jan. 25, 2013). In addition to finalizing requirements of the HITECH Act that were proposed in the July 14, 2010, NPRM, the Department adopted modifications to the previous Enforcement Rule modifications provided in an interim final rule, 74 FR 56123 (Oct. 30, 2009), and to the Breach Notification Rule provided in an interim final rule, 74 FR 42740 (Aug. 24, 2009). The Department also finalized previously proposed Privacy Rule modifications as required by the Genetic Information Nondiscrimination Act of 2008, 74 FR 51698 (Oct. 7, 2009).

[111] *See* 78 FR 5566 (Jan. 25, 2013) (explaining that the Department was using its general authority under HIPAA to make several changes to the Privacy Rule that were intended to increase

Department explained in the 2010 NPRM, information gleaned from contact with the public through various forums and through the process of enforcement supported the proposed technical corrections to improve workability, effectiveness, and flexibility.[112]

The Department also modified the Privacy Rule to implement the HITECH Act's provisions that extended direct liability for compliance with certain provisions of the Privacy Rule to business associates.[113]

In the 2013 Omnibus Rule, the Department issued regulations expanding the HITECH Act requirements to avoid ''a complex set of disparate requirements for access,'' such as different requirements for access to paper versus electronic records.[114] The Department strengthened the right of access by applying section 13405(e) of the HITECH Act uniformly to all PHI in one or more designated record sets, regardless of whether the PHI is in an electronic health record or the copy is in electronic form.[115] The Department also explained that the Privacy Rule already applied the right of access to PHI held in designated record sets and required a covered entity to provide the PHI in the ''form and format'' requested by the individual, including electronically, if ''readily producible.'' [116]

The 2013 Omnibus Rule also finalized provisions requiring covered entities to transmit a copy of an individual's PHI directly to a person designated by the individual if the individual's request for access directs the covered entity to do so.[117] The Department noted that, in contrast to other access requests by individuals pursuant to 45 CFR 164.524, requests to transmit a copy of PHI to another person must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.[118]

With respect to fees for access, the 2000 Privacy Rule permitted a covered entity to impose only a reasonable, cost-based fee for a copy of PHI under the right of access. Additionally, section 13405(e)(2) of the HITECH Act provided that, where a covered entity uses or maintains an electronic health record, any fee for providing electronic copies (or summary or explanation) of PHI shall not be greater than the entity's labor costs in responding to the request. Therefore, to implement the fee provisions of the HITECH Act, the 2013 Omnibus Rule amended 45 CFR 164.524(c)(4) to provide that fees could include labor or supplies whether the PHI was in paper or electronic form.[119]

4. 2014 Privacy Rule

In 2011, the Department proposed modifications to the Privacy Rule, in conjunction with proposed modifications to the regulations under the Clinical Laboratory Improvement Amendments of 1988 [120] (CLIA), that were intended to provide individuals with a new way to obtain direct access to their PHI.[121] These proposals were based on recommendations from a Federal advisory committee that identified CLIA regulations as being perceived by some stakeholders as imposing barriers to the exchange of health information.[122]

In 2014, the Department adopted modifications to remove barriers to an individual's direct access to their own test reports from laboratories in a final rule entitled, ''CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports'' [123] (''2014 Privacy Rule''). The Department acknowledged that the Privacy Rule already gave individuals the right to obtain access to their laboratory test reports from their covered health care providers, but explained that these changes gave patients a new option to obtain their test reports directly from the laboratory while maintaining strong protections for patients' privacy.[124]

The 2014 Privacy Rule eliminated the exception to an individual's right to access their PHI when it is held by a CLIA-certified or CLIA-exempt laboratory. Thus, both those laboratories that are subject to CLIA and those that are exempt from it have the same obligations as other types of covered health care providers with respect to providing individuals, or their personal representatives, with access to their PHI in accordance with the individual right of access.

5. 2016 HIPAA Access Guidance

On January 7, 2016, the Department issued guidance (''2016 Access Guidance'') to educate the public about the individual right of access at 45 CFR 164.524.[125] The 2016 Access Guidance explained the right of access to inspect and obtain PHI and the right of access to direct a copy of PHI to another person. It also clarified the pre-existing conditions and requirements of the individual access right, including its fee limitations and requirements with respect to the form and format and manner of access, as they applied to the right of access to direct. The guidance stated that the limitations on access fees applied, regardless of whether the individual requested that the copy of PHI be sent to the individual or directed the copy of PHI to a person designated by the individual.

6. 2018 HIPAA Rules Request for Information

In 2018, the Department published the ''Request for Information on Modifying HIPAA Rules to Improve Coordinated Care'' [126] (''2018 RFI'') to solicit public comments that offered recommendations for modifying existing regulations or guidance, or developing new guidance on reducing regulatory barriers to coordinated care. The 2018 RFI solicited public input on whether and how the Department could modify the HIPAA Rules to support care coordination and case management and promote value-based care, while preserving the privacy and security of PHI.

The Department solicited recommendations on how best to use the HIPAA Rules to support care coordination in three specific ways:

- Promoting information disclosure for care coordination and case management.

workability and flexibility, decrease burden, and better harmonize the requirements with those under other Departmental regulations). The Department's general authority to modify the Privacy Rule is codified in HIPAA section 264(c), and OCR conducts rulemaking under HIPAA based on authority granted by the Secretary.

[112] 75 FR 40868, 40871 (July 14, 2010).

[113] *See* 78 FR 5566 (Jan. 25, 2013); *see also* ''Direct Liability of Business Associates,'' Office for Civil Rights, U.S. Department of Health and Human Services (July 16, 2021), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html.*

[114] 75 FR 40868, 40901 (July 14, 2010).

[115] *Id.*

[116] 45 CFR 164.524(c)(2)(ii); *see also* 78 FR 5566, 5633 (Jan. 25, 2013).

[117] 45 CFR 164.524(c)(3)(ii); *see also* 78 FR 5566, 5634 (Jan. 25, 2013).

[118] 78 FR 5566, 5634 (Jan. 25, 2013).

[119] *Id.* at 5566, 5635–36.

[120] 42 U.S.C. 263a. CLIA and the implementing regulations established nationwide quality standards to ensure the accuracy, reliability, and timeliness of clinical laboratories' test results. The NPRM also proposed modifications to CLIA regulations to allow laboratories subject to CLIA to give a patient or the patient's personal representative access to the patient's completed test reports, using the laboratory's authentication process, on the patient's or patient's personal representative's request.

[121] 76 FR 56712 (Sept. 14, 2011).

[122] *Id.* at 56713.

[123] 79 FR 7290 (Feb. 6, 2014).

[124] *Id.* at 7291.

[125] *See* ''Individuals' Right under HIPAA to Access their Health Information 45 CFR 164.524,'' Office for Civil Rights, U.S. Department of Health and Human Services (Jan. 7, 2016). This guidance is no longer available on OCR's website. OCR will issue updated guidance on the right of access in the future.

[126] 83 FR 64302 (Dec. 14, 2018).

• Promoting parental and caregiver involvement and addressing the opioid crisis and serious mental illness (SMI).

• Modifying the NPP requirements for signatures and recordkeeping.

Specifically, the 2018 RFI sought input on individuals' right of access to their own PHI and the amount of time covered entities should be permitted to respond to such request for access. The 2018 RFI sought input to help determine whether and how to modify the Privacy Rule to address the opioid crisis and SMI and to promote family involvement in the care of loved ones experiencing these health situations. Additionally, the 2018 RFI also sought input on whether the Department should eliminate or modify the NPP signature and recordkeeping requirements associated with distribution of the NPP practices.

7. Ciox Health, LLC v. Azar

In 2020, the U.S. District Court for the District of Columbia, in *Ciox,* rejected modifications made to the Privacy Rule by the 2013 Omnibus Rule that required providers to deliver an individual's PHI to a person designated by the individual regardless of whether the PHI was contained in an electronic health record or the request was to transmit the PHI in an electronic format.[127] The court found that the right of access to direct PHI to a person designated by the individual, established by section 13405(e) of the HITECH Act,[128] did not extend to PHI in locations other than an electronic health record, and did not apply to requests to transmit such PHI in a non-electronic format, such as paper. Further, the court reviewed the 2016 Access Guidance and held that the Department's application of the individual fee limitations to an individual's request that a copy of their PHI be sent to a person designated by the individual was a legislative rule imposed in violation of the Administrative Procedure Act's (APA's) notice and comment requirement. Thus, the court vacated the 2016 Access Guidance insofar as it, without notice and comment rulemaking, extended the individual fee limitations to when an individual requests that a copy of their PHI be sent to a person designated by the individual.

8. 2021 Privacy Rule NPRM

In January 2021, the Department proposed modifications to select provisions of the Privacy Rule to reduce barriers to coordinated care and case management and limit the regulatory burdens of other provisions that do not sufficiently compensate for, or offset, such burdens through privacy protections.[129] As part of the 2021 Privacy Rule NPRM, the Department expressed concern that some regulatory barriers may impede the transformation of the health care system from a system that pays for procedures and services to a system of value-based health care that pays for quality care.[130]

The Department intended for the 2021 Privacy Rule NPRM to support the full scope of care coordination and case management activities to further the Department's goal of achieving value-based health care.[131] Some of the NPRM proposals included clarifying the scope of covered entities' abilities to disclose PHI to social service agencies and eliminating the requirement that a direct treatment provider make a good faith effort to obtain an individual's written acknowledgment of receipt of such provider's NPP. The Department carefully considered the extent to which each proposed modification would impact privacy protections compared to the likely benefit of making PHI more available for coordination of care or case management. The Department also proposed modifications to the individual right of access and fee limitations provisions that were consistent with the *Ciox* opinion.[132]

9. 2024 Part 2 Rule

Following the enactment of the CARES Act,[133] the Department proposed modifications to the Privacy Rule to align certain aspects of 42 CFR part 2 (''Part 2'') with the HIPAA Privacy Rule and the HITECH Act (''2022 Part 2 NPRM'').[134] The proposed modifications included requirements for covered entities and Part 2 programs to provide notice to individuals regarding privacy practices related to Part 2 records, including patients' rights and uses and disclosures that are permitted or required without authorization.[135] While the Department published a final rule adopting modifications to Part 2 in 2024,[136] the Department stated that corresponding modifications to the NPP would be included in a later HIPAA rulemaking.[137]

10. 2024 Privacy Rule

In 2023, the Department proposed modifications to the Privacy Rule (''2023 Privacy Rule NPRM'') to limit uses and disclosures of PHI for certain purposes where the use or disclosure of information is about reproductive health care.[138] Also among the proposed modifications were changes to the requirements for the NPP corresponding to, and consistent with, those proposed for uses and disclosures.[139]

On April 26, 2024, the Department adopted modifications related to uses and disclosures of PHI about reproductive health care and the NPP in the 2024 Privacy Rule.[140] The 2024 Privacy Rule also finalized certain modifications to the NPP provisions that were previously proposed in the 2022 Part 2 NPRM (''Part 2-related NPP provisions''). The Part 2-related NPP provisions were unrelated to the proposals contained in the 2023 Privacy Rule NPRM but were finalized at the same time to minimize burdens on covered entities by allowing them to address all required modifications to their NPPs at one time.[141]

The 2024 Privacy Rule had an effective date of June 25, 2024, and established December 23, 2024, as the compliance date for most of its modifications to the Privacy Rule.[142] The 2024 Privacy Rule established February 16, 2026, as the compliance date for all the NPP modifications.[143]

The 2024 Privacy Rule has generated several legal challenges.[144] On June 18, 2025, the U.S. District Court for the Northern District of Texas in *Carmen Purl* v. *U.S. Department of Health and Human Services* (''*Purl*''), issued an order vacating most of the 2024 Privacy Rule.[145] In fashioning its remedy, the

[127] *Ciox,* 435 F. Supp. 3d 30 (D.D.C. 2020).

[128] 42 U.S.C. 17935(e).

[129] 86 FR 6446 (Jan. 21, 2021).

[130] *Id.* at 6447.

[131] *Id.* at 6449.

[132] *Id.* at 6452. The Department did not appeal the *Ciox* decision.

[133] Public Law 116–136, 134 Stat. 281 (Mar. 27, 2020).

[134] 87 FR 74216 (Dec. 2, 2022). Part 2, also referred to as the Confidentiality of Substance Use Disorder (SUD) Patient Records regulations, protects records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to SUD education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by the Federal government. *See also* 42 U.S.C. 290dd–2.

[135] *Id.* at 74224.

[136] 89 FR 12472 (Feb. 16, 2024).

[137] *Id.* at 12530.

[138] *See* 88 FR 23506 (Apr. 17, 2023).

[139] *Id.* at 23516.

[140] 89 FR 32976 (Apr. 26, 2024).

[141] *Id.*

[142] *Id.* at 32979.

[143] *Id.* at 32976, 33048.

[144] *See* Complaint, *Texas* v. *U.S. Department of Health and Human Services,* No. 5:24-cv-00204 (N.D. Tex. Sept. 4, 2024); Complaint, *Purl* v. *U.S. Department of Health and Human Services,* 787 F. Supp. 3d 284 (N.D. Tex. June 18, 2025); Complaint, *Missouri* v. *U.S. Department of Health and Human Services,* No. 4:25–cv–00077 (E.D. Mo. Jan. 17, 2025); Complaint, *Tennessee* v. *U.S. Department of Health and Human Services,* No. 3:25–cv–00025 (E.D. Tenn. Jan. 17, 2025).

[145] *See Purl,* 787 F. Supp. 3d at 331. An amended judgment, which did not alter the scope of the

court severed the Part 2-related NPP provisions from the rest of the 2024 Privacy Rule and did not vacate them. Thus, the Part 2-related NPP provisions and the compliance date for the provisions not vacated by the court remain in effect.[146]

III. Justification for This Rulemaking

A. An Effective Health Care System Requires That Individuals Have Access to Their Health Information and That Others Are Able To Use and Disclose Health Information About Individuals

To further empower individuals and achieve the promise of Make America Healthy Again, as described in the Executive Summary, the Department must take action to create systemic improvements in health care through the appropriate use and disclosure of health information. By building on the existing policy framework for patient access and interoperability, the Department can drive large-scale adoption of health management and care navigation applications, reduce barriers to information access and exchange, realize the potential of recent innovations in health care that promote better health outcomes, and accelerate progress toward a patient-centric learning health system.[147]

The Department's initiatives today build on the work of the Institute of Medicine[148] (IOM), which, in its 1998 landmark report on the quality of the U.S. health care system, identified six attributes of a high functioning health care system.[149] According to the IOM, health care should be: safe, effective, patient-centered, timely, efficient, and equitable because a system with these attributes would enable individuals to obtain care that is ''safer, more reliable, more responsive, more integrated, and more available.''[150] Not only would individuals benefit, but clinicians and others involved in the provision of health care would also experience increased satisfaction because they would be ''providing care that was more reliable, more responsive to [individuals], and more coordinated.''[151]

As part of its work, the IOM created a set of ten rules to guide the redesign of the health care system. The IOM's rules and report highlighted the importance of ensuring the bi-directional flow of information, not only between clinicians, but also between individuals and clinicians. According to the IOM, the health care system ''must be designed to serve the needs of [individuals], and to ensure that they are fully informed, retain control and participate in care delivery whenever possible, and receive care that is respectful of their values and preferences.''[152] Additionally, ''[it] must facilitate the application of scientific knowledge to practice, and provide clinicians with the tools and supports necessary to deliver evidence-based care consistently and safely.''[153] The IOM report made clear that, without improved communication and transfer of knowledge, health outcomes would suffer.

One of the IOM's recommendations highlighted the connection between high-quality health care, care coordination, and the timely flow of information. Specifically, Recommendation 4 encouraged stakeholders to redesign the health care process to prioritize the individual by ensuring that individuals are able to obtain the care that they need at a time and location that is convenient for them; in a manner that responds to their choices and preferences; and based on shared decision making that is informed by their access to their PHI, clinical knowledge, and evidence-based science. According to the IOM, this prioritization of the individual should occur while also limiting administrative burden and waste.

When taken together, Recommendation 4 and the goal of HIPAA as described by the Department[154] ultimately are the same: a health care system that ensures the best possible health outcomes for individuals in a manner that limits the administrative burdens. To achieve that goal, individuals and people involved in their care need to have prompt access to the individual's PHI in a manner that both protects the individual's privacy and minimizes burdens on individuals, health care providers and other participants in the health care sector, and other stakeholders.

1. Individuals Need To Have Access to Their Own Information for Many Purposes, Including Understanding Their Health Status, Coordinating Their Health Care, and Obtaining Government Benefits

As discussed in greater detail above, the right of individuals to access their PHI has been a central component of the Privacy Rule since its inception. NCVHS stated in its initial 1997 recommendations to the Secretary that, while the exact scope of this right—in particular, potential exceptions—was a subject of debate, committee members found universal agreement with the basic principle of individual access rights.[155] And later that same year, in its recommendations to Congress on the contents of privacy legislation, the Department counseled that individuals should be afforded a certain level of control over their health records. Specifically, the Department recommended that ''[p]atients should be able to see and get copies of their records [. . .]''[156] with limited exceptions.[157] The Department also recommended that such legislation include a limitation on Federal requirements to disclose health information to anyone other than the individual.[158] As we explained, ''[t]he ability to see one's own record is central to effective control of information [. . .].''[159] This recommendation was consistent with recommendations from at least as early as the 1970s to provide individuals with the right to access records about themselves.[160] As explained by the Department:

vacatur, was issued on July 3, 2025. With regard to the modifications to the NPP requirements at 45 CFR 164.520, the court vacated only the provisions that were deemed unlawful, namely 45 CFR 164.520(b)(1)(ii)(F), (G), and (H). The remaining modifications to the NPP requirements—specifically, the Part 2-related NPP provisions—were undisturbed and remain in effect. As a result of the court order, the Department cannot and is not enforcing the vacated provisions.

[146] *See Purl,* 787 F. Supp. 3d at 331.

[147] 90 FR 21034, 21036 (May 16, 2025).

[148] The IOM was renamed the National Academy of Medicine on July 1, 2015. *See* Press Release, ''Institute of Medicine to Become National Academy of Medicine,'' Institute of Medicine (Apr. 28, 2015), *https://web.archive.org/web/20190905015356/http://www.nationalacademies.org/hmd/Global/News%20Announcements/IOM-to-become-NAM-Press-Release.aspx.*

[149] ''Crossing the Quality Chasm: A New Health System for the 21st Century,'' Institute of Medicine (US) Committee on Quality of Health Care in America, at Executive Summary (2001), *https://www.ncbi.nlm.nih.gov/books/NBK222271/.*

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id.*

[154] *See supra* Sec. II.A.1.

[155] Letter from NCVHS Chair Don E. Detmer to HHS Secretary Donna E. Shalala, at Patient Access and Amendment of Health Information (June 27, 1997) (forwarding NCVHS' recommendations), *https://web.archive.org/web/20240228021816/https://ncvhs.hhs.gov/rrp/june-27-1997-letter-to-the-secretary-with-recommendations-on-health-privacy-and-confidentiality/.*

[156] *See* ''Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996,'' Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services, Section I.G. (Sept. 10, 1997), *https://aspe.hhs.gov/reports/confidentiality-individually-identifiable-health-information.*

[157] *Id.* at II.C.2.

[158] *Id.* at I.D.

[159] *Id.* at II.C.2.

[160] *Id.* (citing recommendations made by the Secretary's Advisory Committee on Automated

Continued

[T]he right recommended here is not simply a right to fair procedure in an administrative transaction or criminal or civil legal action (which may be provided in any case by other law); it is a freestanding fair information practice right to see one's record at a time of one's choosing regardless of actual use in a proceeding or for decision making. It should be available unless there is a danger that patient access would impede the investigation.[161]

While Congress did not enact specific legislation on health information privacy, the Department's recommendations served as the underpinnings for its original Privacy Rule. Thus, the Department's recommendations to Congress, and the privacy considerations undergirding them, are instructive here.

Providing individuals with access to their health information is not only a fair information practice; it also is essential for the individual's ability to engage in shared decision making,[162] a fundamental component of an improved health care system. Shared decision making is ''a collaborative process in which [individuals] and clinicians work together to make healthcare decisions informed by evidence, the care team's knowledge and experience, and the [individual's] values, goals, preferences, and circumstances. Families and caregivers also play an important role in [shared decision making].'' [163] Ultimately, this means that, ''to effectively manage their health, individuals need to be able to access and use their health information when, where, and how they want, including sending it to the people and tools helping them to become or stay healthy—neighbors, friends, relatives, health care providers who are treating or consulting with the individual, or even third-party software tools used for self-management.'' [164] Thus, it is critical for individuals to be able to obtain access to their information promptly and efficiently.

Not only do individuals need access to their PHI, but research shows that individuals generally want to be able to access it and to have some level of control over the PHI that others are able to access.[165] According to the qualitative study of individuals with diabetes who engage with the U.S. Department of Veterans Affairs (VA) patient portal, ''having access to the patient portal puts control over health information into the hands of patients. When patients want to share information between providers, patients can send information themselves.'' [166] The evolution of the VA's capabilities for providing individuals with electronic access to their PHI also illustrates how technology has increasingly enabled individuals to obtain and use their health information. For example, the study describes how VA's My HealtheVet portal [167] and Blue Button [168] functionality enable individuals to access clinical information electronically, and how individuals use that information to support their care, including for care coordination between VA and non-VA health care providers.[169] Thus, allowing individuals to direct a covered entity to provide access to that individual's PHI to a person designated by the individual, for example, by using the functionalities of a patient or health plan member portal, enables coordination among people involved in the individual's care, including among health care providers. Sharing PHI in this manner can reduce duplicate and unnecessary testing, saving time and health care resources.[170]

Research also demonstrates that individuals are more likely to consent to disclosing their health information electronically through health information exchanges (HIEs) [171] when they have greater control over what health information is shared and with whom.[172] When individuals can exercise more control over disclosing their health information, the privacy concerns associated with requests for individuals to share their information are reduced and trust in health care professionals increases, which, in turn, results in higher consent rates.[173] Thus, providing individuals with greater control over who has access to their information, including the ability to direct copies of their information to another person, is likely to increase their willingness to agree to (or authorize, where required) disclosures of that information for other purposes, such as clinical research. We believe that the Department can foster this increased trust and willingness and the attendant benefits for health care and public health by improving individuals' ability to obtain, and direct the disclosure of, their information in a manner that is timely, efficient, and privacy protective.

2. Persons Involved in Caring for Individuals Need To Use Their PHI

Individuals are not alone in their need to use their PHI. Persons involved in caring for individuals—health care providers, family members, caregivers, community-based organizations, and others—also may need to obtain individuals' PHI to facilitate care coordination and case management and enable such individuals to obtain necessary health care and related services. Some of these persons may be covered entities, but others may not.

a. Improving Cooperation Is a Common Element in Existing Definitions of Care Coordination and Case Management

As we explained in the 2021 Privacy Rule NPRM, neither care coordination nor case management has a precise, commonly agreed upon definition. However, both terms have been interpreted broadly to refer to activities that are aimed at promoting cooperation among persons involved in caring for an individual, such as family members, caregivers, and community-based organizations, with the goal of ensuring the best possible health outcomes for the individual. For example, the Department's Office of Inspector General (OIG) defines ''coordination and management of care'' as the ''deliberate organization of patient care activities and sharing of information between two

Personal Data Systems and the Privacy Protection Study Commission in 1973 and 1977, respectively).

[161] *Id.*

[162] ''About Shared Decision Making,'' Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services (May 2023), *https://www.ahrq.gov/sdm/about/index.html.*

[163] *Id.*

[164] Karen B. DeSalvo, et al., ''When and Where You Need It Most: Your Rights to Access and Transmit Your Health Information,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Jan. 11, 2016), *https://www.healthit.gov/buzz-blog/privacy-and-security/your-rights-to-access-and-transmit-your-health-information.*

[165] Kelly Caine, et al., ''Designing a Patient-Centered User Interface for Access Decisions about EHR Data: Implications from Patient Interviews,'' Journal of General Internal Medicine, p. 7–16 (Dec. 6, 2014), *https://rdcu.be/eCVvN.*

[166] Maureen T. Stewart, et al., ''The Promise of Patient Portals for Individuals Living with Chronic Illness: Qualitative Study Identifying Pathways of Patient Engagement,'' Journal of Medical internet Research (July 2020), *https://www.jmir.org/2020/7/e17744/PDF.*

[167] ''Manage your health care with My HealtheVet,'' U.S. Department of Veterans Affairs, *https://www.va.gov/health-care/manage-health/.*

[168] ''Blue Button Resources: Center to Improve Veteran Involvement in Care (CIVIC),'' U.S. Department of Veterans Affairs, *https://www.portlandcoin.research.va.gov/BlueButton.asp.*

[169] ''The Promise of Patient Portals for Individuals Living with Chronic Illness: Qualitative Study Identifying Pathways of Patient Engagement,'' *supra* note 166.

[170] *Id.*

[171] An HIE is a type of health information organization. *See* 45 CFR 160.103 (definition of ''Business associate'' at (3)(i)). *See also* 45 CFR 171.102 (definition of ''Health information network or health information exchange'').

[172] Mohamed Adelhamid, ''Greater patient health information control to improve the sustainability of health information exchanges,'' Journal of Biomedical Informatics, p. 150–58 (July 2018), *https://www.sciencedirect.com/science/article/pii/S1532046418301084.*

[173] *Id.*

or more VBE [value-based enterprise] participants, one or more VBE participants and the VBE, or one or more VBE participants and patients, that is designed to achieve safer, more effective, or more efficient care to improve the health outcomes of the target patient population.'' [174]

CMS has described care coordination and management as ''the foundation of a value-based health care delivery system'' [175] and as including a range of activities that link individuals to services and improve communication flow.[176] In its 2014 guidance addressing a particular Medicaid benefit, CMS explained that the various definitions of this term share three key concepts:

- Comprehensive coordination of all services, including services delivered by systems other than the health system.
- Patient-centered coordination that is designed to meet the needs of the patient.
- Access and follow-up, which is described as ensuring the delivery of appropriate services and information flow among providers and back to the primary care provider.[177]

In a 2019 fact sheet on the Medicaid program's health home benefit, CMS described the following six mandatory core services to promote access to and coordination of care:

- Comprehensive care management.
- Care coordination.
- Health promotion.
- Comprehensive transitional care and follow-up.
- Individual and family support.
- Referral to community and social services.[178]

Additionally, the regulations that govern state Medicaid plans include a definition of ''case management services'' that is similar in meaning.[179] In the context of HCBS waivers, CMS has explained that case management usually entails (but is not limited to) conducting the following functions:

- Evaluation and/or re-evaluation of level of care.
- Assessment and/or reassessment of the need for waiver services.
- Development and/or review of the service plan.
- Coordination of multiple services and/or among multiple providers.
- Linking waiver participants to other Federal, state, and local programs.
- Monitoring the implementation of the service plan and participant health and welfare.
- Addressing problems in service provision.
- Monitoring compliance with HCBS settings criteria.
- Reporting, and following-up on, critical incidents.
- Responding to participant crises.
- For waivers with cost or service duration limits, monitoring to detect and resolve situations when the needs of an individual might exceed the limit(s) to ensure health and welfare of waiver participants.[180]

The Department's Agency for Healthcare Research and Quality (AHRQ) describes care coordination as ''a proactive approach to bringing together care professionals and providers to meet the needs of service users to ensure that they receive integrated, person-focused care across various settings,'' [181] that is a ''deliberate organization of patient care activities between two or more participants (including the patient) involved in a patient's care to facilitate the appropriate delivery of health care services.'' [182] It explains that ''[o]rganizing care involves the marshalling of personnel and other resources needed to carry out all required patient care activities and is often managed by the exchange of information among participants responsible for different aspects of care.'' [183] AHRQ describes a broad approach to care coordination as involving commonly used practices to improve health care delivery, including teamwork, care management, medication management, health IT, and patient-selected health care homes.[184] AHRQ also describes specific activities to help achieve care coordination, such as creating a proactive care plan, patient monitoring and follow-up, supporting patient self-management goals, and linking to community resources.[185]

Another definition comes from the National Quality Forum,[186] an organization that works to improve health care outcomes, safety, and affordability through consensus on quality measurement and improvement standards and practices. It defines ''care coordination'' as ''the deliberate synchronization of activities and information to improve health outcomes to ensure patients' and families' needs and preferences for healthcare and community services are met over the course of their treatment and care.'' [187]

Definitions of ''case management'' are equally varied. The Case Management Society of America defines case management as ''a collaborative process of assessment, planning, facilitation, care coordination, evaluation, and advocacy for options and services to meet an individual's and family's comprehensive health needs through communication and available resources to promote patient safety, quality of care, and cost-effective outcomes.'' [188] The American Case Management Association describes case management as ''professional and collaborative, occurring in a variety of settings where medical care, mental health care, and social supports are delivered. Services are facilitated by diverse disciplines in conjunction with the care recipient and

[174] 42 CFR 1001.952(ee)(14)(i); *see* 85 FR 77684, 77721 (Dec. 2, 2020). Value-based care replaces traditional fee-for-service payments that focus on the volume of services, and instead rewards health care providers who deliver higher quality care, better population health, and lower health care costs. *See* ''Value-Based Care,'' sec. 6 of the Health IT Playbook, Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (May 20, 2025), *https://playbook.healthit.gov/playbook/value-based-care/.*

[175] 85 FR 77492, 77498 (Dec. 2, 2020).

[176] ''Making Connections: Strengthening Care Coordination in the Medicaid Benefit for Children & Adolescents,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services, p. 3 (Sept. 2014), *https://www.medicaid.gov/medicaid/benefits/downloads/epsdt-care-coordination-strategy-guide.pdf.*

[177] *Id.*

[178] ''Medicaid Health Homes: An Overview,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Jan. 2019), *https://www.chcs.org/media/HH-Fact-sheet-January-2019.pdf.*

[179] *See* 42 CFR 440.169.

[180] *See* ''CMS Waiver Applications,'' (The 1915(c) Application and Accompanying Materials—Instructions, Technical Guide and Review Criteria, Version 3.7 HCBS Waiver Application), Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (last accessed Oct. 26, 2026), *https://wms-mmdl.cms.gov/WMS/faces/portal.jsp.*

[181] ''Updating the Framework for the Agency for Healthcare Research and Quality's National Healthcare Quality and Disparities Report,'' Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services, p. 30 (July 2025), *https://effectivehealthcare.ahrq.gov/sites/default/files/related_files/updating-framework-qdr-technical-brief-50.pdf.*

[182] ''Care Coordination Measures Atlas,'' Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services, p. 6 (updated June 2014), *https://www.ahrq.gov/sites/default/files/publications/files/ccm_atlas.pdf* (citing Kathryn M. McDonald, et al., ''Closing the Quality Gap: A Critical Analysis of Quality Improvement Strategies: Volume 7—Care Coordination, Technical Reviews,'' No. 9.7, conducted for AHRQ (2007)).

[183] *Id.*

[184] ''Care Coordination Measures Atlas,'' *supra* note 182.

[185] *Id.*

[186] *See* ''About Us,'' National Quality Forum (last accessed Feb. 26, 2026), *https://www.qualityforum.org/en-us/about-us.*

[187] ''Leveraging Electronic Health Record (EHR)-Sourced Measures to Improve Care Communication and Coordination,'' National Quality Forum, p. 5 (Sept. 19, 2022), *https://digitalassets.jointcommission.org/api/public/content/c0a04822de574f76995e60d1c3afcfae?v=4220bbc8.*

[188] ''The Impact of Case Management on the Healthcare System,'' Case Management Society of America (2024), *https://cmsa.org/wp-content/uploads/2024/05/FINAL-The-Impact-of-Case-Management-on-the-Healthcare-System-.pdf.*

their support system.'' Case management includes help with navigating ''complex systems to achieve mutual goals, advocate for those they serve, and recognize personal dignity, autonomy, and the right to self-determination.'' [189]

Despite the variation in definitions, the goal of care coordination and case management is generally the same: to improve health outcomes for individuals.

b. Care Coordination and Case Management Improve Health Outcomes and Decrease the Cost of Care

While the definitions of care coordination and case management may vary, they consistently recognize that access to an individual's PHI, gathered from disparate sources, is integral to improving health outcomes for individuals. Research on care coordination and case management generally demonstrates the benefits of exchanging PHI for care coordination and case management for individuals and for the health care system. A 2026 qualitative study based on interviews with twenty hospital and health care system leaders found that current HIEs represent an improvement over alternative means of sharing information between settings of care.[190] According to a 2019 literature review, the annual costs associated with the failure of care coordination (*i.e.,* unnecessary admissions or avoidable complications and readmissions) ranged from $27.2 billion to $78.2 billion, while the annual cost savings associated with five different care coordination interventions, including the use of a HIE, ranged from $29.6 billion to $38.2 billion.[191] These figures do not include costs associated with unnecessary testing or procedures, nor do they include savings from decreases resulting from related interventions.[192] A 2019 study of data collected from 2011 to 2014 examined the effects of electronic data exchange by hospitals in Florida with other health care providers on health outcomes for individuals who experienced an acute myocardial infarction and found that hospitals that participated in HIEs performed significantly better than hospitals that did not participate.[193] The study showed a greater decrease in 30-day all-cause readmissions for participating hospitals than non-participating hospitals and sustained decreases for readmissions at 45 days and 60 days.[194] The study also found an association between HIE participation, readmission reduction, and increased intensity in the inpatient treatment received by individuals who experienced an acute myocardial infarction, which, according to the study's authors, suggested that HIE participation may play a role in determining the cost trade-offs of inpatient care as opposed to readmission.[195] This further suggests that electronically exchanging information may have helped participating hospitals evaluate the most appropriate and cost-effective health care for each individual during their initial admission. As another example, a 2021 study found that there was a significant association between the use of an HIE by primary care physicians to obtain the PHI of individuals recently released from the hospital and visits to emergency departments and rehospitalizations.[196] In such cases, the individual's likelihood of visiting the emergency department was reduced by 53 percent, while the risk of rehospitalization was reduced by 61 percent.[197] Additionally, if the individual was rehospitalized, the median length of time between the hospital visits more than doubled, increasing from 99 days to 238 days.[198] A 2023 study of 2018 data found that Medicare beneficiaries with Alzheimer's disease were 23 percent less likely to die during a readmission where the readmission was fragmented [199] and the associated hospitals shared an HIE as compared with fragmented readmissions to hospitals that did not share an HIE.[200] Additionally, beneficiaries who experienced fragmented readmissions where the hospitals shared an HIE were more likely to be discharged home with home health, as opposed to a skilled nursing facility (SNF), regardless of whether they had Alzheimer's disease.[201] And in another example, researchers found that individuals enrolled in a certain Medicaid section 1115 demonstration project generally experienced improved health outcomes when participating sites implemented, among other things, health IT that enabled the electronic exchange of PHI.[202] Not only did health outcomes improve, but the cost of care decreased significantly.[203] The specific health IT adopted by the sites varied, including EHRs,[204] case management platforms, cloud-based storage, and

[189] ''Definition of Case Management,'' American Case Management Association (last accessed Jan. 13, 2026), *https://www.acmaweb.org/section.aspx?sID=4.*

[190] *See* Sara D. Turbow, et al., ''Better than nothing, far from perfect: hospital and healthcare system leaders' perspectives on health information exchanges,'' JAMIA Open, Volume 9, Issue 1, p. ooaf178 (Jan. 5, 2026), *https://pmc.ncbi.nlm.nih.gov/articles/PMC12794009/.*

[191] William H. Shrank, et al., ''Waste in the US Health Care System: Estimated Costs and Potential for Savings,'' JAMA, p. 1505 (Oct. 15, 2019), *https://vbidcenter.org/wp-content/uploads/2021/10/jama_shrank_2019_sc_190005.pdf* (Authors classified the interventions into the following categories: (1) emergency department-based strategies; (2) care coordination within accountable care organizations; (3) HIEs; (4) transitional care programs (focused on hospital-to-home transitions); and (5) effective care management for medically complex patients.).

[192] *Id.* (The literature review grouped articles that addressed costs of waste from overtreatment with articles that addressed the costs of waste from low-value care, rather than with articles that addressed ''failure of care coordination.'').

[193] Min Chen, et al., ''Does Health Information Exchange Improve Patient Outcomes? Empirical Evidence From Florida Hospitals,'' Health Affairs, p. 197–204 (Feb. 2019), *https://www.healthaffairs.org/doi/epdf/10.1377/hlthaff.2018.05447.*

[194] *Id.* at 201.

[195] *Id.* at 202.

[196] Chantel Sloan-Aagard, et al., ''The Impact of Community Health Information Exchange Usage on Time to Reutilization of Hospital Services,'' Annals of Family Medicine, p. 19–26 (Jan./Feb. 2023), *https://www.annfammed.org/content/annalsfm/21/1/19.full.pdf.*

[197] *Id.*

[198] *Id.*

[199] A fragmented readmission occurs when an individual's admission and readmission are to different hospitals. *See* Sara D. Turbow, et al., ''Association of Fragmented Readmissions and Electronic Information Sharing With Discharge Destination Among Older Adults,'' JAMA Network Open, p. 2 (May 16, 2023), *https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804993.*

[200] *Id.*

[201] *Id.* (Discharges to home with home health cost less than discharges to SNFs and are associated with less risk for subsequent readmission.).

[202] ''Final Evaluation of California's Whole Person Care (WPC) Program,'' UCLA Center for Health Policy Research (Dec. 2022), *https://healthpolicy.ucla.edu/sites/default/files/2024-03/whole-person-care-final-evaluation-report-approved-with-signature_03_11_24.pdf.* In 2015, CMS approved a sec. 1115 demonstration for California's Medicaid program. The demonstration, conducted from 2016 through 2021, aimed to improve access, quality of care, and health outcomes for Medicaid enrollees who are high-risk and high utilizers of health care services with complex care needs to improve their overall health and well-being. While the study did not define ''high risk,'' participating sites were required to target one or more of the following six populations: (1) high utilizers of avoidable emergency department, hospitals, or nursing facilities (high utilizers); (2) individuals with two or more chronic physical conditions (chronic physical conditions); (3) individuals with severe mental illness and/or substance use disorders (SMI/SUD); (4) individuals experiencing homelessness (homeless); (5) individuals at-risk-of-homelessness; and (6) individuals recently released from institutions, including jail or prison (justice-involved). *Id.* at 27. Among the requirements for participant sites was that they implement health IT tools to enable the electronic exchange of PHI. *Id.* at 82.

[203] *Id.* at 230–44.

[204] For purposes of this final rule, we use the term ''EHR'' to refer to the commonly understood meaning of the term, *i.e.,* a system that stores electronic health information across different health care settings. We use the term ''electronic health record'' when referring to the term defined in the HITECH Act and this final rule. *See* 42 U.S.C. 17921(5) (definition of ''Electronic health record''); 45 CFR 164.501 (definition of ''Electronic health record'').

centralized repositories (*e.g.,* HIEs), but overall, the participant sites reported improvements in the selected health outcomes measured.[205] Accordingly, ensuring that persons involved in caring for individuals have access to the individuals' PHI is a critical component for enabling care coordination and case management.

A study also identified the ability of individuals to directly access PHI as an opportunity for improved program evaluation.[206] A 2019 study of the ties between entities in a network of health care organizations and social services agencies demonstrated the importance of integration between these organizations to network performance. According to study authors, ''more cohesive interorganizational networks of health care and social service organizations are associated with lower levels of potentially avoidable health care use and spending among beneficiaries.'' [207] The authors of a review of the effectiveness of initiatives to address health-related factors that influence health outcomes concluded that there is a ''need for policy incentives to more effectively integrate [such] data into EHR systems and foster stronger community partnerships to ensure broader, sustainable impact.'' [208] Thus, to improve the efficiency and effectiveness of the health care system, covered entities must be able to partner with and disclose PHI to social services and community-based organizations that are working to address health-related factors for care coordination and case management.

As then-HHS Deputy Secretary Eric D. Hargan explained before the Brookings Institution on January 30, 2019, care coordination is a necessary component of achieving value-based care:

> One of [the components of value-based care] is coordinated care and the drive to coordinated care provokes some obvious questions that point towards the need for broad-based regulatory reform in this area. Some of the questions and challenges that we got along the way [. . .] [include]: how can we expect physicians to act as navigators of the health system while also holding them accountable if their decision-making is hamstrung by outdated regulations; or how can we expect providers to get on board with payments based on outcomes if we're not willing to give them the freedom to experiment and coordinate with one another [. . .] how can we really make major steps in preventing and curing disease without also rethinking how regulations [. . .] could impede patients and providers working together in creative arrangements [. . .] ? [209]

Former Secretary Azar later praised the advancement of coordinated care with the publication of final rules on interoperability, access to health information, and certification of electronic health record technology.[210] The Secretary stated, ''[t]hese rules are the start of a new chapter in how patients experience American healthcare, opening up countless new opportunities for them to improve their own health, find the providers that meet their needs, and drive quality through greater coordination.'' [211] And, when announcing the publication of a final rule modifying regulations on the confidentiality of substance use disorder (SUD) treatment records to expand care coordination and quality, Secretary Azar explained, ''[t]his reform will help make it easier for Americans to discuss substance use disorders with their doctors, seek treatment, and find the road to recovery.'' [212]

More recently, Secretary Robert F. Kennedy Jr. noted, in his announcement of expanded enforcement of the information blocking regulations, ''[w]hen a patient visits an emergency room, doctors need to access that patient's medical history. They need to know about medications, blood types, allergies, and prior diagnoses. Otherwise, how can they provide the right care? Information technology should make this easy.'' [213] And at a recent U.S. Senate hearing, the National Coordinator for Health Information Technology, Dr. Thomas Keane explained:

> No patient should be treated like a stranger at their next health care encounter simply because their records did not follow them [. . .]. Access to data will [. . .] help inform providers' clinical decision making which can lead to improved care and patient safety [. . .]. In some cases, missing information is not just frustrating, it is dangerous. A patient with a known drug allergy who shows up at a new facility without their records may be prescribed improper medication that could have been avoided if their history were available.[214]

Thus, it is essential that HIPAA not only permit, but also encourage, the coordination of care where appropriate.

B. The Health Care Environment Has Changed Since the Privacy Rule's Right of Access and Care Coordination Provisions Were Last Revised

Over the course of the last decade, the U.S. health care system has changed significantly. The Department has modified the Privacy Rule a few times in the intervening years, but none of those modifications have addressed the reasons for the shift towards the electronic exchange of health information. While the Privacy Rule is technology neutral, the Department must consider the causes of the change in the U.S. health care system, such as the implementation of laws, spread of technology, and the breadth of research that encourage care coordination, to determine how the changes interact with the Privacy Rule and their implications for the goals of HIPAA.

---

[205] *See* ''Final Evaluation of California's Whole Person Care (WPC) Program,'' *supra* note 202, at 85–87.

[206] Jessica M. Sautter, et al., ''Health outcomes reported by healthcare providers and clients of a community-based medically tailored meal program,'' BMC Nutrition, p. 10 (Nov. 4, 2024), *https://rdcu.be/e1oRR.*

[207] Amanda L. Brewster, et al., ''Collaboration in Health Care and Social Service Networks for Older Adults: Association with Health Care Utilization Measures,'' Medical Care, p. 331 (May 2019), *https://www.ovid.com/jnls/lww-medicalcare/pdf/10.1097/mlr.0000000000001097~collaboration-in-health-care-and-social-service-networks-for.*

[208] Pavani Rangachari, et al., ''Impact of hospital and health system initiatives to address Social Determinants of Health (SDOH) in the United States: a scoping review of the peer-reviewed literature,'' BMC Health Services Research (Mar. 5, 2025), *https://rdcu.be/e1m3E; see also* ''Better than nothing, far from perfect: hospital and healthcare system leaders' perspectives on health information exchanges,'' *supra* note 190 (finding that participating in a value-based model influenced institutional policies around information exchange—participants from value-based care organizations reflected that they have more incentives, and in some cases, requirements, to use the HIE system to perform population health tasks and to ensure that tests are not being duplicated).

[209] ''Reforming Stark/Anti-Kickback Policies,'' Brookings Institution, p. 7 (Jan. 30, 2019), *https://www.brookings.edu/wp-content/uploads/2019/02/es_20190130_stark_reform_transcript.pdf.*

[210] *See generally* 85 FR 25510 (May 1, 2020); 85 FR 25632 (May 1, 2020).

[211] Press Release, ''HHS Finalizes Historic Rules to Provide Patients More Control of Their Health Data,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Mar. 9, 2020), *https://www.cms.gov/newsroom/press-releases/hhs-finalizes-historic-rules-provide-patients-more-control-their-health-data.*

[212] Press Release, ''Health Privacy Rule 42 CFR part 2 is Revised, Modernizing Care Coordination for Americans Seeking Treatment for Substance Use Disorders,'' Substance Abuse and Mental Health Services Administration, U.S. Department of Health and Human Services (July 13, 2020), *https://www.samhsa.gov/newsroom/press-announcements/202007131115.*

[213] ''Secretary Kennedy Announces Expanded Enforcement of Health Care Information Blocking Regulations'' at 01:47, U.S. Department of Health and Human Services, YouTube (Sept. 3, 2025), *https://www.youtube.com/watch?v=u1N7bX0cgvI.*

[214] Testimony of Thomas Keane, M.D., *supra* note 6.

1. Newer Laws Build on HIPAA's Goal of Developing a Nationwide Information Network and Promote the Electronic Exchange of Health Information

a. Congress Has Enacted Legislation To Improve Health Outcomes Through Care Coordination Supported by the Electronic Exchange of Health Information and Individual Access to Health Information

Since the Privacy Rule's provisions that address the individual's right of access and care coordination were last revised, Congress has made significant changes in Federal law expressly to provide individuals and others with increased electronic access to PHI with the goal of improving health outcomes through various activities, including care coordination. Since 2013, Congress has enacted several pieces of legislation aimed at furthering this goal.[215] For example, in April 2015, Congress passed the Medicare Access and CHIP Reauthorization Act of 2015 [216] (MACRA), which declares the widespread exchange of health information through interoperable certified EHR technology (CEHRT) nationwide to be a national objective.[217] MACRA's definition of ''interoperability'' focuses on using health IT to exchange health information for coordinated care and improved health outcomes.[218] The statute also includes provisions to prevent the blocking of information sharing [219] and establish metrics for determining whether widespread interoperability [220] had been achieved.[221] As part of MACRA, Congress required the Secretary to establish a methodology for paying certain health care providers based on their performance.[222] Congress further directed that as part of this methodology, the Secretary was to establish and adopt performance measures on which incentive payments for the health care providers would be based, including measures of care coordination.[223] Additionally, MACRA expanded the ability of certain entities to use Medicare data for the purpose of improving the quality of patient care.[224] Congress also codified certain existing CMS initiatives on chronic care management services that enabled additional categories of health care professionals to bill for chronic care management services and requires the Secretary to conduct an education and outreach campaign to health care professionals and beneficiaries about these benefits.[225]

The following year, Congress enacted the Cures Act,[226] which encouraged certain persons, including covered entities and their business associates, to provide individuals with electronic access to their PHI and enable covered entities to more easily exchange ePHI.[227] For example, among the Cures Act's provisions were directions to the National Coordinator for Health Information Technology (''National Coordinator'') and OCR to jointly promote patient access to PHI in a form and manner that is both convenient to the individual and not burdensome for the involved health care provider.[228] The Cures Act also included directions to the National Coordinator and OCR to assist individuals and health care providers in understanding the right of access, including best practices for requesting their PHI in a computable format, such as using patient portals or applications and common cases when a health care provider is permitted to exchange and provide access to PHI.[229] As another example, Congress directed the Secretary to promote policies that ensure that a patient's electronic health information [230] (EHI) is accessible to the patient and their designee(s) in a manner that facilitates communication with the patient's health care providers and others, including researchers, consistent with the patient's consent.[231] The Cures Act also required the Department to issue guidance clarifying the permitted uses or disclosures of PHI for purposes of communicating with a patient's family member, caregiver, or other individual, to the extent that such family member, caregiver, or individual is involved in caring for the patient.[232]

Even more recently, Congress enacted the CARES Act.[233] The CARES Act enabled and encouraged care coordination and case management through targeted grant reauthorizations, regulatory requirements to facilitate information sharing, increased provider flexibility, the provision of additional funding for certain at-risk populations, and telehealth expansion. Among other things, Congress directed the Secretary to establish a grant program for the quality improvement activities of small health care providers and specifically permitted the grants to be used for activities related to increasing care coordination, enhancing chronic disease management, and improving patient health outcomes.[234] The CARES Act allocated almost $1 billion to the Administration for Community Living for services that include case management for older adults and individuals with disabilities.[235] Additionally, Congress directed the Secretary to provide grants for programs designed to support the training of health professionals in geriatrics with

[215] *See* Nora Wells, ''Digital Health Information Interoperability: Background and Selected Policy Considerations,'' Congressional Research Service, R49436 (Sept. 29, 2026) (discussing the Department's efforts to further interoperability in support of a learning health system).

[216] Public Law 114–10, 129 Stat. 87 (Apr. 16, 2015).

[217] Sec. 106(b)(1)(A) of Public Law 114–10, 129 Stat. 138 (Apr. 16, 2015).

[218] Sec. 106(b)(1)(B)(ii) of Public Law 114–10, 129 Stat. 139 (Apr. 16, 2015).

[219] Sec. 106(b)(2) of Public Law 114–10, 129 Stat. 139 (Apr. 16, 2015).

[220] Sec. 106(b)(1)(B)(i) of Public Law 114–10, 129 Stat. 139 (Apr. 16, 2015).

[221] Sec. 106(b)(1)(C) of Public Law 114–10, 129 Stat. 139 (Apr. 16, 2015).

[222] *See* sec. 101 of Public Law 114–10, 129 Stat. 89–128 (Apr. 16, 2015).

[223] *Id.*

[224] *See* sec. 105(a) of Public Law 114–10, 129 Stat. 133 (Apr. 16, 2015).

[225] *See* sec. 103(a) of Public Law 114–10, 129 Stat. 87, 131 (Apr. 16, 2015) (codified at 42 U.S.C. 1395w–4(b)).

[226] Public Law 114–255, 130 Stat. 1033 (Dec. 13, 2016).

[227] Among other things, the Cures Act directed the Secretary to use existing authorities to encourage partnerships between HIEs/health information networks (HINs) and health care providers, health plans, and other appropriate entities with the goal of enabling individuals to access their ePHI in a single, longitudinal format that is easy to understand, secure, and automatically updatable. It also directed the Secretary, in coordination with OCR to educate providers on how to leverage HIEs/HINs to provide individuals with access to their ePHI, clarify misunderstandings by health care providers about the use of HIEs/HINs for individual access, and, to the extent practicable, educate providers about HIEs/HINs that employ capabilities that enable individual access to ePHI. *See* sec. 4006(a) of Public Law 114–255, 130 Stat. 1181 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–19(c)).

[228] *See* sec. 4006(d) of Public Law 114–225, 130 Stat. 1182 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–19(d)).

[229] *See* sec. 4006(e)(1)(B) of Public Law 114–225, 130 Stat. 1182 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–19(e)(1)(B)).

[230] While the statute does not define ''electronic health information,'' for purposes of the information blocking regulations, ONC has defined it to mean, with reference to HIPAA Rules, ePHI that is subject to the right of access under 45 CFR 164.524. *See* 45 CFR 171.102.

[231] *See* sec. 4006(e) of Public Law 114–225, 130 Stat. 1182 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–19(e)).

[232] *See* sec. 11003(b)(3)(A) of Public Law 114–225, 130 Stat. 1271 (Dec. 13, 2016) (codified at 42 U.S.C. 1320d–2 note).

[233] Public Law 116–136, 134 Stat. 281 (Mar. 27, 2020).

[234] *See s*ec. 3213(4)(A) of Public Law 116–136, 134 Stat. 372 (Mar. 27, 2020) (codified at 42 U.S.C. 254c(g)(1)).

[235] *See* Public Law 116–136, 134 Stat. 559; *see also* Press Release, ''ACL Announces Nearly $1 Billion in CARES Act Grants to Support Older Adults and People with Disabilities in the Community During the COVID–19 Emergency,'' Administration for Community Living, U.S. Department of Health and Human Services (Apr. 21, 2020), *https://acl.gov/news-and-events/announcements/acl-announces-nearly-1-billion-cares-act-grants-support-older-adults.*

an emphasis on patient and family engagement, the integration of geriatrics with primary care and other appropriate specialties, and collaboration with community partners to address gaps in health care for older adults.[236] Congress also used the CARES Act to support the electronic exchange of health information by encouraging providers of SUD treatment to access state-based prescription drug monitoring programs [237] (PDMPs) when clinically appropriate.[238]

b. Using Its Statutory Authority, the Department Has Published Regulations That Require or Encourage Covered Entities and Business Associates To Adopt Technology That Enables the Electronic Exchange of Health Information, Individual Access to Health Information, and Care Coordination

To implement the requirements of the HITECH Act and other laws, the Department has published numerous rulemakings that also serve to further the electronic exchange of health information. For example, the Medicare and Medicaid EHR Incentive Programs were established in 2011 to incentivize the adoption and meaningful use of CEHRT by eligible hospitals, critical access hospitals (CAHs), and eligible professionals (''eligible health care providers'').[239] Stage 1 of the programs focused on a few specific goals, including electronically capturing health information in a structured format; using that information to track key clinical conditions and communicating that information for care coordination purposes; and using CEHRT to engage patients and families.[240] The goals of the programs' Stage 2 included encouraging the use of health IT for continuous quality improvement at the point of care and the exchange of information in the most structured format possible.[241] Stages 2 and 3 included increasingly robust expectations for health information exchange to support the goal that information follows the patient.[242] Stage 3 generally focused on the advanced use of EHR technology to promote improved patient outcomes and health information exchange and established a clear vision for how participation in the programs supported CMS' long-term system reform goals and the future use of EHRs across a multitude of health care providers.[243]

The Merit-based Incentive Payment System (MIPS), a part of the Quality Payment Program (QPP), replaced the Medicare EHR Incentive Program for eligible clinicians in 2017.[244] The goals of the QPP currently include the following:

- Advancing the sharing of health care information between allied providers and patients.
- Improving the care received by Medicare beneficiaries.
- Educating, engaging, and empowering patients as members of their care team.[245]

As part of the QPP, MIPS eligible clinicians must demonstrate that they are engaging in certain activities focused on promoting interoperability and engaging in care coordination.[246]

Additionally, in May 2020, CMS published the Interoperability and Patient Access Final Rule, designed to advance interoperability and patient access to health information.[247] This rule, part of the MyHealthEData initiative launched during the first Trump Administration,[248] focused on empowering patients to take charge of their own health care by requiring certain health plans that CMS regulates to provide individuals with certain information through an application programming interface [249] (API) (''Patient Access API'') based on specified electronic transaction standards, if requested by the individual.[250] To further advance the electronic exchange of information that supports effective transitions of care, the rule also requires that certain health care providers send event notifications at specified times to other providers engaged in the individual's care who need the information for treatment, care coordination, or quality improvement purposes.[251]

Building on this rule, in 2024, CMS published the Interoperability and Prior Authorization Final Rule,[252] which required that certain health plans do all of the following by the applicable compliance dates, generally beginning January 1, 2027 (or, for Medicaid and CHIP managed care plans, the rating period beginning on or after that date):

- Provide additional information to patients through the Patient Access API.[253]
- Maintain an API for the purpose of exchanging certain health information with other health plans to ensure patients have continued access to their health information when they change

[236] *See* sec. 3403 of Public Law 116–136, 134 Stat. 372 (codified at 42 U.S.C. 294c).

[237] A PDMP is an electronic database that tracks prescriptions of controlled substances. ''Prescription Drug Monitoring Programs (PDMPs),'' U.S. Centers for Disease Control and Prevention, U.S. Department of Health and Human Services (May 7, 2024), *https://www.cdc.gov/overdose-prevention/php/interventions/prescription-drug-monitoring-programs.html.*

[238] *See* sec. 3221(k) of Public Law 116–136, 134 Stat. 379.

[239] The Medicare and Medicaid EHR Incentive Programs were also referred to as the Meaningful Use Programs. *See* 75 FR 44314 (July 28, 2010). Among the programs' initial requirements were all of the following: (1) performance or review of a security risk analysis in accordance with the requirements of the Security Rule; and (2) implementation of security updates as necessary and correction of identified security deficiencies as part of an eligible professional's risk management process. *See also* 77 FR 53968, 54002–03 (Sept. 4, 2012); ''Security Risk Analysis Tipsheet: Protecting Patients' Health Information,'' Centers for Medicare & Medicaid Services and Office for Civil Rights, U.S. Department of Health and Human Services (Dec. 2013), *www.cms.gov/files/document/security-risk-assessment-fact-sheetupdated-2014–04–18pdf.*

[240] *See* 75 FR 44314, 44321 (July 28, 2010).

[241] *See* 77 FR 53968, 53973 (Sept. 4, 2012).

[242] *Id.* In addition to the security-related requirements from Stage 1, Stage 2 added a requirement for eligible professionals to address the encryption and security of data at rest. *See* 77 FR 53968, 54002–03 (Sept. 4, 2012).

[243] *See* 80 FR 62762, 62765 (Oct. 16, 2015).

[244] *See* sec. 1903(t)(4)(A)(iii) of the SSA; *see also* 75 FR 44319, 44569–62 (July 28, 2010). CMS renamed the Medicare and Medicaid EHR Incentive Programs for eligible hospitals and CAHs as the Promoting Interoperability Programs as part of the FY2018 Hospital Inpatient Prospective Payment Systems for Acute Care Hospitals and the Long-Term Care Hospital Prospective Payment System final rule. 83 FR 41144, 41150 (Aug. 17, 2018). The Medicaid Promoting Interoperability Program ended on Dec. 31, 2021. ''Promoting Interoperability Program,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Sept. 11, 2026), *https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs.*

[245] ''About QPP,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (last accessed Jan. 15, 2026), *https://qpp.cms.gov/get-started/what-is-qpp/about-qpp.*

[246] *See* 90 FR 49266, 49654–64, 49868–49903 (Nov. 5, 2025); *see also* ''Promoting Interoperability: Traditional MIPS Requirements,'' Quality Payment Program, Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (last accessed Jan. 15, 2026), *https://qpp.cms.gov/reporting-requirements/ways-to-report/traditional-mips/promoting-interoperability;* ''APM Performance Pathway,'' Quality Payment Program, Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (last accessed Feb. 10, 2026), *https://qpp.cms.gov/reporting-requirements/ways-to-report/app.*

[247] *See generally* 85 FR 25510 (May 1, 2020).

[248] Fact Sheet, ''Trump Administration Announces MyHealthEData Initiative at HIMSS18,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Mar. 6, 2018), *https://www.cms.gov/newsroom/fact-sheets/trump-administration-announces-myhealthedata-initiative-himss18.*

[249] *See* NIST definition of ''Application Programming Interface (API),'' Glossary, Computer Security Resource Center, National Institute for Standards and Technology, U.S. Department of Commerce, *https://csrc.nist.gov/glossary/term/application_programming_interface.*

[250] *See* 85 FR 25510, 25512 (May 1, 2020).

[251] *See* 42 CFR 482.24, 482.61, 485.638; *see also* 85 FR 25510, 25584–25603 (May 1, 2020).

[252] *See* 89 FR 8758 (Feb. 8, 2024).

[253] *See* 42 CFR 422.119; 42 CFR 431.60; 42 CFR 438.242; 42 CFR 457.730; 45 CFR 156.221(b); 89 FR 8758, 8768–87 (Feb. 8, 2024).

health plans and support continuity of care (''Payer-to-Payer API'').[254]

- Maintain an API for the purpose of exchanging certain health information with health care providers to ensure that providers have access to individuals' health information for care coordination purposes (''Provider Access API'').[255]
- Implement new processes for prior authorization to reduce the burden on patients, providers, and health plans (''Prior Authorization API'').[256]

More recently, CMS published the Interoperability Standards and Prior Authorization for Drugs Proposed Rule,[257] which would require that certain health plans implement APIs to support electronic prior authorization for drugs that require prior authorization.[258] The proposals in the NPRM would encourage care coordination by enabling a more seamless exchange of ePHI, requiring health plans to make prior authorization decisions more quickly, and increasing the transparency of the prior authorization process for drugs that require prior authorization.[259]

Relatedly, CMS also announced an effort to modernize the nation's digital health ecosystem, including an expansion of data-sharing capabilities.[260] As part of this effort, CMS announced a call to action through an interoperability framework, aimed at bringing together health data networks to increase the electronic exchange of health information.[261] The initial framework criteria included several goals, such as:

- Enabling patients to access their electronic medical information anywhere the information lives on the network using applications of their choosing.
- Sharing patient consent preferences with all involved parties and supporting such preferences when required by law or policy.
- Facilitating care coordination by supporting queries for treatment purposes where the requesting provider has had their identity verified.
- Ensuring the availability of chart notes and clinical documents in machine- and human-readable formats, as specified in the United States Core Data for Interoperability (USCDI), Version 3.[262]
- Providing or facilitating access to health information using APIs.[263]

ONC has also issued numerous regulations that advance care coordination and individuals' access to their PHI, specifically their ePHI. As authorized by the HITECH Act, ONC established a voluntary certification program for health IT [264] and established the initial set of health data technical standards, implementation specifications, and certification criteria in 2010.[265] ONC routinely updates the standards, implementation specifications, and certification criteria to encourage the adoption of functionalities that enable care coordination or individual access through the electronic exchange of PHI, among other purposes.[266] For example, in 2024, ONC published the Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (''HTI–1'') final rule.[267] The HTI–1 final rule implements, among other things, certain provisions of the Cures Act that directed the Secretary to update certain provisions of the ONC Health IT Certification Program.[268] More recently, in alignment with the goals of Executive Orders 14192 [269] and 14267,[270] ONC revised the ONC Health IT Certification Program to focus on API-enabled interoperability solutions.[271]

ONC also has promulgated regulations that implement section 4004 of the Cures Act, which defines information blocking practices and authorizes civil monetary penalties and appropriate disincentives for the entities subject to the definition (referred to as the ''information blocking regulations'').[272] Information blocking refers to practices by actors [273] that, except as required by law or covered by an exception, are likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI, and that otherwise meet the requisite regulatory requirements.[274] While ONC has established exceptions for actions that otherwise would constitute information blocking, as authorized by statute,[275] the exceptions are limited to activities that are deemed reasonable and necessary as required by statute.[276] Since publication of the initial regulations in 2020, ONC has modified the information blocking regulations several times, generally to promote the access, exchange, and use of EHI.[277]

And in 2022, also as authorized under the Cures Act,[278] ONC published Version 1.0 of the Common Agreement,[279] which launched the Trusted Exchange Framework and Common Agreement (TEFCA), a

---

[254] *See* 42 CFR 422.121(b); 42 CFR 431.61(b); 42 CFR 457.731(b); 45 CFR 156.222(b); 89 FR 8758, 8820–58 (May 1, 2020).

[255] *See* 42 CFR 422.121(a); 42 CFR 431.61(a); 42 CFR 457.731(a); 45 CFR 156.222(a); 89 FR 8758, 8787–8820 (Feb. 8, 2024).

[256] *See* 42 CFR 431.80(b); 42 CFR 457.732(b); 45 CFR 156.223(b); 89 FR 8758, 8858–94 (Feb. 8, 2024).

[257] *See* 91 FR 19890 (Apr. 14, 2026).

[258] *Id.* at 19892.

[259] *Id.* at 19908–11.

[260] ''Health Technology Ecosystem: Overview,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Sept. 16, 2026), *https://www.cms.gov/priorities/health-technology-ecosystem/overview.*

[261] ''Health Technology System: Interoperability Framework,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Aug. 6, 2026), *https://www.cms.gov/health-technology-ecosystem/interoperability-framework.*

[262] The USCDI is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange. *See* ''United States Core Data for Interoperability (USCDI),'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (June 2025), *https://isp.healthit.gov/united-states-core-data-interoperability-uscdi#uscdi-v3.*

[263] ''Health Technology System: Interoperability Framework,'' *supra* note 261.

[264] *See* 45 CFR part 170, subparts A through E; 75 FR 36158 (June 24, 2010) (establishing a temporary certification program for health IT); 76 FR 1262 (Jan. 7, 2011).

[265] *See* 45 CFR part 170, subparts A–D; 75 FR 44590 (July 28, 2010).

[266] *See, e.g.,* 77 FR 54163 (Sept. 4, 2012); 80 FR 62602 (Oct. 16, 2015); 85 FR 25642 (May 1, 2020); 90 FR 36536 (Aug. 4, 2025).

[267] *See* 89 FR 1192 (Jan. 9, 2024).

[268] *See id.*

[269] 90 FR 9065 (Feb. 6, 2025).

[270] 90 FR 15629 (Apr. 9, 2025).

[271] *See* 91 FR 67916 (Oct. 28, 2026); *see also* ''Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity (HTI–5) Proposed Rule,'' Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Dec. 29, 2025), *https://www.healthit.gov/topic/laws-regulation-and-policy/health-data-technology-and-interoperability-astponc-deregulatory-actions-unleash-prosperity.*

[272] *See* 45 CFR part 171; 85 FR 25642 (May 1, 2020). OIG and CMS also play a role in administering and enforcing the information blocking regulations. *See* 88 FR 42820 (July 3, 2023); 89 FR 54662 (July 1, 2024).

[273] *See* 45 CFR 171.102 (definition of ''Actor'').

[274] *See* 45 CFR 171.102 (definition of ''Electronic health information'').

[275] *See* sec. 3022(a)(3) of the PHSA (42 U.S.C. 300jj–52(a)(3)).

[276] *See* 85 FR 25642, 25649 (May 1, 2020).

[277] *See, e.g.,* 89 FR 1192 (Jan. 9, 2024); 89 FR 101772 (Dec. 16, 2024); 89 FR 102512 (Dec. 17, 2024); 90 FR 36536 (Aug. 4, 2025).

[278] *See* sec. 4003(b) of the Cures Act, Public Law 114–255, 130 Stat. 1033, 1165, which amends sec. 3001(c) of the PHSA (codified at 42 U.S.C. 300jj–11(c)) (requiring the National Coordinator to build consensus and develop or support a trusted exchange framework, including a common agreement among health information networks nationally).

[279] ''ONC Completes Critical 21st Century Cures Act Requirement, Publishes the Trusted Exchange Framework and the Common Agreement for Health Information Networks,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Jan. 18, 2022), *https://www.hhs.gov/about/news/2022/01/18/onc-completes-critical-21st-century-cures-act-requirement-publishes-trusted-exchange-framework-common-agreement-health-information-networks.html.*

mechanism to enable the nationwide exchange of EHI across disparate health information networks [280] (HINs).[281] Among other things, TEFCA provides individuals and others, such as health care providers, health plans, and public health agencies, with easier, more efficient, secure access to more health information and reduces the number of connections that individuals, health care providers, and certain other parties that are part of or interact with the health care system need, to obtain health information.[282] The initial use cases for TEFCA support the secure electronic exchange of information for activities that are central to care coordination and individual access and include TPO and individual access services, among others.[283]

The Department also, as required by the Cures Act,[284] has published several guidance documents and engaged in education campaigns designed to promote individual access and to support the electronic exchange of health information. For example, the Department published guidance on the application of the HIPAA Rules to cloud computing solutions [285] and in an electronic exchange environment.[286] The Department also issued guidance on the individual right of access, health apps, and APIs to address questions about the implementation of the individual right of access when using health apps and APIs,[287] as well as publishing guidance on how the HIPAA Rules would apply in specific scenarios involving the use of health apps.[288] Additionally, in conjunction with the Federal Trade Commission, the Department published an interactive tool designed to help developers of certain mobile apps understand the Federal laws and regulations that may apply to them.[289] OCR and ONC also partnered to develop a series of materials designed to educate individuals about the right of access and promote patient access to their health information in a manner that ensures that such information is available in a form convenient for the patient, in a reasonable manner, without burdening the health care provider involved.[290]

Additionally, as required by the CARES Act, the Department modified the regulations that govern the confidentiality and disclosure of SUD patient records protected by Part 2 to decrease burdens on patients and providers, improve coordination of care and access to care and treatment, and strengthen certain confidentiality protections for SUD patient records.[291] These revisions to Part 2 have improved alignment with the Privacy Rule and provided greater flexibility for disclosures of patient identifying information within the health care system, while continuing to protect the confidentiality of Part 2 records.[292]

This discussion is not an exhaustive list of the changes in Federal law that support care coordination and case management or individuals' access to their PHI. Rather, it demonstrates the breadth and depth of the Department's commitment to improving care coordination and case management and empowering individuals by ensuring ready access to their PHI. When viewed through that lens, it is clear that Federal law has evolved significantly since the relevant provisions of the Privacy Rule were last modified, with an increased emphasis on the electronic exchange of health information to improve and encourage care coordination and support individuals' access, including their ability to direct a covered entity (and in some cases, a business associate), to provide access to their health information to other persons.

2. Technology That Enables the Electronic Exchange of PHI Is More Widely Available Today Than It Was in 2013 When the Omnibus Final Rule Was Published

The implementation of the laws discussed above and the availability of consumer-focused technology has spurred the adoption of EHRs and other health IT by various participants in the health care system.[293] In 2008, before the enactment of the HITECH Act, less than 10 percent of non-Federal acute care hospitals had implemented what was referred to at the time as a ''Basic EHR'' [294] (*i.e.,* an EHR). By 2018, approximately 99 percent of non-Federal acute care hospitals had adopted a Basic EHR and a certified EHR.[295] The ability of regulated entities to exchange information electronically increased with this shift from paper-based to electronic methods of record-keeping and the adoption of transaction, code set, and interoperability standards. This ability increased again with the adoption of API-standards based access

[280] An HIN is a type of health information organization. *See* 45 CFR 160.103 (definition of ''Business associate'' at (3)(i)).

[281] *See* ''TEFCA™: What is the Trusted Exchange Framework and Common Agreement™?,'' The Sequoia Project (last accessed Jan. 16, 2026), *https://rce.sequoiaproject.org/tefca/.*

[282] ''Trusted Exchange Framework and Common Agreement™ (TEFCA™),'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 1 (Nov. 2023), *https://www.healthit.gov/sites/default/files/page/2023-11/TEFCA_2-Pager_Digital_508.pdf.*

[283] ''TEFCA Framework: Exchange Purposes Explained,'' Sequoia Project (last accessed Oct. 8, 2026), *https://rce.sequoiaproject.org/exchange-purposes-explained/.* Currently, there are six approved Exchange Purposes under the Common Agreement: Government Benefits Determination; Health Care Operations; Individual Access Services; Payment; Public Health; and Treatment.

[284] *See* sec. 4006 of Public Law 114–255, 130 Stat. 1181 (Dec. 13, 2016) (directing the Department to issue guidance to health care providers on best practices for providing individuals with access to their PHI).

[285] ''Guidance on HIPAA & Cloud Computing,'' Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 7, 2016), *https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html.*

[286] ''Health Information Technology,'' Office for Civil Rights, U.S. Department of Health and Human Services (Sept. 2, 2020), *https://www.hhs.gov/hipaa/for-professionals/faq/health-information-technology/index.html.*

[287] ''The access right, health apps, & APIs,'' Office for Civil Rights, U.S. Department of Health and Human Services (Sept. 2, 2020).

[288] ''Health App Use Scenarios & HIPAA,'' Office for Civil Rights, U.S. Department of Health and Human Services (May 25, 2016), *https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf.*

[289] ''Mobile Health App Interactive Tool,'' U.S. Federal Trade Commission (Nov. 2024), *https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool.*

[290] *See* ''Get it. Check it. Use it.,'' U.S. Department of Health and Human Services (July 11, 2017), *https://www.hhs.gov/hipaa/for-individuals/right-to-access/index.html.*

[291] *See generally* 89 FR 12472 (Feb. 16, 2024).

[292] *Id.* at 12472, 12479.

[293] *See* 75 FR 44314–44588 (July 28, 2010); *see also* 75 FR 2014–47 (Jan. 13, 2010); 75 FR 36158–36209 (June 24, 2010); 75 FR 44590–44654 (July 28, 2010); 76 FR 1262–1331 (Jan. 7, 2011).

[294] Wesley Barker, et al., ''ONC Data Brief: Non-Federal Acute Care Hospital Electronic Health Record Adoption, 2008–2024,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (June 2026), *https://healthit.gov/data/data-briefs/non-federal-acute-care-hospital-electronic-health-record-adoption-2008-2024/;* A Basic EHR includes computerized capabilities for patient demographics, physician notes, nursing assessments, patient problem lists, electronic lists of medications taken by patients, discharge summaries, advanced directives, orders for medications, viewing laboratory results, and viewing radiology results. *Id.* at Definitions.

[295] ''ONC Data Brief: Non-Federal Acute Care Hospital Electronic Health Record Adoption, 2008–2024'' *supra* note 294; When used here, ''certified EHR'' means EHR technology that meets the technological capability, functionality, and security requirements adopted by the Department as certification criteria at 45 CFR part 170; *see also* ''Certified EHR Technology,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (updated Sept. 10, 2024), *https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs/certified-ehr-technology#:~:text=In%20order%20to%20efficiently%20capture,the%20Medicare%20Promoting%20Interoperability%20Program* (''In order to efficiently capture and share patient data, health care providers need certified electronic health record (EHR) technology (CEHRT) that stores data in a structured format. Structured data allows health care providers to easily retrieve and transfer patient information and use the EHR in ways that can aid patient care.'').

and exchange and the implementation of the information blocking regulations in 2020.[296] In 2014, 41 percent of such hospitals routinely had electronic access to clinical information from outside providers or sources when treating a patient.[297] By 2023, 70 percent of non-Federal acute care hospitals engaged in all domains of interoperable exchange routinely or sometimes, a significant increase.[298] By 2024, more than 85 percent of non-Federal acute care hospitals were integrating third-party data into their EHRs for clinical or administrative purposes, while a similar percentage regularly were providing third parties with data from their EHRs.[299] In 2016, 38 percent of hospitals had enabled patients to access their health information using an application, and in 2018, 57 percent had enabled patient access to their clinical notes in their patient portal; by 2021, 70 percent of hospitals enabled patients to access their health information using an application, and 82 percent enabled patients to view their clinical notes in their patient portal.[300] By 2024, the percentage of hospitals that supported patient access through apps increased to 90 percent.[301]

Research has demonstrated the important role that patient and health plan member portals, one method of providing individual access encouraged by the Department,[302] currently play in increasing patient centeredness of care and health information-seeking self-efficacy for individuals.[303] In 2020, the Health Information National Trends Survey [304] (HINTS) found that more than half of individuals with a mobile health app used it to facilitate discussions with their health care provider that same year, while approximately the same percentage used their health app to make decisions about how to treat an illness or condition.[305] According to the 2024 HINTS, more than 75 percent of respondents reported being offered access to their PHI at least once during the previous year, and almost two-thirds of individuals reported accessing their records during that same time period.[306] Respondents also reported that proxy and caregiver access had more than doubled. Among individuals surveyed, 69 percent of patients with at least one chronic condition, and 76 percent of individuals with a recent cancer diagnosis, reported accessing their patient portal or online medical records in the previous year.[307]

Patient and health plan member portals are not the only technology that is more widely available today than it was in 2013. Health apps, while available in 2013, were not used or relied upon to the degree that they are today. The 2024 HINTS shows that 57 percent of respondents reported using an app to access their records during the year, a significant increase over the 38 percent that reported doing the same in 2020.[308] A 2023 study examined downloads of specific mobile health apps from the Google Play website [309] and data from HINTS 6 to learn about people's use of apps to access health information. Among the apps used by individuals to access their PHI reviewed in the study, almost 99 percent of the app downloads were for patient portal apps provided to the individual by a covered entity or business associate.[310] The remaining 1 percent of the app downloads were for personal health apps provided directly to individuals.[311] While a small percentage, this actually represented significant growth over 2021, with one app responsible for 77 percent of that growth.[312] Research by ONC indicated that, in 2022, 2 percent of individuals reported using a ''portal organizing app,'' that is an app that aggregates an individual's PHI from different patient portals or online medical records; by 2024, the figure had increased to 7 percent.[313] And the Department anticipates that this number will increase even further in response to the recent launch of the Medicare App Library, a centralized directory of vetted digital health care options for Medicare beneficiaries.[314] This suggests that mobile apps, particularly patient portal apps, are an entry point for individuals to obtain access to and engage with their PHI today. We anticipate that the use of both patient and health plan member portal apps and apps provided directly to individuals is likely to increase over time, particularly in light of the changes to Federal law in the last 10 years, as discussed below.

[296] *See* 85 FR 25642 (May 1, 2020); *see also* sec. 4003(b) and 4004 of Public Law 114–255, 130 Stat. 1165 and 1176 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–11(c) and 42 U.S.C. 300jj–52).

[297] Dustin Charles, et al., ''ONC Data Brief: Interoperability among U.S. Non-federal Acute Care Hospitals, 2014,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 1 (Aug. 2015), *https://healthit.gov/wp-content/uploads/2017/03/onc_databrief25_interoperabilityv16final_081115.pdf.*

[298] Meghan Hufstader Gabriel, et al., ''ONC Data Brief: Interoperable Exchange of Patient Health Information Among U.S. Hospitals: 2023,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 1 (May 2024), *https://healthit.gov/wp-content/uploads/2024/05/Interoperable-Exchange-of-Patient-Health-Information-Among-U.S.-Hospitals-2023.pdf.*

[299] Catherine Strawley, et al., ''ONC Data Brief: Hospital Use of APIs to Enable Data Sharing between EHRs and Third-Party Technology,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Feb. 2026), *https://healthit.gov/data/data-briefs/hospital-use-of-apis-to-enable-data-sharing-between-ehrs-and-third-party-technology/.*

[300] Wesley Barker, et al., ''ONC Data Brief: Hospital Capabilities to Enable Patient Electronic Access to Health Information, 2021,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 2, 5 (Oct. 2022) (estimates based on non-Federal acute care hospitals and applications configured to meet the API specifications in the hospital's EHR), *https://healthit.gov/wp-content/uploads/2022/12/hospital_capabilities_to_enable_patient_access_ONC_DB2021-Updated.pdf.*

[301] ''ONC Data Brief: Hospital Use of APIs to Enable Data Sharing between EHRs and Third-Party Technology,'' *supra* note 299.

[302] Stage 1 of the Meaningful Use Program required eligible health care providers to provide electronic copies of health information or discharge instructions and timely access to health information. *See* 75 FR 44314, 44321 (July 28, 2010). Stage 2 replaced this objective with a requirement that eligible health care providers provide patients with the ability to view online, download, and transmit their health information within a specified period of time. 77 FR 53968, 53973 (Sept. 4, 2012). Stage 2 also required eligible health care professionals to use secure electronic messaging to communicate with patients on relevant health information. *Id.* at 54031.

[303] Maryum Zaidi, et al., ''Association Between Patient Portal Use and Perceived Patient-Centered Communication Among Adults With Cancer: Cross-section Survey Study,'' JMIR Cancer (Aug. 2022), *https://cancer.jmir.org/2022/3/e34745/PDF.*

[304] HINTS is a nationally representative survey of U.S. adults.

[305] Christian Johnson, et al., ''ONC Data Brief: Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2020,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Sept. 2021), *https://healthit.gov/data/data-briefs/individuals-access-and-use-patient-portals-and-smartphone-health-apps-2020/.*

[306] Chelsea Richwine, ''ONC Data Brief: Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2024,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 8 (July 2025), *https://healthit.gov/data/data-briefs/individuals-access-and-use-patient-portals-and-smartphone-health-apps-2024/.*

[307] *Id.* at p. 3.

[308] *Id.* at p. 5.

[309] Google Play is the app store for users of Android devices and devices with the Chrome operating system.

[310] Wesley Barker, et al., ''Patient Usage of Apps to Access Online Medical Records,'' JAMA Network Open, p. 2 (Nov. 14, 2023), *https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2811823.* Patient portal apps, when used in reference to this study, includes apps developed by EHR vendors, health care providers, and health plans. *Id.*

[311] *Id.*

[312] *Id.*

[313] ''ONC Data Brief: Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2024,'' *supra* note 306, at p. 7.

[314] ''Medicare App Library,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Aug. 24, 2026), *https://www.cms.gov/priorities/health-technology-ecosystem/overview/medicare-app-library.*

3. Individuals Benefit When Their PHI Can Be Accessed and Exchanged Electronically

As technology enabling access to and exchange of PHI and other health information has evolved and been implemented widely, it has become apparent that providing individuals with access to their PHI electronically provides significant benefits to the individuals who take advantage of that access. Based on telephone interviews with 40 individuals living with diabetes who use the VA patient portal, individuals generally found patient portals to be ''useful for receiving help in managing symptoms, coordinating their care, and learning about their health.'' [315] Reading clinical notes and test results helped the individuals to understand their health information, to gauge the seriousness of their health issues, and to make decisions regarding their care plan.[316] Having access to test results enabled individuals to be proactive in response to those results.[317]

Recent studies have found the use of patient portals to be associated with improved health outcomes.[318] For example, a 2025 study examined the relationship between patient portal enrollment and retention in care and disease management, specifically human immunodeficiency virus (HIV) viral suppression, and found that an active patient portal account was associated with improved HIV care outcomes for people living with HIV, such as viral suppression and retention in care.[319] A 2024 analysis of data from HINTS 5 found that the use of patient portals by patients ''may build health information efficacy, which seems to promote communication between patients and health care providers,'' particularly for patients with low social support.[320] According to a 2023 study of adult patients' experiences with patient portals, among the benefits reported by patients were the ability to communicate with their providers electronically, viewing test results and visit summaries, managing appointments and receiving reminders, easy access to their health information, getting prescription refills and reviewing medications, and the ease of use and convenience.[321] This evidence suggests that there is a correlation between individual health outcomes and use of patient portals, raising the possibility that encouraging the use of technology that enables individuals and certain other persons to access the individual's PHI could positively affect health outcomes.

The integration of patient-reported information with PHI in EHRs also may allow for improved communication between individuals and their health care providers and facilitate better medication management. A 2022 publication evaluated the use of a particular application for medication management that was integrated into the patient portal of a health care provider's EHR. According to the study's authors, the individuals who were able to use the application benefited from ''real-time medication reconciliation and support for patient-provider communication,'' which enabled patients ''to pull and display the actual, up-to-date medication list for review with a pharmacist in the comfort and convenience of the patient's home setting,'' an innovation that was welcomed by patients.[322] It also enabled patients to learn about the falsehoods associated with medications, identify errors in their active medication list, and learn about the side effects and indications of medications.[323] And it alleviated concerns about newly prescribed medications, such as dosage and timing.[324] Based on an analysis of the 2022 HINTS, 42 percent of individuals who used an app to access their online medical records reported that they accessed those records at least six times in the previous year, while 28 percent of those who used only a web-based portal reported doing so.[325] According to ONC, this ''suggests [that] the use of apps may make it easier and more convenient for patients to track and engage with their health information.'' [326] Another 2022 publication studied the role that the type of portal access plays in promoting patient engagement and found that patients who accessed their medical records through a mobile health app, rather than solely through an online portal, were more likely to view online, download, and transmit their health information; interact with their providers; and interact with their PHI.[327] Participants who accessed their medical records through a mobile health app were more likely to use that information to make decisions about health care and download medical results or share them with another party. They also were more likely to use the app to add information to their medical records, correct their medical records, send secure messages to their providers, request prescription refills, and view medical results.[328] According to an ONC report, by 2024, nearly two-thirds of non-Federal acute care hospitals offered patients the ability to submit health information directly to the EHR.[329] This suggests that there will be even greater potential for improvements in care management as individuals grow accustomed to having this ability and this new channel for communication with health care providers.

The benefits to individuals of the electronic exchange of PHI are not limited to circumstances where the individuals themselves have access to the information. Individuals also may benefit from enabling access to their PHI in a portal or mobile health app for caregivers, family members, personal representatives, and other persons designated by the individual as being involved in their care. A 2024 HINTS showed that the number of persons who accessed the online medical record or patient portal of an individual for whom

[315] ''The Promise of Patient Portals for Individuals Living with Chronic Illness: Qualitative Study Identifying Pathways of Patient Engagement,'' *supra* note 166.

[316] *Id.*

[317] *Id.*

[318] *See also* Elisa H. Son, et al., ''Adult Patients' Experiences of Using a Patient Portal With a Focus on Perceived Benefits and Difficulties, and Perceptions on Privacy and Security: Qualitative Descriptive Study,'' JMIR Human Factors (Jan. 2023), *https://humanfactors.jmir.org/2023/1/e46044.*

[319] Jessica P. Ridgway, et al., ''Association Between Electronic Patient Portal Enrollment and HIV Care Outcomes Among People Living with HIV at an Urban Academic Medical Center,'' AIDS and Behavior (Aug. 10, 2025), *https://link.springer.com/article/10.1007/s10461-025-04869-7.*

[320] Suhwoo Ahn, et al., ''Patients' Use of Electronic Health Records Facilitates Patient-Centered Communication: Findings from the 2017 Health Information National Trends Survey,'' Journal of Medical internet Research (Nov. 2024), *https://www.jmir.org/2024/1/e50476.*

[321] ''Adult Patients' Experiences of Using a Patient Portal With a Focus on Perceived Benefits and Difficulties, and Perceptions on Privacy and Security: Qualitative Descriptive Study,'' *supra* note 318.

[322] Susan E. Spratt, et al., ''Feasibility of Electronic Health Record Integration of a SMART Application to Facilitate Patient-Provider Communication for Medication Management,'' CIN: Computers, Informatics, Nursing, p. 538–46, 544 (Aug. 2022), *https://journals.lww.com/cinjournal/fulltext/2022/08000/feasibility_of_electronic_health_record.6.aspx.*

[323] *Id.*

[324] *Id.*

[325] Catherine Strawley, et al., ''ONC Data Brief: Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2022,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 9 (Oct. 2023), *https://healthit.gov/wp-content/uploads/2023/10/DB69_IndividualsAccess-UsePatientPortals_508.pdf.*

[326] *Id.*

[327] Theophile Ndabu, et al., ''The Role of Access Type and Age Group in the Breadth of Use of Patient Portals: Observational Study,'' Journal of Medical internet Research (Dec. 27, 2022), *https://pmc.ncbi.nlm.nih.gov/articles/PMC9832356/.*

[328] *Id.*

[329] ''ONC Data Brief: Hospital Use of APIs to Enable Data Sharing between EHRs and Third-Party Technology,'' *supra* note 300.

they are providing care or making health care decisions (proxy access or caregiver access) more than doubled between 2020 and 2024, from 24 to 51 percent.[330]

Research suggests that ''[r]outine assessment and support of family caregivers are elements of high-quality clinical care and robust systems of long-term services and supports.'' [331] Being able to directly access PHI in patient or health plan member portals or through mobile apps can provide caregivers with convenient and continuous access, which can increase their engagement in and understanding of the individual's condition and care.[332] Where appropriate, being able to use the patient or health plan member portal or app to interact with the individual's PHI or health care providers can enable those caregivers and others involved in caring for the individual to communicate directly with the individual's health care provider and provides greater legitimacy to their interactions with the covered entity when such access is obtained using their own unique identity credentials, rather than those of the individual.[333]

C. To Continue To Improve the Efficiency and Effectiveness of the Health Care System, the Department Must Modify the Privacy Rule To Address Issues That Impede Care Coordination and Individuals' Access to Their PHI

As our understanding of an effective and efficient health care system evolves and the health care environment changes, the Department must periodically reconsider whether the Privacy Rule is properly balancing the interests of individuals in the privacy of their PHI with the need for their PHI to be used or disclosed to improve their health outcomes and their ability to access their health information and to share it with others. As part of this examination, the Department must determine whether the Privacy Rule accurately reflects the obligations of regulated entities and the rights of individuals, whether regulated entities are correctly interpreting and applying the Privacy Rule, and whether the Privacy Rule unnecessarily imposes real or perceived barriers to the accomplishment of HIPAA's goals.

1. The Department Must Ensure that the Privacy Rule Accurately Reflects the Obligations of Regulated Entities and the Rights of Individuals

The Department's authority to adopt and modify standards relating to the privacy of individually identifiable health is limited to its authority under HIPAA,[334] the HITECH Act,[335] and certain other statutes.[336]

The APA generally requires that, when issuing a new regulation or modifying an existing one, the Department publish a NPRM in the **Federal Register**.[337] The notice must include, among other things, either the terms or substance of the proposed rule or a description of the subjects and issues involved.[338] The APA also generally requires that after the notice is published, the Department must provide interested persons with an opportunity to provide comment on the notice.[339]

As discussed above, Congress established, in section 13405(e) of the HITECH Act, that individuals have the right of access to direct a covered entity to transmit an electronic copy of PHI in an electronic health record to a person designated by the individual. In 2010, the Department issued an NPRM and solicited public comment on a proposal to extend that right to all PHI and for copies in any format. The Department finalized this proposal as part of the 2013 Omnibus Rule. However, in 2020, the court in *Ciox* vacated the Department's actions with respect to section 13405(e).[340] In light of the *Ciox* court's vacatur of this provision, the Department was required to propose to implement section 13405(e) in a manner that is consistent with the court's decision and seek comment on that proposal, which we did in the 2021 Privacy Rule NPRM. The Department now engages in final agency action—*i.e.,* publishes a final rule—to implement this right.

2. Regulated Entities Misinterpret the Privacy Rule in Ways That Are Inconsistent With an Efficient and Effective Health Care System

An efficient and effective health care system requires that PHI is used and disclosed appropriately. As discussed above, both Congress and the Department have taken steps to increase the efficiency and effectiveness of the health care system by making it easier to use and disclose PHI, while also protecting individuals' privacy. And yet, the Department continues to receive reports that covered entities are refusing to disclose PHI to individuals, other covered entities, family members, caregivers, and others, absent burdensome measures that are, at best, not required by the Privacy Rule, and at times, are inconsistent with the Privacy Rule and/or other laws that govern the use and disclosure of PHI.[341] In 2024, the right of access was among the top five issues alleged in the HIPAA complaints that the Department resolved.[342] As discussed in greater

[330] ''ONC Data Brief: Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2024,'' *supra* note 306, at p. 2.

[331] Jennifer L. Wolff, et al., ''Shared Access to Patient Portals for Older Adults: Implications for Privacy and Digital Health Equity,'' JMIR Aging (May 2022), *https://aging.jmir.org/2022/2/e34628/.*

[332] *Id.*

[333] *Id.*

[334] *See* Public Law 104–191, 110 Stat. 1936 (Aug. 21, 1996) (codified at 42 U.S.C. 201 note); *see also Association of American Physicians & Surgeons, Inc.* v. *U.S. Department of Health and Human Services,* 224 F. Supp. 2d 1115 (S.D. Tex. 2002) (holding that HIPAA falls within Congress' Commerce Clause authority).

[335] *See* Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111–5, 123 Stat. 226 (Feb. 17, 2009) (codified at 42 U.S.C. 201 note); sec. 2(a)(iii) of E.O. 14219, 90 FR 10583 (Feb. 25, 2025).

[336] *See* Genetic Information Nondiscrimination Act of 2008 (GINA), title I, sec. 105, Public Law 110–233, 122 Stat. 881 (May 21, 2008) (codified at 42 U.S.C. 2000ff); 21st Century Cures Act, Public Law 114–255, 130 Stat. 1033 (Dec. 13, 2016); CARES Act, Public Law 116–136, 134 Stat. 281 (Mar. 27, 2020); *see also* sec. 2(a)(iii) of E.O. 14219, 90 FR 10583 (Feb. 25, 2025).

[337] 5 U.S.C. 553(b).

[338] 5 U.S.C. 553(b)(3).

[339] 5 U.S.C. 553(c).

[340] *Ciox,* 435 F. Supp. 3d 30.

[341] *See, e.g.,* Steve Alder, ''Renown Health Pays $75,000 to Settle HIPAA Right of Access Case,'' The HIPAA Journal (Feb. 11, 2021), *https://www.hipaajournal.com/renown-health-pays-75000-to-settle-hipaa-right-of-access-case/;* Press Release, ''OCR Settles Sixteenth Investigation in HIPAA Right of Access Initiative,'' Office for Civil Rights, U.S. Department of Health and Human Services (Feb. 12, 2021), *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/sharp/index.html;* Press Release, ''Eleven Enforcement Actions Uphold Patients' Rights Under HIPAA,'' Office for Civil Rights, U.S. Department of Health and Human Services (July 15, 2022); Press Release, ''HHS Civil Rights Office Resolves HIPAA Right of Access Investigation with $20,000 Settlement,'' Office for Civil Rights, U.S. Department of Health and Human Services (Dec. 15, 2022), *https://www.hhs.gov/about/news/2022/12/15/hhs-civil-rights-office-resolves-hipaa-right-of-access-investigation-with-20000-dollar-settlement.html;* Press Release, ''Lab Pays $16,500 Settlement to HHS, Resolving Potential HIPAA Violation over Medical Records Request,'' Office for Civil Rights, U.S. Department of Health and Human Services (Jan. 3, 2023), *https://www.hhs.gov/about/news/2023/01/03/lab-pays-16-thousand-5-hundred-dollar-settlement-to-hhs-resolving-potential-hipaa-violation.html;* Press Release, ''HHS Office for Civil Rights Imposes a $200,000 Penalty Against Oregon Health & Science University for Failure to Provide Timely Access to Patient Records,'' Office for Civil Rights, U.S. Department of Health and Human Services (Mar. 6, 2025), *https://www.hhs.gov/press-room/penalty-against-or-health-science-university.html;* Press Release, ''HHS' Office for Civil Rights Settles HIPAA Right of Access Investigation with Azul Vision, Inc.,'' Office for Civil Rights, U.S. Department of Health and Human Services (Aug. 27, 2026), *https://www.hhs.gov/press-room/hhs-ocr-settles-hipaa-investigation-with-azul-vision.html.*

[342] The number of complaints resolved in a given calendar year is the sum of administrative closures, technical assistance closures, and investigated closures. *See* ''Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification

detail below, in the 2018 RFI and 2021 Privacy Rule NPRM, the Department has received public comments stating that covered entities often refuse to disclose PHI without a written authorization in situations where the Privacy Rule permits or requires such disclosures absent a written authorization, as well anecdotal reports of the same from other Federal agencies. For example, while the Privacy Rule permits (but does not require) a covered entity to obtain an individual's consent to disclose PHI for treatment purposes (*e.g.,* care coordination), some covered entities refuse to disclose PHI to a health care provider for these purposes without a written authorization.[343] Depending on the circumstances, requiring that the individual provide a written authorization—or in some cases, a written form that requires less information than a written authorization—could increase the burden on the individual and/or delay essential health care. Additionally, ONC has received 2,450 possible claims of information blocking against health care providers, HIEs/HINs, and health IT developers of certified health IT.[344] Of the 2,450 possible claims, approximately 63 percent were filed by patients.[345] Approximately 13 percent were filed by third parties (other than attorneys) on behalf of a patient, while approximately 10 percent were filed by health care providers.[346] An overwhelming majority of the claims—approximately 79 percent—were filed against health care providers,[347] most of whom are also covered entities. Almost 14 percent of complaints were filed against developers of health IT that have developed products that are on ONC's list of certified products.[348] Such developers are often business associates under the HIPAA Rules.[349] As Congress explicitly recognized, at least some of the allegations in these complaints also may indicate possible violations of the Privacy Rule.[350] For example, a health care provider's delay in responding to an individual's request for a copy of their ePHI may be a violation of both the information blocking regulations [351] and the Privacy Rule [352] where the health care provider is both an ''actor'' and a covered entity.[353] The Department also is aware that there may be instances in which the parents of minor children are not receiving access to their children's PHI to the extent required by the Privacy Rule or their access is substantially delayed.[354]

Additionally, as Congress has enacted and/or the Department has implemented the laws discussed above (*e.g.,* the Cures Act, the Interoperability and Patient Access Final Rule, the Cures Act Final Rule), questions have arisen regarding the ability of regulated entities to comply with these new statutes and regulations and the Privacy Rule. Far too often, regulated entities cite HIPAA or the HIPAA Rules as a reason that they cannot disclose PHI, even in circumstances where the Privacy Rule permits the requested disclosure. For example, when evaluating the success of California's section 1115 demonstration that required the implementation of health IT to encourage the exchange of PHI for care coordination, researchers found that among the most frequently cited barriers to the exchange of PHI among participant sites and their

Rule Compliance for Calendar Year 2024,'' Office for Civil Rights, U.S. Department of Health and Human Services, p. 9, *https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2024.pdf.*

[343] 45 CFR 164.506(b) and (c)(2). HIPAA excepts, from its general preemption authority, contrary provisions of state law that impose requirements, standards, or implementation specifications that are more stringent than those of the Privacy Rule. *See* Health Insurance Portability and Accountability Act of 1996, sec. 264(c)(2) of Public Law 104–191, 110 Stat. 2033 (codified at 42 U.S.C. 1320d–2 note); 45 CFR 160.203(b). If a provision of state law provides greater privacy protection than a provision of the Privacy Rule, and it is possible for regulated entities to comply with both the state law and the Privacy Rule (*e.g.,* where a state law requires that a covered entity obtain an individual's consent before disclosing PHI for treatment purposes), there is no conflict between the laws, and no preemption. *See also* ''My state law provides greater privacy protections on patients' HIV information than the HIPAA Privacy Rule. Is this more protective state law preempted by the Privacy Rule?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #405 (Mar. 23, 2007), *https://www.hhs.gov/hipaa/for-professionals/faq/405/is-this-more-protective-state-law-preempted-by-the-privacy-rule/index.html.*

[344] *See* ''Information Blocking Claims: By the Numbers,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (July 2026), *https://www.healthit.gov/data/quickstats/information-blocking-claims-numbers;* 45 CFR 170.103 (definition of ''Actor''). For more information on the information blocking regulations, *see generally* 45 CFR 170.100 *et seq.* Most health care providers, HIE/HINs, and developers of certified health IT are either covered entities or business associates because they either: (1) perform a covered function for, or on behalf of, a covered entity (*e.g.,* an HIE/HIN transmits PHI on behalf of a health care provider); or (2) they provide a service that involves the disclosure of PHI from a covered entity or another business associate (*e.g.,* a developer of a certified EHR maintains the EHR software and may require access to the PHI to provide such maintenance services). *See* 45 CFR 160.103 (definitions of ''Covered entity'' and ''Business associate'').

[345] *See* ''Information Blocking Claims: By the Numbers,'' *supra* note 344.

[346] *Id.*

[347] *Id.*

[348] *Id.*

[349] *See* ''Health App Use Scenarios & HIPAA,'' Office for Civil Rights, U.S. Department of Health and Human Services (Feb. 2016), *https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf.*

[350] The Cures Act specifically affords HHS OIG with the ability to refer instances of information blocking to OCR for resolution if OIG determines that a consultation regarding the Privacy Rule will resolve an information blocking claim. *See* sec. 4004 of the Cures Act, Public Law 114–255, 130 Stat. 1033, 1177 (Dec. 13, 2016), which amends subtitle C of title XXX of the PHSA (42 U.S.C. 300jj–51 *et seq.*) (codified at 42 U.S.C. 300jj–52(b)(3)).

[351] *See* ''When would a delay in fulfilling a request for access, exchange, or use of EHI be considered an interference under the information blocking regulation?,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Mar. 2021), *https://healthit.gov/faq/when-would-delay-fulfilling-request-access-exchange-or-use-ehi-be-considered-interference-under/.*

[352] *See* 45 CFR 164.524(b)(2).

[353] Although the information blocking regulations and the Privacy Rule impose similar obligations on covered health care providers, the obligations are not identical. Thus, a covered health care provider's delay in responding to a right of access request is not always a violation of both the information blocking regulations and the Privacy Rule. *Compare* 45 CFR part 171 *et seq. with* 45 CFR 164.524.

[354] *See* Letter to Colleagues from OCR Director Paula M. Stannard (Dec. 3, 2025) (reminding health care providers (and other covered entities) about HIPAA provisions that require them to provide parents access to their children's PHI, consistent with applicable law), *https://www.hhs.gov/sites/default/files/ocr-letter-hipaa-privacy-rule-and-parental-access-to-minor-childrens-medical-records.pdf;* 45 CFR 164.502(g)(3); Press Release, ''OCR Settles Nineteenth Investigation in HIPAA Right of Access Initiative,'' Office for Civil Rights, U.S. Department of Health and Human Services (June 2, 2021), *https://us.pagefreezer.com/en-US/wa/browse/0a7f82bb-be6e-448a-ae11-373d22c37842?find-by-timestamp=2022-12-24T06:33:59Z&url=https:%2F%2Fwww.hhs.gov%2Fabout%2Fnews%2F2021%2F06%2F02%2Focr-settles-nineteenth-investigation-hipaa-right-access-initiative.html&timestamp=2022-12-24T03:43:08Z;* Press Release, ''OCR Resolves Twentieth Investigation in HIPAA Right of Access Initiative with $80,000 Settlement,'' Office for Civil Rights, U.S. Department of Health and Human Services (Sept. 10, 2021), *https://us.pagefreezer.com/en-US/wa/browse/0a7f82bb-be6e-448a-ae11-373d22c37842?find-by-timestamp=2022-12-27T06:17:59Z&url=https:%2F%2Fwww.hhs.gov%2Fabout%2Fnews%2F2021%2F09%2F10%2Focr-resolves-twentieth-investigation-in-hipaa-right-of-access-initiative-with-settlement.html&timestamp=2022-12-27T03:43:10Z;* ''Eleven Enforcement Actions Uphold Patients' Rights Under HIPAA,'' *supra* note 341; Resolution Agreement and Corrective Action Plan, ''Optum Medical Care,'' Office for Civil Rights, U.S. Department of Health and Human Services (Nov. 15, 2023), *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/optum-medical-care.html;* Notice of final determination, ''Hackensack Meridian Health, West Caldwell Care Center,'' Office for Civil Rights, U.S. Department of Health and Human Services (Jan. 12, 2024), *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/hackensack-meridian-health-west-caldwell-care-center/index.html#nfd;* Press Release, ''HHS Office for Civil Rights Imposes a $70,000 Civil Monetary Penalty Against Gums Dental Care for Failure to Provide Timely Access to Patient Records,'' Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 17, 2024), *https://www.hhs.gov/about/news/2024/10/17/hhs-office-civil-rights-imposes-70000-civil-monetary-penalty-against-gums-dental-care-failure-provide-timely-access-patient-records.html.*

partners was a fear of violating HIPAA or other data privacy laws, even where the disclosure of PHI would be between departments within the same agency.[355] More recently, a study published in 2025 examined key barriers and facilitators influencing compliance with certain substance abuse performance metrics.[356] The study found that ''[w]hile regulations like [. . .] [the Privacy Rule] offer privacy protections, inconsistencies in [its] interpretation contribute to uncertainty and reluctance to share data.'' [357] And as another example, despite evidence that individuals and family members are interested in shared access to the individual's PHI,[358] a 2022 study found that few individuals and family members have taken advantage of it. While the study did not examine the reasons for the wasted potential, the authors speculate that providers may hesitate to encourage shared access because of concerns that they might be in violation of the Privacy Rule.[359] This reluctance to share information for care coordination and with individuals, their family members, their personal representatives, and their caregivers is inefficient and decreases the effectiveness of the quality of the care that individuals receive. Thus, it is imperative that the Department clarify the relationship between the Privacy Rule and the laws enacted after its publication that similarly encourage the electronic exchange of health information for care coordination and support individual access.

3. Regulations That Unnecessarily Impose Real or Perceived Burdens Are Barriers to an Efficient and Effective Health Care System

Unnecessary or outdated regulations can impose significant costs on regulated entities, decreasing the resources available for high-quality health care.[360] Thus, it is incumbent upon the administering agency to periodically consider whether such regulations continue to serve their original purpose or whether they impose a significant cost without sufficient benefits to offset those costs.[361] An important component of Making America Healthy Again is preventing and treating chronic diseases. Accordingly, the Department must take steps to eliminate regulations or regulatory requirements that draw resources away from this goal. For example, based on overwhelming feedback from the public, the Department believes that, at this point, unnecessary administrative burdens are imposed on both individuals and workforce members without meaningful corresponding benefits by the requirement that, with limited exceptions, covered health care providers with a direct treatment relationship to an individual make a good faith effort to obtain a written acknowledgment from the individual that they have received a copy of the covered health care provider's NPP. As such, the Department believes that it is necessary to remove the requirement.

As another example, stakeholders have shared with the Department anecdotal accounts of a regulated entity refusing to allow a workforce member to use a TRS [362] communications assistant [363] to share PHI with other workforce members or outside persons as needed to perform their duties. While a longstanding frequently asked question (FAQ) addresses the use of TRS by a covered entity to communicate with individuals who are deaf, hard of hearing, or deaf-blind, or who have a speech disability and explicitly provides that a business associate agreement is not required in such circumstances, the FAQ does not address its use by workforce members (who are similarly situated) of a regulated entity to share PHI with other workforce members or outside parties as needed to perform their duties.[364] As discussed below, because of the unique legal status of TRS providers, requiring that regulated entities enter into business associate agreements with TRS providers so that workforce members can use them to share PHI with other workforce members or outside persons would increase the burden on regulated entities without sufficient benefits to offset the costs. Accordingly, the Department believes that it is necessary to modify the Privacy Rule to expressly exclude TRS providers from the definition of business associate.

And as another example, while the Privacy Rule generally permits covered entities to use and disclose PHI of Armed Services personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, subject to certain conditions,[365] it does not permit such uses and disclosures for other similarly situated personnel of nonmilitary Uniformed Services. Members of the USPHS Commissioned Corps and the NOAA Commissioned Corps are required to meet similar medical requirements and standards for mission readiness, but the absence of a Privacy Rule permission that applies to them means that it is more challenging and burdensome for the Departments of Health and Human Services (USPHS Commissioned Corps) and Commerce (NOAA Commissioned Corps) to use and disclose PHI to ensure the medical readiness and the ability of their respective Commissioned Corps to fulfill their respective missions. Modifying the Privacy Rule to reflect the similar roles and responsibilities of the USPHS and NOAA Commissioned Corps and the Armed Services will remove unnecessary burdens on USPHS and NOAA Commissioned Corps, reduce costs to the U.S. taxpayer, and facilitate the medical readiness of the Uniformed Services.

D. The Department Has Performed the Statutorily Required Consultations

In accordance with 42 U.S.C. 1320d–1(c)(2)(B),[366] the Department has determined that the requirement that the Secretary adopt standards [367] that

[355] *See* ''Final Evaluation of California's Whole Person Care (WPC) Program,'' *supra* note 202, at p. 91.

[356] Mengyi Wei, et al., ''Advancing Health Equity Through Substance Use Medical Record Data Sharing: Insights from Health Care Providers,'' International Journal of Environmental Research and Public Health (Mar. 21, 2025), *https://doi.org/10.3390/ijerph22040462.*

[357] *Id.*

[358] *See, e.g.,* Jennifer L. Wolff, et al., ''Sharing in Care: Engaging Care Partners in the Care and Communication of Breast Cancer Patients,'' Breast Cancer Research and Treatment (Aug. 2019), *https://europepmc.org/article/MED/31165374.*

[359] ''Shared Access to Patient Portals for Older Adults: Implications for Privacy and Digital Health Equity,'' *supra* note 331.

[360] *See* sec. 1 of E.O. 14192, 90 FR 9065 (Feb. 6, 2025); *see also* sec. 2(v) of E.O. 14219, 90 FR 10583 (Feb. 25, 2025).

[361] *See* sec. 2(v) of E.O. 14219, 90 FR 10583 (Feb. 25, 2025).

[362] TRS is a service that enables people who are deaf, hard of hearing, or deaf-blind, or who have a speech disability to communicate by either transliterating text or interpreting American Sign Language (ASL) to voice and vice versa. *See* ''Consumer Guide, Telecommunications Relay Service,'' Federal Communications Commission (Aug. 16, 2022), *https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs.*

[363] A TRS communications assistant facilitates telephone calls between individuals who are deaf, hard of hearing, or deaf-blind, or who have a speech disability, and others. *See* 47 CFR 64.601(a)(12) (definition of ''Communications assistant'').

[364] *See* ''When a covered entity, such as a doctor, uses a certified Telecommunications Relay Service to contact patients with hearing or speech impairments, is the Relay Service a business associate of the doctor?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #500 (Apr. 6, 2004), *https://www.hhs.gov/hipaa/for-professionals/faq/500/is-a-relay-service-a-business-associate-of-a-doctor/index.html.*

[365] *See* 45 CFR 164.512(k).

[366] *See* sec. 262 of HIPAA, Public Law 104–191, 110 Stat. 2024 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d–1(c)(2)(B)(i)).

[367] *See* sec. 262 of HIPAA, Public Law 104–191, 110 Stat. 2024 (Aug. 21, 1996) (codified at 42 U.S.C.

have been developed, adopted, or modified by a standard setting organization [368] does not apply with respect to standards for the privacy of IIHI because no standard setting organization has developed, adopted, or modified such standards.

In accordance with 42 U.S.C. 1320d–1(c)(3) and (g), and 42 U.S.C. 1320d–2 note, the Department has consulted with the National Uniform Billing Committee, the National Uniform Claim Committee, the Workgroup for Electronic Data Interchange, the American Dental Association, NCVHS, the Attorney General, appropriate Federal and state agencies and private entities before adopting or modifying the standards relating to the privacy of IIHI.[369] Also, as required by 42 U.S.C. 1320d–1(f), the Department has relied on the recommendations of NCVHS in its development of this final rule.[370]

IV. Summary of Final Rule Provisions and Public Comments and Responses

The Department provides this section-by-section description of the final rule.

A. Individual Right of Access

General Policy Considerations

As discussed in the 2021 Privacy Rule NPRM and above, the ability of individuals to access and direct disclosures of their own health information, including PHI, is key to care coordination. Section 164.524 of the Privacy Rule generally requires most covered entities [371] to provide individuals, upon request, with access to their PHI in a designated record set [372] maintained by or for the covered entity. Business associates are not directly liable for most provisions of the right of access, including the right of access to direct.[373] However, they are contractually liable for all other Privacy Rule obligations that are included in their business associate agreements.[374] While many covered entities may delegate the responsibility for responding to access requests on their behalf to a business associate, the covered entity remains responsible for ensuring that its obligations under the right of access, including the right of access to direct, are met.[375]

The right of access includes the right to inspect or obtain a copy, or both, of the PHI, and to access the PHI in the form and format requested if readily producible, as well as the right of an individual to direct a covered entity to transmit an electronic copy of PHI in an electronic health record to a person designated by the individual.[376] Individuals have a right to access this PHI for as long as it is maintained by a covered entity, or by a business associate on behalf of a covered entity, regardless of the date the information was created; whether the information is maintained on paper or in an electronic information system [377] onsite, remotely, or archived, subject to certain limitations discussed below; or where the PHI originated (*e.g.,* from the covered entity, another health care provider, the individual). The individual right to inspect PHI in a designated record set, either in addition to obtaining copies or in lieu thereof, requires a covered entity to arrange with the individual a convenient time and place to inspect the PHI. Importantly, the right of access, including the right of access to direct, extends to an individual's personal representative (*i.e.,* someone authorized under state or other applicable law to act on behalf of the individual in making decisions related to health care), with limited exceptions.[378] The right of access excludes psychotherapy notes [379] and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[380] However, the right of access does include the underlying PHI from the individual's designated record set (*i.e.,* medical, payment, or other records that are used to generate the types of records that are not subject to the individual's right of access).[381] The right of access does not require a covered entity to create new information, such as explanatory materials or analyses, that does not exist already in the designated record set.[382]

Under certain limited circumstances, a covered entity may deny an individual's request for access to all or a portion of the PHI requested.[383] In some of these circumstances, an individual has a right to have the denial of an access request reviewed by a licensed health care professional designated by the covered entity who

1320d(7)); 45 CFR 160.103 (definition of ''Standard'').

[368] *See* sec. 262 of HIPAA, Public Law 104–191, 110 Stat. 2024 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d(8)); 45 CFR 160.103 (definition of ''Standard setting organization'').

[369] *See* sec. 262 of HIPAA, Public Law 104–191, 110 Stat. 2024 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d–1(c)(2)(B)(i)); sec. 264(d) of HIPAA, Public Law 104–191, 110 Stat. 2034 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d–2 note).

[370] *See* sec. 262 of HIPAA, Public Law 104–191, 110 Stat. 2024 (Aug. 21, 1996). NCVHS was convened virtually on Apr. 16, 2026, and among other things, unanimously recommended that the Secretary adopt the 2021 Privacy Rule NPRM ''consistent with documenting the proposed disclosure expansions to comply with HIPAA's minimum necessary [standard], [. . .] HITECH [. . .] Act of 2009 access rights, and other specific federal safeguards.'' *See* ''Meeting Minutes,'' National Committee on Vital and Health Statistics, U.S. Department of Health and Human Services (Apr. 16, 2026), *https://www.cdc.gov/faca/media/pdfs/2026/07/NCVHS-Public-Committee-Meeting-Summary-04.16.26.pdf.*

[371] The term ''covered entity'' includes health plans, health care clearinghouses, and most health care providers. *See* 45 CFR 160.103 (definition of ''Covered entity''). Health care clearinghouses are not subject to the same individual access requirements as health plans and covered health care providers. *See* 45 CFR 164.500(b)(1).

[372] *See* 45 CFR 164.501 (definition of ''Designated record set''). A designated record set may include records from multiple disparate systems and include records across an individual's lifespan, to the extent that they are maintained by or for the covered entity, which may be linked by a master patient index.

[373] *See* section 13404 of the HITECH Act, Public Law 111–5, 123 Stat. 264 (Feb. 17, 2009) (codified at 42 U.S.C. 17934); 45 CFR 164.502(a)(4)(ii); *see also* 78 FR 5566, 5598–99 (Jan. 25, 2013); ''Direct Liability of Business Associates,'' *supra* note 113.

[374] 78 FR 5566, 5591–92 (Jan. 25, 2013). We do not refer explicitly to business associates when discussing all provisions of the Privacy Rule that address uses and disclosures by covered entities. Such references are unnecessary because a business associate generally may only use or disclose PHI in the same manner as a covered entity. Therefore, any Privacy Rule limitation on how a covered entity may use or disclose PHI automatically extends to a business associate. *See id.* at 5597.

[375] However, under the Privacy Rule, a business associate is required to disclose PHI to the covered entity or, when specified in the business associate agreement, to the individual or individual's designee, as necessary to satisfy a covered entity's obligations under the right of access, including the right of access to direct, with respect to an individual's request for ePHI. Accordingly, a business associate is directly liable under the Privacy Rule if it fails to provide the covered entity, the individual, or the individual's designee (as dictated by the business associate agreement) with access to a copy of the ePHI required to satisfy individual's access request (or with respect to the right of access to direct, an electronic copy of the PHI in an electronic health record). *See* 45 CFR 164.502(a)(4)(ii); 78 FR 5566, 5598–99 (Jan. 25, 2013).

[376] In accordance with the court order in *Ciox,* the Department has not been enforcing a right of access to direct, to a person designated by the individual, non-electronic copies of PHI or copies of PHI that are not in an electronic health record. These types of disclosures continue to be permitted with a valid authorization or under another applicable Privacy Rule permission.

[377] *See* 45 CFR 164.304 (definition of ''Information system'').

[378] *See* 45 CFR 164.502(g) and 164.524(a)(3)(iii). Thus, where we use the term ''individual'' when discussing the right of access throughout this document, the term includes personal representatives.

[379] *See* 45 CFR 164.524(a)(1)(i); *see also* 45 CFR 164.501 (definition of ''Psychotherapy notes'').

[380] *See* 45 CFR 164.524(a)(1)(ii).

[381] *See* 65 FR 82462, 82554 (Dec. 28, 2000); *see also* 45 CFR 164.501 (definition of ''Designated record set''); ''Does an individual have a right under HIPAA to access more than just test results from a clinical laboratory?,'' U.S. Department of Health and Human Services, Office for Civil Rights (June 24, 2016), *https://www.hhs.gov/hipaa/for-professionals/faq/2049/does-an-individual-have-a-right-under/index.html.*

[382] *See* 79 FR 7290, 7303 (Feb. 6, 2014).

[383] *See* 45 CFR 164.524(a)(2) and (3).

did not participate in the original decision to deny the request.[384]

Despite extensive guidance and outreach on the right of access, the Department continues to hear that individuals often encounter barriers to exercising that right. These barriers frequently cause delays in, or denials of, individual access.[385] In addition to adding to the burden on individuals and the health care system, such delays or denials may inhibit care coordination, require duplication of tests and procedures, and contribute to worse health outcomes for individuals.[386]

After careful consideration of responses to the 2018 RFI and the Department's analysis of the Privacy Rule, we proposed to amend the Privacy Rule to strengthen the individual right of access and to remove barriers that may limit or discourage coordinated care or case management among covered entities and individuals, or that otherwise may impose regulatory burdens. Additionally, consistent with the court's decision in *Ciox,*[387] the Department proposed to modify aspects of the individual's right of access to direct.

Summary of Proposals To Modify the Individual Right of Access

The Department proposed to amend the individual right of access by incorporating definitions into the Privacy Rule that support the implementation of certain provisions of the HITECH Act by ensuring clarity. The proposed definitions for electronic health record and personal health application in 45 CFR 164.501 would build on language from the HITECH Act definitions of electronic health record [388] and personal health record.[389] We also proposed to strengthen the individual right of access by strengthening the right to inspect and obtain copies of PHI and by shortening the time limits for covered entities to respond to access requests. Additionally, the Department addressed requirements regarding the form and format in which covered entities must respond to individuals' requests for access by proposing to clarify that a ''readily producible'' copy of PHI would include a copy of ePHI requested through a secure, standards-based API using an app chosen by the individual, as well as a copy in any form and format required by applicable state and other laws. The Department also proposed that the individual right of access to direct a copy of PHI to a person designated by the individual be limited to a right to direct an electronic copy of PHI in an electronic health record to a person designated by the individual. To clearly distinguish between the scope and requirements of the individual right to inspect and obtain copies of PHI and the right of access to direct, the Department proposed to list these distinct rights of access in separate paragraphs in the regulatory text:

- The individual right to inspect and obtain copies of PHI within the current rule requires covered entities to provide the requested information (with some exceptions) within a specific time limit and allows covered entities to charge a limited fee for copies of such information. The 2021 Privacy Rule NPRM proposed to strengthen the individual right to inspect a copy of PHI at proposed 45 CFR 164.524(a)(1)(ii), while retaining the implementation specifications for the individual rights to inspect and obtain copies of PHI at 45 CFR 164.524(c).
- The right of an individual to direct the transmission of electronic copies of PHI in an electronic health record to a person designated by the individual is established by the HITECH Act and interpreted by the *Ciox* decision to apply only to PHI in an electronic health record. The Department proposed to codify the right of access to direct, with the *Ciox* limits, into regulatory text at 45 CFR 164.524(d).
- As part of the right of access to direct, the Department also proposed to create a pathway for individuals to direct the sharing of an electronic copy of PHI in an electronic health record among covered health care providers and health plans. The NPRM proposed to require a covered health care provider or health plan (''Requestor-Recipient''), at the individual's direction, to submit the individual's access request regarding their own ePHI to another covered health care provider (''Discloser''), requesting that the Discloser transmit the ePHI maintained by or on behalf of the Discloser in its electronic health record to the Requestor-Recipient.

Finally, with respect to fees charged by covered entities to individuals exercising the right of access, the Department proposed to adjust and clarify the fees that covered entities may charge for copies of PHI and require covered entities to provide advance notice of approximate fees for copies of PHI requested under the right of access or with an individual's valid authorization. The Department also proposed technical clarifications to the Privacy Rule provision requiring business associates to disclose PHI as needed for the covered entity to fulfill its obligations under the right of access.

1. Adding Definition of ''Electronic Health Record''

a. Issues To Address

Section 13405(e)(1) of the HITECH Act added a new right within the individual right of access that requires covered entities to transmit an electronic copy of PHI in an electronic health record to a person designated by an individual when directed to do so by the individual [390] and codified a definition of electronic health record that specifically applies to that Act's privacy and security provisions for regulated entities.[391] The HITECH Act defines ''electronic health record'' as ''an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.'' [392] However, the Privacy Rule currently does not define the term ''electronic health record.''

b. Proposed Rule

Accordingly, to effectively implement this right, discussed in greater detail below, the Department proposed to add a definition of electronic health record

[384] *See* 45 CFR 164.524(a)(3).

[385] *See* 86 FR 6446, 6459 (Jan. 21, 2021); *see also* Press Release, ''Four HIPAA Enforcement Actions Hold Healthcare Providers Accountable With Compliance,'' Office for Civil Rights, U.S. Department of Health and Human Services (Mar. 28, 2022), *https://www.hhs.gov/about/news/2022/03/28/four-hipaa-enforcement-actions-hold-healthcare-providers-accountable-with-compliance.html;* Press Release, ''HHS' Office for Civil Rights Settles HIPAA Right of Access Investigation with Concentra, Inc.,'' Office for Civil Rights, U.S. Department of Health and Human Services (Dec. 16, 2025), *https://www.hhs.gov/press-room/ocr-settles-with-concentra.html;* Press Release, ''HHS' Office for Civil Rights Settles HIPAA Right of Access Investigation with Azul Vision, Inc.,'' Office for Civil Rights, U.S. Department of Health and Human Services (Aug. 27, 2026), *https://www.hhs.gov/press-room/hhs-ocr-settles-hipaa-investigation-with-azul-vision.html.*

[386] *See, e.g.,* The Joint Commission, ''Safe Informed Care,'' *https://digitalassets.jointcommission.org/api/public/content/91d0580a0ff243099480e9bb48718cae?v=c0f3b5c2* (discussing National Performance Goal #7, providing safe and informed care to all patients, including the importance of ensuring patients receive information about their care to improve health outcomes); Dalia Alomar, et. al., ''The Impact of Patient Access to Electronic Health Records on Health Care Engagement: Systematic Review,'' Journal of Medical internet Research (Nov. 20, 2024), *https://pmc.ncbi.nlm.nih.gov/articles/PMC11618012/.*

[387] *Ciox,* 435 F. Supp. 3d at 38.

[388] 42 U.S.C. 17921(5) (definition of ''Electronic health record'').

[389] *Id.* at 17921(11) (definition of ''Personal health record'').

[390] *See* sec. 13405(e) of the HITECH Act, 123 Stat. 264 (Feb. 17, 2009) (codified at 42 U.S.C. 17935(e)).

[391] *See* sec. 13400(5) of the HITECH Act, 123 Stat. 259 (Feb. 17, 2009) (codified at 42 U.S.C. 17921(5)).

[392] *Id.*

in 45 CFR 164.501 that would be consistent with the HITECH Act definition. We also proposed, as part of the definition, to clarify some of the terms used within the definition that are not defined in the statute or the Privacy Rule.

For example, as we discussed in the 2021 Privacy Rule NPRM, the Privacy Rule does not define the term ''clinician,'' and the Department has not identified a uniform statutory or regulatory definition of the term. To minimize uncertainty about the scope of the term for purposes of the Privacy Rule, we explained that we intended to interpret ''authorized health care clinicians and staff'' to at least include covered health care providers who are able to access, modify, transmit, or otherwise use or disclose PHI in an electronic health record, and who have direct treatment relationships with individuals; and members of their workforce [393] who support the provision of such treatment by virtue of their qualifications or job role. Thus, under this interpretation, an electronic health record would include electronic records consulted by any covered health care provider, or a workforce member of such a covered health care provider, so long as the provider has a direct treatment relationship with individuals. The Department did not propose specifically to include covered health care providers who have indirect treatment relationships [394] with individuals.

With respect to the types of information in an electronic health record, the Department proposed to equate ''health-related information on an individual'' with the scope of the familiar, defined term, ''individually identifiable health information.'' [395] We also proposed to interpret the term ''health-related information'' as equating to the Privacy Rule's definition of ''health information.'' [396] Further, the Department proposed to interpret ''on an individual,'' to refer to information that is ''individually identifiable.''

c. Overview of Comments

Several commenters expressed support for the Department's proposed definition of an electronic health record. Many commenters urged us to adopt a common definition of electronic health record for the various components of the Department. Some commenters expressed concerns about the proposal to limit the definition of electronic health record to apply only where a health care provider has a direct treatment relationship with individuals because they asserted that health care providers who have an indirect treatment relationship with individuals also maintain electronic health records that contain PHI to which individuals should have access. Some commenters expressed opposition to the Department's proposal to equate ''health-related information'' to the Privacy Rule's definition of ''health information'' because it would include both clinical and non-clinical data.

d. Final Rule

The final rule adopts the new term ''electronic health record'' and its definition with two modifications. Consistent with the statutory definition, we are not including the word ''their'' in the definition. Thus, the definition will refer to ''authorized health care clinicians and staff.'' Additionally, we are modifying our interpretation of ''authorized health care clinicians'' specifically to include health care providers that have indirect treatment relationships with individuals. As we explained in the 2021 Privacy Rule NPRM, health care providers who have indirect treatment relationships generally deliver health care based on the orders of another health care provider.[397]

In the 2021 Privacy Rule NPRM, we also explained that we believed that the direct treatment provider would be the entity documenting information about services, products, or reports provided by an indirect treatment provider, and thus it would be appropriate to limit our interpretation of clinicians to direct treatment providers. However, we are persuaded by commenters that a health care provider who has an indirect treatment relationship with an individual may not provide all of their services, products, or reports to the health care provider who has the direct treatment relationship with the individual. For example, providers who furnish durable medical equipment (DME) generally do not provide all of the data recorded by the DME to the ordering health care provider. The same is true of providers of medical devices. And while clinical laboratories may send laboratory reports to the ordering clinician, the reports may not include every single lab value in their documentation. Thus, PHI in the electronic health record of the provider who has the direct treatment relationship may not include all of the PHI created by an indirect treatment provider. If our interpretation of clinicians is limited to only those providers with direct treatment relationships with individuals, the PHI to which an individual would be entitled to direct to a person they designate is thereby limited. Additionally, according to several commenters, distinguishing between health care providers with direct treatment relationships with individuals and those with indirect treatment relationships would create uncertainty about the scope of PHI included in the right of access to direct because direct and indirect treatment providers may create, receive, maintain, and transmit PHI in the same electronic health record. By including both health care providers with direct treatment relationships with individuals and those with indirect treatment relationships, we eliminate this uncertainty and maximize the amount of PHI included within the right of access to direct. Accordingly, the Department is modifying our interpretation of ''clinicians'' to include both health care providers that have a direct treatment relationship with individuals and health care providers that have an indirect treatment relationship with individuals.[398]

The HITECH Act does not define an electronic health record to mean a specific electronic information system, application, or software; rather, it defines it as an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.[399] Thus, whether information is part of an electronic health record is not dependent on the particular system, application, or place in which the information is maintained, but rather on whether it is health-related information about an individual and on who creates, gathers, manages, and consults it. For example, an electronic record maintained by a business associate for, or on behalf of, a covered entity may be part of the covered entity's electronic health record if the record otherwise meets the definition.

Accordingly, the scope of information included in an individual's electronic health record may vary across different health care providers because covered health care providers have substantial

[393] *See* 45 CFR 160.103 (definition of ''Workforce'').

[394] *See* 45 CFR 164.501 (definition of ''Indirect treatment relationship'').

[395] *See* 45 CFR 160.103 (definition of ''Individually identifiable health information'').

[396] *See* 45 CFR 160.103 (definition of ''Health information'').

[397] *See* 45 CFR 164.501 (definition of ''Indirect treatment relationship'').

[398] *Id.*

[399] *See* sec. 13400(5) of the HITECH Act, 123 Stat. 259 (Feb. 17, 2009) (codified at 42 U.S.C. 17921(5)).

flexibility in determining the appropriate composition of that electronic health record for their particular circumstances. Additionally, because the definition includes the term ''record,'' [400] which covered entities already understand from the definition of designated record set, this new definition is clear and workable. Accordingly, this definition is intended to provide a clear standard that health care providers can use to identify what PHI is subject to requirements of the HITECH Act that address PHI in an electronic health record. We believe that this new definition will improve understanding of whether certain aspects of a covered entity's electronic records are included in an electronic health record, which will enable a covered entity to assess whether such ePHI is subject to the right of access to direct.

For example, an electronic health record includes the work product of health care providers that have indirect treatment relationships with individuals, such as electronic lab test reports created by workforce members of a large health system who are licensed clinical laboratory personnel, and who perform clinical lab tests for patients treated by the health system. An electronic health record also includes electronic images taken by an imaging technician who is a workforce member of a radiology group practice and electronic reports of a pathologist who is employed by a small hospital where the reports contain the pathologist's analysis of tissue samples taken from an individual. Electronic billing records created, gathered, managed, and consulted by workforce members of a covered health care provider that has a direct treatment relationship with an individual (*e.g.,* a hospital) are included in the term electronic health record because health care billing information is health-related information.[401] Consistent with the modification we are making to the proposed definition, electronic billing records created, gathered, managed, and consulted by workforce members of a covered health care provider that has an indirect treatment relationship with an individual (*e.g.,* an independent clinical laboratory or single specialty radiology practice) also are included in an electronic health record.

e. Response to Public Comments

Comment: Several commenters expressed support for the Department's proposed definition of an electronic health record. One commenter expressed support for the proposal because they believed that the proposed definition would include all ePHI. Another commenter expressed support because they believed that it would expand upon and align with the way the term is used by health care providers. One commenter recommended that the Department define electronic health record as broadly as possible.

Many commenters expressed opposition to the proposal because they believed that it would be overly inclusive. Several commenters asserted that the proposed definition would not align with the common industry definition of an EHR; instead, according to some commenters, the proposed definition would better align with the definition of ''health information technology.'' Many commenters recommended that the Department limit the definition to one that would be consistent with the HITECH Act. Many also expressed concern that the proposed definition would include non-clinical information, such as billing records, that often is maintained separately from clinical information. According to commenters, combining information that is maintained in separate electronic information systems would be burdensome. One commenter asserted that billing records should be considered as part of an electronic health record only to the extent that such records are included in a designated record set. Another commenter stated that state law may prevent covered entities from disclosing personally identifiable information in billing records. Several commenters requested that the Department exclude certain types of information from the definition or clarify whether certain types of information would be included in the definition.

Response: The Department is finalizing its proposed definition of electronic health record with minimal modifications, as described above. The definition that we are adopting for the Privacy Rule is consistent with the HITECH Act, which provides a definition of electronic health record that applies specifically to the provisions that address the privacy and security of PHI. As explained above, that HITECH Act definition is ''an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.'' Where the HITECH Act did not specifically define terms used in the definition, we rely upon existing definitions of similar terms. For example, while the HITECH Act does not define ''health-related information on an individual,'' section 13101 of the HITECH Act defines ''health information'' by reference to section 1171(4) of the SSA,[402] in a manner that is consistent with the definition of the term contained in the Privacy Rule. Thus, we believe that it is reasonable to interpret the term ''health-related information'' to be at least as broad as ''health information.'' [403] As we explained in the 2021 Privacy Rule NPRM, ''health information'' includes not only clinical, but also billing and other data. Accordingly, the broader term ''health-related information'' could be expected to include such data and not be limited to clinical data.

We understand that other components of the Department may have adopted a variety of definitions of electronic health record or similar terms, such as ''certified EHR technology'' [404] or ''qualified electronic health record.'' [405] These terms also are defined in the HITECH Act. However, these definitions occur in Subtitle A of the HITECH Act, ''Promotion of Health Information Technology,'' and are codified in a new title (''Health Information Technology and Quality'') in the PHSA at 42 U.S.C. 300jj, while the definition of ''electronic health record'' is codified in 42 U.S.C. 17921 and occurs in Subtitle D of the HITECH Act, ''Privacy,'' the same subchapter that establishes the right of access to direct.[406]

Because Congress adopted a different term and definition for purposes of the HITECH Act's privacy and security provisions, the rule of statutory

[400] *See* 45 CFR 164.501 (definition of ''Designated record set'').

[401] *See* Kelly Devers, et al., ''The Feasibility of Using Electronic Health Data for Research on Small Populations,'' Urban Institute (prepared for the Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services) (Sept. 2013), *https://aspe.hhs.gov/report/feasibility-using-electronic-health-data-research-small-populations.*

[402] *See* sec. 13101 of the HITECH Act, Public Law 111–5, 123 Stat. 228 (Feb. 17, 2009) (adding sec. 3000(4) to the PHSA, codified at 42 U.S.C. 300jj(4) (definition of ''Health information'' by reference to sec. 1171(4) of the SSA, codified at 42 U.S.C. 1320d(4)). Section 1171 was added to the Social Security Act by HIPAA.

[403] *See* 45 CFR 160.103 (definition of ''Health information'').

[404] Sec. 13101 of the HITECH Act, Public Law 111–5, 123 Stat. 228 (Feb. 17, 2009) (amending 42 U.S.C. 300jj) (definition of ''Certified EHR technology'').

[405] Sec. 13101 of the HITECH Act, Public Law 111–5, 123 Stat. 229 (Feb. 17, 2009) (amending 42 U.S.C. 300jj) (definition of ''Qualified electronic health record'').

[406] Sec. 13400(5) of the HITECH Act, Public Law 111–5, 123 Stat. 259 (Feb. 17, 2009) (codified at 42 U.S.C. 17921(5)) (definition of ''Electronic health record''); sec. 13405(e) of the HITECH Act, Public Law 111–5, 123 Stat. 264, 268 (Feb. 17, 2009) (codified at 42 U.S.C. 17935(e)) (''Access to certain information in electronic format'').

interpretation against surplusage (generally, a presumption that every clause and word in a statute should be given meaning and not be superfluous) guides us to interpret electronic health record as meaning something different in the context of the HIPAA Rules.[407] As discussed above, ''electronic health record'' is defined in the HITECH Act as ''an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.'' While both ''electronic health record'' and ''qualified electronic health record'' use the term ''an electronic record of health-related information on an individual,'' the latter definition is then arguably limited by additional descriptors:

> [E]lectronic record of health-related information on an individual that—(A) includes patient demographic and clinical health information, such as medical history and problem lists; and (B) has the capacity—(i) to provide clinical decision support; (ii) to support physician order entry; (iii) to capture and query information relevant to health care quality; and (iv) to exchange electronic health information with, and integrate such information from other sources.[408]

The definition of ''electronic health record,'' moreover, does not reference ''certified EHR technology'' (which is defined in part as a ''qualified electronic health record that is certified pursuant to section 3001(c)(5)'' and is, thus, also arguably limited).[409] In addition, the ''health-related information on an individual'' ''is created, gathered, managed, and consulted'' not only by ''authorized health care clinicians,'' but also by ''staff,'' which suggests that the electronic record would not be limited to clinical health information, but also would include information that nonclinical staff create, gather, manage, and consult, such as scheduling, prior authorization, referrals, billing, and other administrative information. Based on the statutory definition of ''electronic health record'' (and how it differs from the definitions of those other terms), we believe that Congress intended for electronic health record, when used in the context of the individual right of access, to refer to an electronic record of an individual's health, rather than a file about an individual in a specific system or technology, and we have interpreted it accordingly.

We clarify that, while the definition of an electronic health record may include PHI that is not part of the designated record set, as discussed below, the right of access, including the right of access to direct, does not extend to such information. Also, as discussed in detail below, it does not extend to psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[410]

Regulated entities are required to identify and document which records are part of the designated record set.[411] For example, clinical laboratory test reports become part of the laboratory's designated record set when they are ''complete,'' which means that all results associated with an ordered test are finalized and ready for release. However, other information concerning the test may be part of the designated record set, and thus accessible to the individual even if the test report has not yet been completed, such as test orders, ordering provider information, billing information, and insurance information.[412]

The definition of electronic health record, like the definition of designated record set, is not dependent on a specific type of system or technology platform or where an organization maintains the information, with the caveat that PHI that is in an electronic health record necessarily is maintained electronically (and, thus, it is ePHI). Accordingly, an electronic health record is not limited to clinical data, but also includes billing and other non-clinical information about the individual. This interpretation is consistent with the scope of the term ''record'' within the definition of ''designated record set.'' [413]

Comment: A few commenters expressed opposition to the Department's proposal to define an electronic health record because they believed that the definition should focus on the information to be protected, rather than the technology used to create, receive, maintain, or transmit the information. One commenter asserted that the Department did not have the authority to interpret the statutory definition. One commenter recommended that the Department adopt a definition that complies with the *Ciox* decision, but that also requires a covered entity to provide—in response to a request from an individual to direct a covered entity to send an electronic copy of PHI in an electronic health record to a person designated by the individual—PHI that is similar in content and extent to the ePHI that the covered entity would be required to provide in response to an individual's request to obtain a copy of their PHI.

Response: As discussed above, the Department is adopting a definition of electronic health record to clarify the scope of the right of access to direct. The definition of electronic health record that we are codifying at 45 CFR 164.501 is consistent with the HITECH Act's definition of the term [414] and the *Ciox* decision. It includes additional language intended only to clarify the terms of the definition for consistency with terms already defined in the HIPAA Rules. The protections provided by the Privacy Rule for PHI are not dependent upon the manner or form and format in which PHI is created, received, maintained, or transmitted, and that remains unchanged by this final rule. Individuals have a right to access PHI in a designated record set, with limited exception. As discussed below, to the extent PHI is within the scope of the individual right of access (including being in the designated record set) and is in an electronic health record, as defined herein, the PHI is within scope of the right of access to direct.

Comment: More than half of the commenters urged us to adopt a common regulatory framework with one set of definitions to be used across the Department because they believed that having different definitions would be burdensome or confusing for regulated entities. One commenter urged the Department to incorporate the term ''electronic health information'' into the definition of electronic health record to

[407] The canon of statutory construction against surplusage supports giving effect to every word and clause in a statute and a reluctance to finding statutory terms to be duplicative or unnecessary. *See* ''Canons of Construction: A Brief Overview,'' Congressional Research Service (May 9, 2025), *https://www.congress.gov/crs-product/IF12992.*

[408] Sec. 13101 of the HITECH Act, Public Law 111–5, 123 Stat. 229 (Feb. 17, 2009) (adding sec. 3000(13) of the PHSA, codified at 42 U.S.C. 300jj).

[409] *Id.*

[410] *See* 45 CFR 164.524(a)(1)(i) and (ii).

[411] 45 CFR 164.524(e); *see also* 65 FR 82462, 82558 (Dec. 28, 2000).

[412] *See* 79 FR 7290, 7295 (Feb. 6, 2014). There is no requirement in the Privacy Rule that clinical laboratories interpret test results for patients. An individual has a right under the Privacy Rule merely to inspect or receive a copy (or direct the copy to a designated person), upon request, of the completed test reports (as well as other information in the designated record set) maintained by a laboratory that is a covered entity. Laboratories may continue to refer patients with questions about the test results back to their ordering or treating providers. However, while not required, a laboratory providing a test report to an individual that has requested access to the report may also provide educational or explanatory materials regarding the test results to individuals if it chooses to do so. Similarly, a laboratory that wishes to include a disclaimer, caveat, or other statement explaining the limitations of the laboratory data for diagnosis or treatment or other purposes may do so. *See* 79 FR 7290, 7303 (Feb. 6, 2014).

[413] *See* 45 CFR 164.501 (definition of ''Designated record set'').

[414] *See* sec. 13400(5) of the HITECH Act, Public Law 111–5, 123 Stat. 259 (Feb. 17, 2009) (codified at 42 U.S.C. 17921(5)) (definition of ''Electronic health record'').

clarify how the proposed definition relates to the information blocking regulations.

Response: We understand that other components of the Department may have adopted a variety of definitions of electronic health record or similar terms; however, we do not have the statutory authority to adopt such definitions here. The definition that we are adopting for the Privacy Rule is consistent with the HITECH Act, which specifically provides a definition of electronic health record that applies to the provisions that address the privacy and security of PHI. We do not believe that this definition conflicts with other laws. Rather, this definition supports the Department's goals of implementing the statutory right of individuals to direct an electronic copy of their PHI in an electronic health record to a person they designate as part of the right of access and enhancing care coordination and case management. Ensuring that individuals can access their PHI and direct such access to others is critical to monitoring various health conditions and improving patient health outcomes.[415] We decline to incorporate the term ''electronic health information'' [416] into the definition of electronic health record. The definition of EHI references definitions codified in the HIPAA Rules, such as ePHI; thus, incorporating EHI into a definition in the Privacy Rule is unnecessary and likely to increase confusion.

Comment: Commenters provided a variety of comments on the relationship between the definitions of electronic health record and designated record set. Several commenters recommended that the Department align the definition of electronic health record with the definition of ''designated record set'' to avoid confusion, to promote clarity, and to align it with the right of access. In contrast, several commenters recommended that the Department not align the definitions of electronic health record and designated record set because they believed that we lacked the statutory authority to do so and it would create confusion. A few commenters recommended that the Department provide additional guidance on the scope of the designated record set. One commenter recommended that the Department add a definition of ''electronic designated record set,'' rather than aligning the definitions of electronic health record and designated record set, asserting that this alternative approach would avoid confusion. A few commenters stated that the definition of electronic health record should be broader than the designated record set because an electronic health record could include PHI that is not part of the designated record set.

Response: The definition of electronic health record in 45 CFR 164.501 is consistent with the HITECH Act's definition that applies to its privacy and security provisions,[417] and includes additional language intended only to clarify the terms of the definition for consistency with terms defined in the HIPAA Rules. We agree with commenters that the right of access to direct should not extend to PHI about the individual that is outside of any designated record set. As discussed below, we are adopting modifications to clarify this within the right of access to direct at 45 CFR 164.524(d).

Comment: A few commenters recommended that the Department interpret the definition of electronic health record using existing terms from the HIPAA Rules to avoid confusion.

Response: We agree with the commenters that relying on existing terms, where appropriate, can help regulated entities better understand new obligations. Thus, we have relied upon existing terms to interpret the HITECH Act's definition of electronic health record to the extent possible and consistent with the statute.[418]

Comment: Some commenters requested that the Department clarify whether the proposed definition would apply only to covered health care providers or also to health plans.

Response: As explained above, an electronic health record is an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. We interpret ''authorized health care clinicians and staff'' to include health care providers who are able to access, modify, transmit, or otherwise use or disclose PHI in an electronic health record. This includes health care providers that have a direct or indirect treatment relationship with individuals,[419] as well as members of the health care provider's workforce [420] who support the provision of treatment. Thus, we intend for the definition of electronic health record to apply broadly, including to electronic records maintained by health care providers and, where applicable, health plans. Where a health plan is integrated with one or more covered health care providers, electronic records created, gathered, managed, and consulted by authorized health care clinicians and staff of those providers may constitute an electronic health record. A health plan's maintenance of claims, enrollment, utilization management, payment, or other administrative records does not, by itself, cause those records, or the electronic information system in which they are maintained, to constitute an electronic health record. Similarly, consultation of such records by a clinician or other professional employed by the health plan does not, by itself, cause the records to constitute an electronic health record.

Furthermore, the application of the definition in this final rule is limited by the scope of the right of access to direct, which is discussed elsewhere in this final rule.

Comment: One commenter requested that the Department clarify the scope of ''health-related information'' to reflect the current understanding of activities that are part of health care, such as information about activities to address the social determinants of health and interactions between individuals and unlicensed workforce members and volunteers. A few commenters recommended that ''health-related information'' include information about the price of health care. Another commenter recommended that the Department limit ''health-related information'' to clinical information that is electronically maintained in a designated record set.

Response: As discussed above, while the HITECH Act does not define ''health-related information on an individual,'' the Privacy Rule defines ''health information'' [421] in a manner that is consistent with the definition of

[415] *See* ''Privacy & Security,'' sec. 7 of the Health IT Playbook, Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Mar. 11, 2020), *https://playbook.healthit.gov/playbook/privacy-and-security/; see, e.g.,* The Promise of Patient Portals for Individuals Living with Chronic Illness: Qualitative Study Identifying Pathways of Patient Engagement,'' *supra* note 166; Elettra Carini, et al., ''The Impact of Digital Patient Portals on Health Outcomes, System Efficiency, and Patient Attitudes: Updated Systematic Literature Review,'' Journal of Medical Internet Research (Sept. 8, 2021), *https://www.jmir.org/2021/9/e26189/.*

[416] *See* 45 CFR 171.102 (definition of ''Electronic health information'').

[417] *See* sec. 13400(5) of the HITECH Act, Public Law 111–5, 123 Stat. 259 (Feb. 17, 2009) (codified at 42 U.S.C. 17921(5)) (definition of ''Electronic health record'').

[418] *See* 45 CFR 160.103 (definitions of ''Health information'' and ''Individually identifiable health information'') and 45 CFR 164.501 (definition of ''Designated record set'').

[419] *See* 45 CFR 164.501 (definitions of ''Direct treatment relationship'' and ''Indirect treatment relationship'').

[420] *See* 45 CFR 160.103 (definition of ''Workforce'').

[421] *See* sec. 262 of HIPAA, Public Law 104–191, 110 Stat. 2022 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d(4)); *see also* 45 CFR 160.103 (definition of ''Health information'').

the term in section 262 of HIPAA. Thus, we believe that it is reasonable to interpret the term ''health-related information'' to be at least as broad as ''health information.'' [422] As we explained in the 2021 Privacy Rule NPRM, ''health information'' includes not only clinical, but also billing and other data. Accordingly, the broader term ''health-related information'' could be expected to include such data and not be limited to clinical data.

Comment: A few commenters expressed support for the Department's proposal to limit the interpretation of ''authorized clinicians and staff'' to those with a direct treatment relationship to individuals because they believed that it would be consistent with the HITECH Act. A few commenters urged the Department to clarify that the proposed definition would include only the records of direct treatment providers. One commenter expressed opposition to the Department's proposal because they believed that it was overly inclusive and suggested that it should be limited to health care providers responsible for providing direct services, alternative care providers, and allied health professionals.

Several commenters expressed concern that the Department proposed to limit the interpretation of ''authorized clinicians and staff'' to health care providers with a direct treatment relationship to individuals and questioned whether PHI received from providers with indirect treatment relationships would be included in the definition of electronic health record. A few commenters disputed the Department's assumption that PHI provided by indirect treatment providers always would be incorporated into the electronic health record of a direct treatment provider.

Several commenters requested that the Department provide specific examples of ''authorized clinicians.'' One commenter encouraged the Department to adopt a more plain language definition of ''clinician'' because other covered entities are facilitating care coordination at a population-level.

According to one commenter, defining the term ''clinician'' would clarify whether an electronic health record contains information outside of the designated record set.

Response: We are modifying our interpretation of authorized clinicians to include both health care providers that have a direct treatment relationship with individuals and those that have an indirect treatment relationship with individuals. The Department is persuaded by commenters who asserted that PHI that is created, received, maintained, or transmitted electronically by health care providers that have an indirect treatment relationship with individuals may not be integrated into the electronic health record of health care providers that have a direct treatment relationship with individuals. As a result, limiting the interpretation of authorized clinicians to direct treatment providers would narrow the scope of an electronic health record, and thus the right of access to direct, in a way that we did not intend.

We based our proposal on the assumption that all PHI created by an indirect treatment provider is securely and electronically shared with (and thus incorporated into the designated record set of) the referring or ordering direct treatment provider, and by extension, the individual has ready access to the PHI through the direct treatment provider's electronic health records. We understand that in some cases, PHI from an indirect covered health care provider may be incorporated into the direct treatment provider's electronic health record, without the direct treatment provider's involvement. However, we also understand from comments that, in many circumstances, indirect treatment providers create and share PHI with a direct treatment provider, who does not incorporate the PHI into their electronic health record. Additionally, we also understand that in some cases, the direct treatment provider who originally ordered clinical services, products, or reports that are produced by an indirect health care provider may not receive all PHI created by the indirect treatment provider (*e.g.,* PHI used to prepare a report), and thus that such PHI would not be in the designated record set of the direct treatment provider.

For example, radiologists generally have indirect treatment relationships with individuals because they deliver diagnostic services based on the orders of other health care providers (*e.g.,* internists, cardiologists, nephrologists, neurologists, obstetricians/gynecologists), and the results or products of those services (*e.g.,* reports, interpretations, images) typically are available to the individual through the direct treatment provider. The radiologist often sends only a report of their findings to the direct treatment provider, rather than providing them with access to the images upon which the report is based.[423] Individuals may seek to access such images for their records or to share with other health care providers or other persons. In such circumstances, the only option for individuals is to request copies of images directly from the radiologist or imaging center, the indirect treatment provider. Similarly, pathologists and clinical laboratories often are indirect treatment providers and generally are in possession of underlying PHI that may not be provided to direct treatment providers. Thus, individuals may need to obtain such PHI directly from pathologists or clinical laboratories, as well.

As another example, a direct treatment provider may be monitoring an individual's DME (*e.g.,* heart monitor), implantable medical device (*e.g.,* pacemaker), or remote monitoring technology. The provider of the DME generally has the complete set of PHI recorded by the monitors, while the direct treatment provider may be sent only summary information or alerts when monitors are malfunctioning. Individuals and direct treatment providers may require access to such PHI for a complete diagnosis and care plan.

To ensure that individuals have the right of access to direct a covered entity to transmit an electronic copy of the full scope of PHI that is consistent with the statute to a person designated by the individual, we believe that it is necessary and appropriate to specify that the definition of electronic health record applies to both health care providers that have a direct treatment relationship with individuals and those that have an indirect treatment relationship with individuals.

Comment: A few commenters urged the Department to include non-clinical workforce members of health care providers in its interpretation of ''staff.'' A few commenters expressed concern that the addition of ''and staff'' would create ambiguity and cause confusion because it would include non-clinicians.

Several commenters recommended that the Department incorporate role-based access into the proposed definition of electronic health record to clarify who is permitted to create, gather, manage, or consult it because they believed that a definition would need to consider workforce members who do not have a direct treatment relationship with individuals, but who may create, gather, manage, or consult the electronic health record for essential purposes (*e.g.,* payment, health care operations).

[422] *See* 45 CFR 160.103 (definition of ''Health information'').

[423] *See* 91 FR 4054 (Jan. 30, 2026).

Response: We interpret ''staff'' to mean workforce [424] members who support the provision of treatment, either directly or indirectly, by virtue of their qualifications or job role.[425] Thus, an electronic health record would include electronic records consulted by a workforce member of a covered health care provider where the workforce member is supporting the provision of treatment by the health care provider. Examples of workforce members that would be ''staff'' include, but are not limited to, medical residents, registration support personnel, schedulers, receptionists, administrative staff who support covered functions (*e.g.,* billing, prior authorization, scheduling, referrals), coding specialists, clinical laboratory personnel, home health assistants, office or practice managers, and care referral coordinators.

2. Adding Definition of ''Personal Health Application''

a. Issues To Address

Section 164.524(a) of the Privacy Rule currently establishes, with limited exceptions, the right of an individual to inspect or obtain (or both) a copy of their PHI to the extent such information is maintained in a designated record set of a covered entity. An individual's right of access exists regardless of the format in which the PHI is maintained, and the standards and implementation specifications that address individuals' requests for access and timely action by the covered entity (*e.g.,* provision of access, denial of access, and documentation) apply to an electronic environment in a similar manner as they do to a paper-based environment.[426]

b. Proposed Rule

The Department proposed to adopt and define a new term, ''personal health application,'' to support the right of an individual to obtain a copy of their PHI through a personal health app pursuant to the right of access, discussed below.

Under the proposed definition, the information in a personal health app would not be managed, shared, or controlled by a covered entity. Additionally, the information would not be managed by the app developer on behalf of or at the direction of a regulated entity (*e.g.,* a patient or health plan member portal used by a covered entity to manage individuals' access to the PHI it maintains) or another party, such as an entity that is not regulated under HIPAA that collects or manages PHI for its own purposes (*e.g.,* research organization). Instead, under the proposed definition, an individual (or their personal representative) would use a personal health app for the individual's own purposes, such as to monitor their health status and access their health information using the app. As we explained in the 2021 Privacy Rule NPRM, because the developer of a personal health app would not be acting on behalf of, or at the direction of, a regulated entity, the app developer would not be a business associate, and therefore, would not be subject to the federal privacy and security obligations of the HIPAA Rules. Also as described in the 2021 Privacy Rule NPRM, a personal health app would be a tool used by, or primarily for, the individual, as opposed to other health apps that contain information that is managed, shared, and controlled by other persons for their own purposes (*e.g.,* patient or health plan member portal, research). Thus, the proposed definition would have focused on apps where only the individual or their personal representative manages, shares, and controls the information and apps that enable the information to be managed, shared, and controlled primarily for the individual. It would not have included apps where the information is managed, shared, and controlled by or primarily for another party.

c. Overview of Comments

Commenters were evenly split in their views of this proposal. Some urged the Department to adopt a broader definition of personal health app (*e.g.,* including apps on the web, mobile devices, and desktop computers, as well as apps that enable individuals to manage and/or to generate insights from their health information), while others recommended that we adopt a narrower one (*e.g.,* to limit the definition to apps that incorporate certain privacy and security protections). Many commenters requested that the Department provide examples of technologies that would meet the proposed definition.

d. Final Rule

We are finalizing our proposal to adopt the new term, ''personal health application,'' at 45 CFR 164.501, with modifications for clarity and readability. Specifically, we are separating the clauses of the definition into two paragraphs, one that addresses what the term expressly includes and one that addresses what the term expressly excludes. Additionally, we are separating the clause that addresses what the term expressly excludes into two sub-paragraphs and clarifying that an electronic application is not a personal health app if the health information in such application is managed, shared, or controlled: (1) by or primarily for a covered entity; or (2) primarily for another person.

Further, we are removing the example of an app developer from the definition and replacing ''party'' with ''person.'' These modifications are not substantive but are made to align with our preference for providing non-exhaustive lists of examples in guidance, rather than in regulatory text, and using defined terms where possible.[427]

This definition is consistent with, and will help further, the Department's ongoing efforts to promote and support individuals' use of technology to exercise the right of access.[428] Individuals increasingly are choosing to use technology to access and manage their health information. Technology, such as personal health apps, that individuals can select to manage, share, and control their health information, gathered from one or more sources, empowers them to be more in control of decisions about their health and well-being. For example, individuals with access to their health information are better able to monitor chronic conditions, adhere to treatment plans, find and request that errors in their health records be amended, track progress in wellness or disease management programs, and directly contribute their health information to research.[429] With the increasing use of and continued advances in health IT, there are novel and increasing ways for individuals to quickly and easily access

[424] 45 CFR 160.103 (definition of ''Workforce'').

[425] *See* 45 CFR 164.501 (definition of ''Treatment'').

[426] *See* ''The HIPAA Privacy Rule's Right of Access and Health Information Technology,'' Office for Civil Rights, U.S. Department of Health and Human Services (Jan. 17, 2009), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf.*

[427] In the preamble to the NPRM, we stated that we were proposing to define a personal health application as ''an electronic application used by an individual to access health information about that individual in electronic form, which can be drawn from multiple sources, provided that such information is managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer.'' *See* 86 FR 6446, 6457 (Jan. 21, 2021). This statement was in error because the proposed amendatory text did not include the unnecessary words ''in electronic form,'' nor does this final rule.

[428] *See* 78 FR 5566, 5631–32 (Jan. 25, 2013); 75 FR 40868, 40901 (July 14, 2010); 65 FR 82462, 82556–57 (Dec. 28, 2000); ''The HIPAA Privacy Rule's Right of Access and Health Information Technology,'' *supra* note 426.

[429] ''Privacy & Security,'' sec. 7 of the Health IT Playbook, Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Mar. 11, 2020), *https://playbook.healthit.gov/playbook/privacy-and-security/playbook.healthit.gov.*

their health information electronically, in real time, and on demand from a variety of sources. The Privacy Rule was designed to be technology neutral and does not mandate the use of any particular technologies, but instead establishes standards that can be met through a variety of means.[430] This approach enables the Department to address in the preamble how the definition applies to technologies in current use without revising the regulatory text solely to account for each new or developing technology. Accordingly, we decline to provide examples of specific technologies that meet the definition in the regulatory text. Rather, the Department believes that the definition we are finalizing provides flexibility to accelerate innovation,[431] empower individuals, and improve individual access to their PHI, while encouraging competition among technology developers.

While covered entities (and business associates acting for or on behalf of covered entities) may offer individuals the ability to access their PHI and other information using apps developed by or for the covered entities,[432] the information in such apps (*e.g.,* patient and health plan member portals) generally is managed, shared, and controlled by or primarily for those regulated entities.[433] Such entities determine, among other things, who can access the information in their apps, what information can be entered, and what happens to the information that is entered. In contrast, individuals generally make such decisions when it comes to personal health apps, subject to the app's terms and conditions or consumer privacy policy, which the individual generally has the opportunity to review and consider when they determine which app to use. For example, an individual selects the app that they prefer to use, the information that they wish to maintain in the app, and whether they prefer that information gathered from multiple sources be integrated or viewed separately. Thus, by limiting the definition to apps that provide an individual with the ability to manage, share, and control the health information that is in the app and to apps that enable the health information in the app to be managed, shared, and controlled by or primarily for the individual, we ensure that the definition encompasses only apps used by the individual or their personal representative, not other persons. This definition is consistent with how individuals view these technologies and supports individuals' ability to obtain all the PHI to which they are entitled under the right of access using the personal health app of their choosing. In contrast, where an app allows another person (*e.g.,* a medical product company conducting research) to manage, share, and control the individual's health information (but not primarily for the individual), requests from the individual to disclose PHI to the app may constitute a request pursuant to the right of access to direct (and would be subject to that right's limitations), depending on the nature and scope of the request.

A personal health app may not allow an individual to perform all three of the functions included in the definition, that is, manage, share, and control the individual's health information. Thus, the definition also allows for circumstances where one or more of those functions is performed by someone other than the individual (*e.g.,* the developer of a personal health app) primarily for the individual. An app connected to a fitness tracker selected by the individual for their own use generally contains information that is managed, shared, and controlled by or primarily for the individual, and thus, likely would meet the definition of a personal health app. As another example, a wellness app selected by the individual for their own use likely would meet the definition of a personal health app because the information in the app generally is managed, shared, and controlled by or primarily for the individual.

We explicitly exclude, from the definition of a personal health app, such apps that are used by individuals to access their health information where the information is managed, shared, or controlled: (1) by or primarily for a covered entity; or (2) primarily for another person. Because business associates, by definition, are acting for or on behalf of covered entities, the term personal health app excludes apps that contain information that is managed, shared, or controlled by a business associate that is acting as a business associate or a subcontractor of a business associate with respect to the app. Thus, by definition, personal health apps are not entities that are regulated under HIPAA.[434] The same holds true for developers of personal health apps with respect to such apps.[435] While a regulated entity may provide an individual with an app to access the patient or health plan member portal, the information in that app is not managed, shared, and controlled by or primarily for the individual. Rather, the information that resides in the app (generally supplied from the regulated entity's electronic information systems) is managed, shared, or controlled by or primarily for the regulated entity, even though the individual may benefit from it. Similarly, where a fitness tracker is provided to the individual by a covered entity, the developer of the app connected to the fitness tracker likely would be a business associate. Thus, the app would not meet the definition of a personal health app. As another example, while an entity managing clinical trials may provide an individual with an app to collect the individual's health information, the information in that app is not managed, shared, and controlled by or primarily for the individual. Rather, the information in such apps is managed, shared, or controlled primarily for the entity that is conducting the clinical trial for research purposes.

e. Responses to Public Comments

Comment: Several commenters expressed support for the proposed definition of personal health app. According to a few commenters, the proposed definition would enable workforce members to distinguish individual access requests from requests for disclosures that require an authorization. One commenter asserted that adding a definition of personal health app would provide clarity and account for new technologies with

[430] 65 FR 82567 (Dec. 28, 2000).

[431] *See, e.g.,* ''Early Adopters and All Pledgees,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Aug. 6, 2026), *https://www.cms.gov/health-tech-ecosystem/early-adopters.*

[432] Persons who develop apps for or on behalf of covered entities or business associates likely are business associates of the covered entity or subcontractors of the business associate because they likely create, receive, maintain, or transmit PHI on behalf of, or provide certain services involving access to PHI for, covered entities or business associates. Accordingly, such persons generally are regulated under the HIPAA Rules as business associates. *See* 45 CFR 160.103 (definition of ''Business associate); *see also* ''Health App Use Scenarios & HIPAA,'' Office for Civil Rights, U.S. Department of Health and Human Services (Feb. 2016), *https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf.*

[433] We use the term PHI to refer exclusively to information that meets the definition in 45 CFR 160.103. We use the terms ''information'' and ''health information'' to address data that may include PHI and data that does not include PHI.

[434] Personal health apps may be regulated by other law. *See* ''Mobile Health App Interactive Tool,'' Federal Trade Commission and U.S. Department of Health and Human Services (Nov. 2024), *https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool.*

[435] Developers of personal health apps may be regulated under HIPAA as business associates with respect to other products or services that they offer.

minimal effects on the operations of covered entities.

A few commenters recommended that the Department clarify the scope of a personal health app. For example, a few commenters questioned whether the term would include electronic apps that are managed, shared, and controlled by an employer for an individual employee and whether it would apply to online or digital tools, platforms, or services that have the functional capabilities of a personal health app, but are not necessarily considered an app.

Several commenters asserted that the proposed definition would be too narrow. One commenter recommended that the Department expand the proposed definition to include apps on the web, mobile devices, and desktop computers, and apps that enable individuals to manage and/or to generate insights from their health information. One commenter recommended that the Department expand the proposed definition to include any app that offers services to individuals and maintains an individual's health information for their use and to explicitly include the ability to access price information.

A few commenters requested that the Department clarify whether apps recommended by health care providers would be considered personal health apps. One commenter recommended that the Department modify the definition to clarify that a personal health app accesses information for the individual.

A few commenters expressed opposition to the proposed definition because they believed that the Department should rely on the HITECH Act's definition of personal health record. One commenter recommended that the Department use the term ''personal health record'' because not all tools or services selected by individuals to manage and maintain their health information will be apps as the term generally is understood. The commenter provided examples of such tools and services, such as online platforms that are accessible by individuals through an internet browser. One commenter asserted that the Department should use personal health records and personal health apps as examples of forms and formats for individual access, rather than defining the term personal health app.

Response: As explained above, we are finalizing the definition of personal health app with a few modifications. Under this definition, a personal health app is a service offered directly to consumers. It is not a service offered to the individual by a covered entity or its business associate, such as an EHR vendor. Neither the covered entity nor its business associate manages, shares, or controls the information, nor does the app developer manage the information on behalf of or at the direction of a health care provider or health plan (*e.g.,* through a patient portal that the regulated entity uses to manage individuals' access to the PHI it maintains). An electronic application also would not be a personal health app where the app developer manages the information on behalf of or at the direction of another person or where another person collects or manages PHI for its own purposes (*e.g.,* a research organization). Instead, an individual (or their personal representative) uses a personal health app (*e.g.,* Individual Access Services [436] (IAS) provided by an IAS Provider in TEFCA (or other party to TEFCA that offers TEFCA IAS), a ''patient facing app'' [437] that connects to CMS Aligned Networks as a participant in the Medicare App Library,[438] fitness tracker, or wellness app) for the individual's own purposes, such as to monitor their own health status and access their own PHI using the app. For example, an individual might request that their health care providers send weight, vital signs, and other PHI to their chosen personal health app either to store in such app or direct it to others.

As we explained in the proposed rule, the definition of personal health app is similar to the HITECH Act definition of personal health record,[439] but specifically addresses a category of health apps, some of which also may be personal health records to the extent that they meet both definitions.[440]

The definition of personal health app generally is technology neutral, with the caveat that the app must be electronic. Thus, a personal health app may include electronic software, applications, or successor technologies. Using this technology, the individual (or their personal representative) is able to manage, store, and control their health information, gathered from one or more sources, including entities not regulated by HIPAA. These technologies often are described as ''direct-to-consumer,'' ''consumer-directed,'' or ''patient-facing.'' [441] They may include mobile apps, online tools, browsers or browser extensions, platforms, or services that provide individuals with the ability to manage, share, and control their own health information.

Some app developers and other technology developers may offer multiple products, including some that are offered directly to consumers and some that are offered to covered entities to provide to individuals. If a technology developer meets the definition of a covered entity or business associate with respect to a particular product (or, in the case of a hybrid entity, a product is offered through a designated health care component), that particular product or technology is not a personal health app; other products or technologies offered by the technology developer may meet the definition of a personal health app if the individual or their personal representative has the ability to manage, share, and control the health information through that product or technology. Technologies that contain an individual's health information would not meet the definition of a personal health app where the health information is managed, shared, or controlled primarily for a person other than the individual or their personal representative.

Comment: Several commenters recommended that the components of the Department align their definitions of a personal health app. One commenter asserted that the proposed definition would align with the information blocking regulations. A few commenters urged the Department to limit the definition to apps that incorporate certain privacy and security protections and/or standards.

Response: The definition of personal health app that we are finalizing is consistent with definitions of similar terms, such as the HITECH Act definition of personal health record,[442] but is tailored to the HIPAA Privacy Rule. The definition captures certain

[436] *See* definition of ''Individual Access Services (IAS),'' ''Common Agreement for Nationwide Health Information interoperability (Version 2.1),'' Assistant Security for Technology Policy and ONC TEFCA Recognized Coordinating Entity, section 1.1 (Nov. 2024), *https://healthit.gov/wp-content/uploads/2025/02/Common_Agreement_2.1.pdf.*

[437] *See* ''Health Tech Ecosystem Categories,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Aug. 5, 2026), *https://www.cms.gov/health-technology-ecosystem/categories.*

[438] *See* ''Requirements for the Medicare App Library,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (Aug. 24, 2026), *https://www.cms.gov/initiatives/health-technology-ecosystem/overview/medicare-app-library.*

[439] 42 U.S.C. 17921(11) (definition of ''Personal health record'').

[440] The same software could be a personal health app under the Privacy Rule definition and a personal health record under the HITECH Act for other purposes, to the extent it meets both definitions.

[441] *See, e.g.,* ''Early Adopters and All Pledgees,'' *supra* note 431.

[442] *See* 42 U.S.C. 17921(11) (definition of ''Personal health record''); *see also* 16 CFR 318.2 (definition of ''Personal health record'').

health apps, some of which also may be personal health records.

Under HIPAA and subtitle D of the HITECH Act, the Department's statutory authority is limited to covered entities and their business associates. A personal health app developer does not meet the definition of a business associate because it is not acting for, or on behalf of, a covered entity or business associate. Instead, the personal health app is a tool that is employed by or primarily for an individual (or their personal representative) to manage, share, and control the individual's health information. The Privacy Rule does not limit an individual's right of access based on the technology that the individual uses to obtain a copy of their PHI or how the information will be used or disclosed once the individual receives it. For instance, a covered entity is not permitted to deny an individual's right of access to their ePHI, where the individual requests that such access be provided through a personal health app, based solely on the covered entity's concerns that the app developer will not adequately protect the privacy of the individual's ePHI or because the app does not encrypt the individual's data at rest. Accordingly, we decline to limit the definition of personal health app to apps that meet certain privacy and security standards.

Comment: Several commenters asserted that covered health care providers would be unable to confirm who will manage, share, and control the ePHI being transmitted to an app. Several commenters requested that the Department provide guidance, including examples, of how to identify when health information about an individual that is in an app is managed, shared, and controlled by or primarily for the individual.

Response: We recognize that app developers may offer some products directly to consumers and some products to covered entities to provide to individuals. We also are aware that there may be situations where an organization has multiple service offerings that use the same technology platform. Covered entities will need to distinguish between requests for PHI submitted through apps that are personal health apps and those that are not, based on the processes and technology that the covered entity implements to enable apps to connect to a covered entity's electronic information systems and transmit requests for disclosures of PHI, including requests for access. For example, for covered entities that have implemented a Health IT Module certified under the ONC Health IT Certification Program to, for example, the certification criterion at 45 CFR 170.315(g)(10) (''Standardized API for patient and population services''), the health IT developer of that Health IT Module is required to maintain a standardized authentication and application authorization process to register and enable applications for use.[443] Similarly, a covered entity that participates in TEFCA should be able to identify, based on information provided to it through TEFCA, whether a request is submitted by an IAS Provider, and whether the request was submitted by the individual.[444] Based on the processes that a covered entity implements and the information provided by an app, covered entities will need to determine whether a request submitted through an app is a request of an individual exercising his or her right of access through a personal health app and, thus, the appropriate response and compliance posture.

3. Strengthening the Access Right To Inspect and Obtain Copies of PHI

a. Current Rule

The Privacy Rule's individual right of access at 45 CFR 164.524(a) includes an individual's right to inspect their PHI in a designated record set and their right to obtain a copy of that PHI.[445] Covered entities must arrange with an individual for a convenient time and place to inspect the PHI.[446]

b. Proposed Rule

In the 2021 Privacy Rule NPRM, the Department proposed to strengthen the right of an individual to inspect their PHI in a designated record set by making it a separate requirement from the right of an individual to obtain a copy of their PHI in a designated record set and adding more detail. Specifically, we proposed to include, within the right of an individual to inspect their PHI in a designated record set, the right to view, take notes, take photographs, and use other personal resources to capture the information.[447] The Department also proposed to clarify that a covered entity would not be required to allow an individual to connect a personal device to the covered entity's electronic information systems. Additionally, we proposed that a covered entity would be permitted to impose requirements to ensure that the individual's recordings would be limited to only the PHI to which the individual has a right of access.

c. Overview of Comments

Most commenters, regardless of whether they expressed support or opposition, raised concerns about the increased burdens of this proposal, such as the need to develop new policies and procedures to address how to protect the privacy and security of other individuals, workforce members, and EHR systems. Most commenters who expressed opposition to the proposal believed that it would increase risks to patient or workforce safety and create risks for intellectual property rights. Several commenters expressed concern that the proposal would require the dedication of additional resources, such as personnel and space, and interrupt workflows. According to commenters, the proposal was unnecessary because most individuals do not seek to access their PHI in person; rather, they prefer to access their PHI electronically.

d. Final Rule

The Department is not finalizing the proposed modifications to the right to inspect. Although the proposal was intended to reduce requests for covered entities to make copies of PHI, we agree with commenters who asserted that the proposal would be overly burdensome for covered entities to implement. Additionally, the existing right of inspection already permits individuals to inspect their PHI in person at a mutually convenient time and place; it does not preclude inspection from occurring in conjunction with a health care appointment. Further, the

[443] Section 4002(a) of the Cures Act requires certified health IT developers to publish APIs and allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law. It also requires that a certified health IT developer provide through an API access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws. *See* sec. 3001(c)(5) of the PHSA, as amended by sec. 4002(a) of the 21st Century Cures Act, Public Law 114–255, 130 Stat. 1159 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–11); 45 CFR 170.315(g)(10); 45 CFR 170.404(b)(1); *see also* Fact Sheet, ''Promoting an Open and Transparent API Ecosystem: API Conditions and Maintenance of Certification Requirements for Certified API Developers in the ONC Health IT Certification Program,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Nov. 2024), *https://healthit.gov/wp-content/uploads/2025/02/certification-api-condition-responsibilities-obligations-factsheet.pdf.*

[444] *See* definition of ''Individual Access Services Provider (IAS Provider),'' ''Common Agreement for Nationwide Health Information interoperability (Version 2.1)'', Assistant Security for Technology Policy and ONC TEFCA Recognized Coordinating Entity, section 1.1 (Nov. 2024), *https://healthit.gov/wp-content/uploads/2025/02/Common_Agreement_2.1.pdf;* ''Exchange Purpose (XP) Implementation SOP: Individual Access Services (IAS),'' Sequoia Project (Aug. 3, 2026), *https://rce.sequoiaproject.org/wp-content/uploads/2026/07/SOP-IAS-XP-v3_June2026_Clean_-5081.pdf.*

[445] 45 CFR 164.524(a)(1).

[446] *See* 45 CFR 164.524(c)(1)–(3).

[447] *See* proposed 45 CFR 164.524(a)(1)(ii).

Department has not received information or complaints from individuals indicating that they frequently face difficulties when they choose to record their health information using their own resources.

e. Responses to Public Comments

Comment: Several commenters expressed support for this proposal because it would provide individuals with access to their PHI in a way that did not depend on technology. Several commenters asserted that covered entities often deny caregivers access to PHI and that this proposal would provide an individual's caregiver with an easier path towards obtaining [448] access.

Response: The Department agrees that the right of inspection provides an individual or their personal representative with another way of obtaining access to the individual's PHI. Accordingly, we are preserving the right to inspect as it currently exists. Under the right to inspect, an individual or their personal representative may view the individual's PHI in a designated record set at a mutually convenient time and place.[449] The mutually convenient time and place for inspection may occur during a health care appointment, and a health care provider may voluntarily allow an individual (or their personal representative) to take photos or use other resources to view and capture images.

Comment: Some commenters expressed concerns about the ability of covered entities to establish policies and procedures that would enable individuals to exercise the proposed right to inspect their PHI without infringing on the privacy of others, including workforce members, or the security of ePHI in EHR systems. A few commenters asserted that individuals should not have access to the electronic information technology systems of covered entities.

Other commenters recommended that the Department require individuals to obtain permission before recording conversations with health care providers. Commenters also expressed concerns about the effect of the proposed change on legal protections for intellectual property and the intersection between this proposal and Federal or state recording laws.

Response: Although the Department is not finalizing the proposed changes to the right to inspect, the existing right does not prohibit covered entities from allowing individuals to use personal resources to capture their PHI. Generally, individuals should be able to use personal resources, such as a smartphone, camera, or other device, to capture information about themselves. However, a covered entity is permitted to establish reasonable policies and safeguards regarding an individual's use of such personal resources for copying PHI to ensure that such use does not interfere with the ability of the covered entity to provide health care to others. These policies and safeguards may also ensure that the individual's personal resources are used in a way that enables the individual to copy or otherwise memorialize only the PHI to which they are entitled under the right of access.

A covered entity is not permitted to establish policies and safeguards that impose unjustified or unreasonable barriers to individual access (*e.g.,* limiting individuals to paper copies of their PHI). However, a covered entity is not required to allow an individual to connect a personal device to the covered entity's electronic information systems (*e.g.,* insert an individual's USB drive into one of the covered entity's workstations, sign an individual's mobile device onto a covered entity's network).

The Department does not believe that individuals capturing their own PHI through video, still camera photos, or audio recordings would be inconsistent with Federal or state recording laws or intellectual property rights protections.

Comment: Some commenters expressed concern about the administrative burdens that this proposal would impose on covered entities, such as the potential disruptions to workflow, and the potential implications for the quality of care. Several commenters asserted that the proposed change would require significant resources, such as extra space and personnel.

Several commenters expressed concern that individuals exercising this proposed right would view PHI that has not been validated or reviewed for accuracy or that is incomplete. A few commenters asserted that covered entities could face liability if certain PHI was not included in the medical record when inspected. One commenter stated that requiring a health care provider to provide access to PHI in real-time could damage the integrity of the medical record because health care providers may hesitate to be candid in their documentation and diagnosis in such cases.

Response: The Department agrees that the proposed changes to the right to inspect could be overly burdensome to covered entities and disruptive to their workflow. Accordingly, we are not finalizing the proposal. The existing right of inspection allows, and the Department encourages, covered entities to provide individuals with on demand, in-person access to requested PHI where appropriate, in whole or in part (if certain access may be denied under the Privacy Rule), including at the point of care.

A covered entity may deny an individual access to all or a portion of PHI requested in only very limited circumstances.[450] For example, a covered entity may deny an individual access if the information requested is not part of a designated record set maintained by the covered entity (or by a business associate for a covered entity),[451] or if the information is excepted from the right of access.[452] As another example, a covered entity may deny an individual access to particular PHI if a licensed health care professional determines in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.[453] Accordingly, a covered entity may deny an individual experiencing suicidal ideation access to such PHI as a health care provider determines in their professional judgment is reasonably likely to lead the individual to take their own life.[454] However, we stress that this ground is narrowly construed in order to protect individuals' autonomy interests and their right under the Privacy Rule to obtain information about themselves, which is fundamental in facilitating individuals' active participation in their own health care. General concerns about psychological or emotional harm (*e.g.,* concerns that the individual will not be able to understand the information or may be upset by it) are not sufficient to deny an individual access. In addition, the requested access must be reasonably likely to cause harm or endanger physical life or safety. Thus, concerns based on the mere possibility of harm are not sufficient to deny access.[455] As a result, we expect this ground for

[448] We use the term ''obtaining'' with respect to access to include both requesting and receiving access to such copies.

[449] *See* revised 45 CFR 164.524(c)(3); 65 FR 82462, 82557 (Dec. 28, 2000).

[450] *See* 45 CFR 164.524(a)(2) and (3); 164.524(e).

[451] This may include certain quality assessment or improvement records, patient safety activity records, or business planning, development, and management records that are used for business decisions more generally rather than to make decisions about individuals. *See* 65 FR 82462, 82554 (Dec. 28, 2000).

[452] *See* 45 CFR 164.524(a)(2)(i).

[453] *See* 45 CFR 164.524(a)(3)(i); 65 FR 82555–56 (Dec. 28, 2000).

[454] *See* 65 FR 82555 (Dec. 28, 2000).

[455] *Id.* at 82556, 82733.

denial to apply only in extremely rare circumstances.

Comment: Several commenters expressed opposition to the proposal because they believed that covered entities should be permitted, not required, to allow individuals to inspect their PHI. Several commenters who expressed opposition to the proposal recommended modifications. For example, some commenters recommended that the Department limit an individual's right to inspect their PHI to certain circumstances, while others recommended that the Department permit covered entities to limit the proposed right to inspect in certain circumstances. Still other commenters requested that the Department provide guidance on circumstances in which covered entities would be permitted to limit an individual's right to inspect.

Response: While in-person, point-of-care access to PHI may not always be appropriate or feasible, the Department declines to limit the existing right of an individual to inspect their PHI in a designated record set. Providing individuals with easy access to their PHI empowers them to make decisions about their health and well-being. Accordingly, as a process matter, covered entities should have in place reasonable procedures to enable individuals to inspect their PHI. The Department believes that responding to requests from individuals to inspect their PHI should impose minimal burden on the covered entity, particularly where the PHI requested is of the type easily accessed onsite or virtually by the covered entity itself in the ordinary course of business, such as during an in-person or virtual visit. The Department encourages covered entities to provide individuals with on demand access to PHI at the point of care where appropriate, in whole or in part (if access to certain PHI may be denied under the Privacy Rule).

Furthermore, where covered entities that are subject to the information blocking regulations employ practices that are likely to interfere with the access, exchange, or use of EHI, such practices may implicate the information blocking regulations.[456] This includes circumstances where an individual seeks to exercise their right to inspect and the requested PHI also meets the definition of EHI.[457]

Comment: One commenter recommended that, instead of creating a specific right to take photographs or videos, individuals should be given the option to take video or photographs, if both parties agree, at a mutually convenient time and place; and if the covered entity does not agree, require the covered entity to provide PHI in an alternative format.

Response: The Department is not modifying the Privacy Rule to include a specific right to take photographs, videos, or use other personal resources to capture PHI as part of an individual's right to inspect. The existing right to inspect does not place limitations on an individual's ability to record their PHI while they inspect it at a mutually convenient time and place. A covered entity may establish reasonable policies and safeguards regarding an individual's use of their own smartphone, camera, or other device for capturing PHI when exercising their right to inspect their PHI to ensure that equipment or technology used by individuals is not disruptive to the entity's operations and is used in a way that enables an individual to copy or otherwise memorialize only the PHI to which they are entitled under the right of access. An individual may inspect PHI in person (whether simply viewing or capturing it using a personal resource consistent with a covered entity's reasonable policies and safeguards), in addition to obtaining copies or in lieu thereof.

Comment: According to a few commenters, the proposal was unnecessary because individuals usually do not seek to access their PHI in person; instead, individuals generally prefer to access their PHI through patient portals or other electronic means.

Response: The Department agrees that the proposed changes are unnecessary, especially in light of (1) the burdens the proposal would impose on covered entities; and (2) the ability of an individual to capture their PHI in person using personal resources, to the extent consistent with a covered entity's reasonable policies and safeguards, while exercising the existing right to inspect their PHI in a designated record set. The Department also agrees that many individuals may prefer to access their PHI through patient or health plan member portals or other electronic means. With the increasing use of and continued advances in health IT, individuals often have the ability to access their PHI electronically quickly and easily, in real time, and on demand. Thus, the right to inspect PHI is not limited to in-person inspection. Rather, an individual may seek to exercise their right to inspect a copy of their PHI using remote communications technology (*e.g.,* communication app on a smartphone or other computing device). Accordingly, the right to inspect PHI can be a convenient method for individuals who choose to exercise their right of access in person or remotely.

Comment: A few commenters expressed support for the idea that covered entities should be permitted to provide individuals with copies of PHI in lieu of in-person inspection when necessary for public health and safety, during emergencies or otherwise.

Response: As explained above, the Department is not finalizing its proposals to add requirements to an individual's right to inspect their PHI in a designated record set. The Privacy Rule does not provide covered entities with the opportunity to deny or delay (beyond the permitted response period and extension) the right of an individual to inspect PHI, whether in person or otherwise, for public health and safety, during emergencies, or other circumstances. However, it does provide the opportunity for the covered entity to arrange with the individual for a time and place, which may be virtual, for the inspection that is mutually convenient.[458] Additionally, the covered entity is permitted to discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.[459]

4. Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access

a. Current Rule

Section 164.524(b)(1) requires a covered entity to permit an individual to request access to inspect or to obtain a copy of PHI about the individual that is maintained in a designated record set. It permits a covered entity to require individuals to make such a request in writing, provided that the covered entity informs individuals of such requirement. Section 164.524(b)(2) requires a covered entity to act on an individual's request for access no later than 30 days after receipt of the request, with an option to extend the time by an additional 30 days if they provide, during the initial 30-day period, a written explanation and the date by which the entity will complete its action on the request. The Department has long maintained that 30 calendar days is an outer limit.[460]

[456] 45 CFR 171.103.

[457] 45 CFR 171.102 (definition of ''Electronic health information'').

[458] *See* 45 CFR 164.524(c)(3)(i); 65 FR 82462, 82557 (Dec. 28, 2000).

[459] *Id.*

[460] *See* 65 FR 82462, 82556 (Dec. 28, 2000).

b. Proposed Rule

The Department proposed to modify the Privacy Rule to clarify that, while a covered entity may require an individual to make a request for access in writing, provided that it informs the individual of such a requirement, it may not impose unreasonable measures that impede the individual from obtaining access when a measure that is less burdensome for the individual is practicable for the entity. We also proposed to clarify that the writing could be in electronic or paper form and to include examples of reasonable and unreasonable measures in regulatory text. The Department proposed to modify the Privacy Rule to require that access be provided as soon as practicable, but no later than 15 calendar days after receipt of the request, with the possibility of one 15-calendar-day extension, provided that certain conditions are met. The Department also proposed that where another Federal or state law requires a covered entity to provide individuals with access to the PHI requested in less than 15 calendar days, we would deem the shorter time period to be practicable for purposes of proposed 45 CFR 164.524(b)(2)(i) and (d)(5).

Additionally, we proposed to add a new condition for the use of an extension that would require a covered entity to establish a written policy to prioritize urgent or other high-priority access requests (especially requests for health and safety and to support individual decisions about treatment options), to limit the need to use a 15-calendar-day extension for such requests. The Department also proposed to provide expressly at 45 CFR 164.524(c)(3) and 45 CFR 164.525(b) that, while a covered entity may discuss aspects of the access request with the individual before fulfilling the request, discussions to clarify the scope, format, and other aspects of the request would not extend the time limit for providing access.

c. Overview of Comments

Most commenters expressed concern that the proposed timeliness requirements would be overly burdensome and insufficiently flexible because of the varying complexity of requests. Even among commenters who were generally supportive, many recommended exceptions for certain types of requests or in certain circumstances (*e.g.,* natural disasters). While some commenters expressed support for the proposal to permit one 15-calendar-day extension if the covered entity adopted a policy to prioritize urgent or high-priority requests, most commenters expressed opposition to this proposal because they believed that it would be confusing and difficult to implement. Some of the commenters who expressed support for the proposal also requested that the Department clarify what would constitute a high priority or urgent request, including examples. Commenters who expressed opposition highlighted the burdens that they believed the proposal would create for both the covered entity and the individual. Commenters provided examples of circumstances that they believed would require additional time. Others expressed their belief that requiring the development and implementation of policies to prioritize responses to requests that are high priority or urgent access was unnecessary because such requests already are addressed by 45 CFR 164.506, which permits a covered entity to use or disclose PHI for TPO, without the individual's authorization, in certain circumstances.

d. Final Rule

We are adopting, with modification, the proposal to clarify the ability of covered entities to require individuals to make requests for access in writing. Specifically, we clarify, in paragraph (ii) of 45 CFR 164.524(b)(1) what we mean by ''in writing.'' We are not including the phrase ''electronic or paper form'' in regulatory text because the term ''form'' could be misinterpreted as requiring a particular form, template, document, or format that an individual must use to request access, which could cause confusion given other uses of the term ''form'' in 45 CFR 164.524. Instead, we clarify that ''in writing'' means that the request itself serves as documentation of the individual's exercise of the right of access, including when the request is submitted electronically or on paper. This language is intended to make clear that requests in writing do not need to be submitted on a particular form or in a particular format.

A request may be in writing when made through one or more written or electronic communications, so long as the communication(s) documents the individual's exercise of the right of access. For example, a request may be submitted using a handwritten letter, a paper form, an email, a secure message, a patient or health plan member portal, or another electronic mechanism. A request also qualifies as ''in writing'' if a covered entity receives a notification or other electronic transmission from a personal health app that contains the information necessary to document the individual's exercise of the right, such as information identifying the individual, the scope of the requested access, and information about where to send the requested PHI. For example, an access request sent through a Qualified Health Information Network [461] (QHIN) using TEFCA to a covered entity from an individual using an IAS Provider that is also a personal health app would constitute a written request where it documents the individual's exercise of their right of access. As another example, a request sent to a covered entity from an individual, through a patient facing app that connects to CMS Aligned Networks as a participant in the Medicare App Library, and such app is a personal health app, similarly would constitute a request that is in writing where it documents the individual's exercise of their right of access.

Covered entities are not required to adopt a particular electronic mechanism for receiving access requests or to receive electronic requests in a manner that the covered entity does not have the capability to support. The Department, however, strongly encourages covered entities to allow individuals to make requests for access electronically and to receive requests through electronic mechanisms that the covered entity has the capability to support.

Additionally, we are finalizing a new paragraph at 45 CFR 164.524(b)(1)(iii) to prevent a covered entity from imposing measures on an individual making requests for access that impede the individual from obtaining access (which includes measures for requesting such access) when there is a measure that is less burdensome for the individual and practicable for the entity. The finalized requirement does not include the term ''unreasonable'' because the regulatory text expressly describes the circumstances in which a measure is prohibited.

Further, we are not finalizing in regulatory text examples of reasonable or unreasonable measures. Including examples in the regulatory text could create the impression that the list is exhaustive, or that only the enumerated measures are permissible or impermissible. Instead, we reaffirm the examples provided in the 2021 NPRM and provide a non-exhaustive list of

[461] *See* 45 CFR 172.102 (definition of ''Qualified health information network''); definition of ''Qualified Health Information Network (QHIN),'' ''Common Agreement for Nationwide Health Information interoperability (Version 2.1),'' Assistant Security for Technology Policy and ONC TEFCA Recognized Coordinating Entity, section 1.1 (Nov. 2024), *https://healthit.gov/wp-content/uploads/2025/02/Common_Agreement_2.1.pdf; see also* ''Meet the Designated QHINs,'' The Sequoia Project, *https://rce.sequoiaproject.org/designated-qhins/.*

additional examples in this preamble to illustrate how the standard may apply in particular circumstances. For example, a covered entity may not require individuals to submit written requests or accept individuals' written requests only in a particular form (*e.g.,* only paper, only through a patient or health plan member portal) or delivered in a particular manner (*e.g.,* only in person at the covered entity's facility, only through the covered entity's online portal) when there is another measure for making such requests that is less burdensome for the individual and practicable for the entity (*e.g.,* emailing a request to a member of the covered entity's workforce responsible for handling requests for access). In addition, where a covered entity has the capability to receive requests for access submitted by the individual through a patient or health plan member portal, a personal health app from a secure standards-based API, or an HIO (*e.g.,* a QHIN), requiring the individual to use a more burdensome method to make the same request may impede access if receiving the request through that mechanism is practicable for the entity. When determining whether receiving requests electronically through such mechanisms is practicable, a covered entity may consider its technical capabilities, its obligations to protect the privacy of PHI under 45 CFR 164.530(c) and the security of ePHI under 45 CFR 164.306, and the costs of implementing such technical capabilities. We intend to issue additional guidance on access requests, including illustrative examples, to help regulated entities to understand the various ways in which requests might be made and the types of information that might need to included in different typ.

We also are adopting a modified version of the proposal to reduce the amount of time in which covered entities must respond to requests for individual access. Specifically, we are modifying 45 CFR 164.524(b)(2)(i) to require that a covered entity provide access to individuals ''as soon as practicable,'' but no later than 15 calendar days after receipt of a request. Relatedly, we are modifying 45 CFR 164.524(b)(2)(ii) to clarify that the 30-day extension that is permissible in certain circumstances refers to 30 calendar days. Additionally, we are adding a new 45 CFR 164.524(b)(2)(iii) to clarify that where Federal or state law requires a covered entity to provide an individual with access to the requested PHI in less than 15 calendar days, that shorter time period will be deemed practicable for purposes of 45 CFR 164.524(b)(2)(i). This will ensure that individuals receive more timely action on their access requests, while retaining the existing possibility of one 30-calendar-day extension (rather than the proposed 15-day extension) to accommodate more complex or difficult requests (*e.g.,* paper records that are archived offsite and not easily accessible, ePHI that may need to be retrieved from offline archival storage). The finalized requirement reduces the time within which covered entities must provide individuals with access to PHI, empowering individuals to take an active role in their care and facilitating care coordination and case management.

As discussed in the 2021 Privacy Rule NPRM, at least eight states require patients to be provided with copies of their health records in less time than the Privacy Rule's current 30-day limits,[462] and at least five states require the opportunity to view or inspect the record in fewer than 30 days.[463] Such requirements generally apply to health care providers, including hospitals and other health facilities, but not to health plans. Because most states do not impose time limits on covered entities that are as short as 15 days, access to PHI in such states will be markedly improved. Additionally, these shorter timelines support the Department's initiatives to implement statutory requirements aimed at empowering individuals to make more informed decisions about health care.[464] Shorter timelines also are consistent with individuals' needs and expectations. For example, most patients expect immediate online access to health information in their medical records, including tests results and clinician notes.[465] Easy online access to medical records—through patient or health plan member portals, personal health apps, or other mechanisms—is vital for those managing chronic conditions, new diagnoses, or another's care.[466]

For the same reasons, we also are adopting our proposal to apply these same timeliness requirements to requests from an individual to a covered entity to direct an electronic copy of PHI about the individual in an electronic health record to a person designated by the individual at new 45 CFR 164.524(d)(5).

Additionally, we are adopting our proposal to modify 45 CFR 164.524(c)(3) to reflect that discussions between the covered entity and the individual about the scope of an individual's request do not extend the amount of time that covered entities have to provide the requested access.

We are not finalizing the proposal to require that a covered entity implement a policy to prioritize certain types of requests. Based on public comments, covered entities already prioritize requests if an individual communicates the urgency of the request. Additionally, we are concerned that such a requirement could incentivize covered entities to require individuals to provide personal information about why a request is urgent, which would place a burden on individuals and could delay responses to such requests.

e. Response to Public Comments

Comment: Some commenters expressed support for the proposal for

[462] *See, e.g.,* Arizona, Ariz. Rev. Stat. 32–1264 (dentist, dental therapist, dental hygienist or denturist or a registered business entity) (15 business days to receive a copy); California, Cal. Health & Safety Code 123110 (health care provider) (15 days to receive a copy); Colorado, 3 Colo. Code Regs. 709–1 (dentists, dental therapists, and dental hygienists) (7 calendar days to receive a copy); Hawaii, Haw. Rev. Stat. 622–57 (10 working days to receive a copy if a patient's attorney requests records); Louisiana, La. Rev. Stat. 40:1165.1 (health care providers) (15 days to receive a copy), La. Rev. Stat. 40:2144 (hospitals) (15 days to receive a copy); New Jersey, N.J. Admin. Code 13:30–8.7 (dentists) (14 days to receive a copy); South Dakota, S.D. Admin. R. 20:43:11:04 (dentists, dental entities) (10 business days to receive a copy); Tennessee, Tenn. Code Ann. 63–2–101 (health care practitioners) (10 working days to receive a copy); Texas, Tex. Health & Safety Code 241.154 (hospitals) (15 days to receive a copy), Tex. Admin. Code 163.3 (physicians) (15 days to receive a copy), Tex. Health & Safety Code 181.102 (health care providers) (15 days to receive electronic copies if using an electronic health records system that is capable of fulfilling the request); and Washington, Wash. Rev. Code 70.02.080 (health care providers) (15 working days to receive a copy).

[463] *See, e.g.,* California, Cal. Health & Safety Code 123110 (5 business days to inspect); Colorado, 6 Colo. Code Regs. 1011:1:II–6.1 (licensed facilities and agencies (*e.g.,* hospitals, nursing facilities, ambulatory surgical centers, home care agencies)) (if a client is currently being provided services, 3 business days to inspect; if a client has been discharged, 10 business days to inspect); Nebraska, Neb. Rev. Stat. 71–8403 (health care providers) (10 days to inspect); Nevada, Nev. Rev. Stat. 629.061 (10 working days to inspect); New York, N.Y. Pub. Health Law 18(2)(a) (10 days to inspect); Texas, Tex. Health & Safety Code 241.154 (hospitals) (15 days to inspect); and Washington, Wash. Rev. Code 70.02.080 (health care providers) (15 working days to inspect).

[464] *See, e.g.,* 85 FR 25510 (May 1, 2020); 85 FR 25642 (May 1, 2020).

[465] *See* Bryan D. Steitz, et al., ''Perspectives of Patients About Immediate Access to Test Results Through an Online Patient Portal,'' JAMA Network Open (Mar. 20, 2023), *https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2802672* (noting that online portals let patients quickly access test results and medical records, and most patients now expect immediate electronic access to this information, including clinician notes); *see also* ''ONC Data Brief: Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2024,'' *supra* note 306, at p. 5 (noting individuals' app-based access to online medical records continues to rise).

[466] ''ONC Data Brief: Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2024,'' *supra* note 306, at p. 1.

reasons such as strengthening an individual's right of access, enabling individuals to obtain PHI more easily, improving care coordination, and enabling plaintiffs in personal injury lawsuits to meet litigation-related deadlines. A few commenters asserted that the fact that some states require covered entities to provide individuals with access to their PHI in less time than is currently required by the Privacy Rule demonstrates that it is possible. Several commenters expressed support for the proposal but recommended that the Department require covered entities to provide access to ePHI more quickly than the proposed timeline because it would benefit individuals to have access to their PHI as quickly as possible and ePHI is easily transmitted by a covered entity to an individual.

Many commenters recommended that the Department include exceptions to the proposed requirement. Commenters recommended exceptions for exigent circumstances or infeasibility (*e.g.,* natural disasters); where a covered entity demonstrates that it has made a good faith effort to retrieve PHI to which it lacks immediate access; for certain health care providers that treat individuals who have been involuntarily committed; and for covered entities that have revenue of less than a certain amount.

Several commenters expressed support for the ''as soon as practicable language'' but expressed opposition to the 15-calendar-day timeline because of concerns about their ability to gather the requested PHI in less time than they currently have or about the time it takes them to obtain clarification from individuals where the requests that they receive are incomplete.

Many commenters expressed opposition to the proposal because they believed that it would be burdensome to implement. Commenters asserted that many covered entities use a manual process for responding to access requests because they rely on legacy systems, requested PHI may be maintained offsite and/or in a form or format that is not easily accessible, or the requested PHI may include sensitive information that is subject to privacy restrictions in other laws. According to these commenters, the manual process can require more than 15 days. Commenters also asserted that the proposal would require extensive changes to workflow, training, orientation, and documentation. One commenter asserted that some hospital records may not be complete within 15 days of an individual's discharge because of delays in completing certain records. Some commenters recommended that the Department adopt alternative timeframes. For example, a few commenters recommended that the Department adopt a 30-day timeliness requirement with the possibility of one 15-day extension. A few commenters urged the Department to modify the proposal to provide different timelines for ePHI and for PHI that is not ePHI.

Several commenters requested that the Department provide guidance on best practices for managing and fulfilling individual access requests within 30 days.

Response: As discussed above, the Department is adopting a modified version of its proposal to reduce the amount of time that a covered entity has to respond to a request made pursuant to the right of access, including the right of access to direct. The final rule requires a covered entity to respond to an individual's request for access as soon as practicable, but no later than 15 calendar days after receiving the request, with the possibility of one 30-calendar-day extension. The Department encourages covered entities to view the 15 calendar days as an outer limit, particularly for requests for electronic copies of ePHI. Indeed, a covered entity may have the capacity to provide individuals with almost instantaneous electronic access to the PHI requested through personal health apps (*e.g.,* a TEFCA IAS Provider, a patient facing app that connects to CMS Aligned Networks as a participant in the Medicare App Library), web portals, or similar electronic means. Further, individuals may reasonably expect a covered entity to be able to respond in a much faster timeframe when the covered entity is using health IT in its day-to-day operations.[467] For example, individuals may be accustomed to receiving treatment from health care providers who use tools that are embedded in their EHRs to make certain information available quickly.[468] Similarly, individuals may reasonably expect to obtain electronic access to PHI from their health plan in a faster timeframe when they request to receive their health information through an API.[469] Additionally, as discussed above, we clarify that where a Federal or state law requires a covered entity to provide individuals with access to the PHI requested in less than 15 calendar days, that shorter time period would be deemed practicable.[470]

We emphasize that the timeliness requirement applies regardless of the circumstances of the request. For example, the timeliness requirement applies without regard to the form or medium (*e.g.,* paper, electronic) in which the requested PHI is maintained. Negotiating with the individual about the form and format of the response does not extend the timeliness requirement. As another example, the

[467] *See* ''Gaps in Individuals' Information Exchange: Health IT Quick Stat,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Sept. 2025), *https://healthit.gov/data/quickstats/gaps-individuals-information-exchange/#overview* (stating that in 2024, about one in five individuals who went to the doctor in the past year reported that they had to wait longer for test results than they thought reasonable); ''Perspectives of Patients About Immediate Access to Test Results Through an Online Patient Portal,'' *supra* note 465 (explaining that most patients want unrestricted access to their medical records and prefer immediately receiving test results); ''ONC Data Brief: Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2024,'' *supra* note 306, at p. 5 (explaining that individuals' app-based access to online medical records continues to rise and that eighty-seven percent of individuals who were encouraged by their health care provider to accessed their patient portal did so at least once in 2024).

[468] Specifically, clinicians who participate in merit-based incentive payment systems (MIPS) must provide patients with the ability to electronically view, download, and transmit certain health information within 4 business days of the information becoming available to the clinician. Participating clinicians also must ensure that the patient (or their personal representative) can access the health information with any application that is configured to meet the technical specifications of the API in the clinician's CEHRT. ''Merit-Based Incentive Payment System (MIPS) Promoting Interoperability Performance Category Measure 2025 Performance Period,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (last accessed Mar. 25, 2026), *https://qpp.cms.gov/reporting-requirements/ways-to-report/traditional-mips/promoting-interoperability.*

[469] Health plans regulated by CMS must maintain an API that permits certain apps to retrieve certain health information requested by an enrollee or that enrollee's personal representative no later than 1 business day. *See* 42 CFR 422.119, 431.60, 438.242, 457.730, 457.1233; 45 CFR 156.221; *see also* 85 FR 25510, 25632 (May 1, 2020); 89 FR 8758, 8974 (Feb. 8, 2024).

[470] *See, e.g.,* 85 FR 25642, 25813 (May 1, 2020) (explaining that actors are to make good faith efforts to work through common and understandable challenges and limitations to enable requestors to access, exchange, and use EHI as quickly and efficiently as possible); ''When would a delay in fulfilling a request for access, exchange, or use of EHI be considered an interference under the information blocking regulation?,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Mar. 2021), *https://healthit.gov/faq/when-would-delay-fulfilling-request-access-exchange-or-use-ehi-be-considered-interference-under/;* ''When a state or federal law or regulation, such as the HIPAA Privacy Rule, requires EHI be released by no later than a certain date after a request is made, is it safe to assume that any practices that result in the requested EHI's release within that other required timeframe will never be considered information blocking?,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Jan. 2021), *https://healthit.gov/faq/when-state-or-federal-law-or-regulation-such-hipaa-privacy-rule-requires-ehi-be-released-no/.*

timeliness requirement also applies to requests for PHI that is on paper, archived offsite and/or offline, and/or not otherwise easily accessible. If a covered entity is unable to provide access within 15 calendar days (*e.g.,* the information is archived offsite on paper and not easily accessible), the covered entity may extend the time to respond by no more than 30 calendar days. To extend the time, the covered entity must, within the initial 15 calendar days, inform the individual in writing of the reasons for the delay and the date by which the covered entity will provide access. Only one extension is permitted per access request.

In certain circumstances, because of the nature of a product or service (*e.g.,* mainstream genetic testing for cancer patients,[471] comprehensive genomic profiling of solid tumors,[472] or molecular biomarker testing [473]), 15 calendar days may not be sufficient to complete the product or service to which the individual has requested access. If the individual submits a request for access to the particular product or service that has not been completed and is not expected to be completed before the end of the 15-calendar-day period, the covered entity may notify the individual in writing within that 15-calendar-day period of the need and specific reason for the delay in providing access to PHI related to the completed product or service and the date by which the covered entity will complete its action on the request, in accordance with 45 CFR 164.524(b)(2)(ii)(A) and 164.524(d)(5)(ii)(B)(*1*). The Privacy Rule permits only one extension on such request, and the extension may not exceed an additional 30 calendar days. In the rare circumstance where 45 total calendar days is insufficient to satisfy the individual's request for access to PHI related to the completed product or service, the covered entity may, at the end of the 45-day period, satisfy the access request by providing the individual with access to the PHI that does exist at the time (*e.g.,* test requisitions, the underlying data being used to generate the reports, other completed test reports) in the designated record set.

However, to avoid this situation to the extent possible, where a covered entity knows that a particular product or service will take longer than the time permitted for responding to a right of access request, we encourage the covered entity to explain this circumstance to the individual. Upon informing an individual of this situation when they request access, the individual may be willing to withdraw or hold their request until a later time to ensure that they get access to the PHI that they want or need. If an individual chooses not to withdraw their request for access, the individual will then have a right, with respect to that request for access, only to obtain PHI in the designated record set at the time the request is fulfilled, which might not include the particular PHI requested because it is not yet available.[474] The individual can obtain the particular PHI requested by making another request for access at a later date. In these circumstances, we encourage covered entities to retain and respond to individuals' requests when the relevant product or service is completed and becomes part of the designated record set; however, they are not required to do so absent a new request.

Comment: Some commenters expressed concern about the ability of small health care providers to comply with the proposal because of limited staffing and other resources. A few commenters asserted that the proposal would have a negative effect on state government and Tribal entities in particular, because of their resource constraints and the associated burdens. These commenters provided examples of reasons why they believed this proposal was uniquely burdensome for them, such as weekend and holiday staffing challenges, their size, language translation needs, special programs, and other laws.

Response: The Department considered commenters' concerns about the potential burdens that the shorter time period may create. We believe that increasing the length of a possible extension to accommodate more complex or difficult requests from 15 calendar days, as proposed, to one 30-calendar-day extension, alleviates many of these concerns. To the extent that implementation burdens remain, the Department believes that the benefits to individuals (*e.g.,* their ability to direct their own health care, enhanced care coordination) outweigh the potential burdens on covered entities.

As discussed previously, the final rule requires that access be provided as soon as practicable, but in no case later than 15 calendar days after receipt of the request. It clarifies that the Department will deem fewer than 15 calendar days to be practicable where a Federal or state law requires such access to be provided more quickly. Where there is no specific law requiring faster access, the Department strongly encourages covered entities to provide individuals with access to their health information as quickly as possible within the allotted 15 calendar days. Moreover, even if regulated entities that also are subject to the information blocking regulations [475] fulfill requests for access within the time period required by the Privacy Rule, a practice that delays the fulfillment of such requests could constitute an interference under the information blocking regulations.[476]

Comment: Several commenters recommended that the Department align timeliness requirements across Federal programs that address aspects of the right of access.

Response: Implementation of certain requirements of the HITECH Act and Cures Act enables covered entities (and their business associates) that choose to use health IT to respond timelier to individual requests for ePHI. For example, developers of certified API technology must publish certain

[471] *See, e.g.,* Kyra Bokkers, et al., ''The Feasibility of Implementing Mainstream Germline Genetic Testing in Routine Cancer Care—A Systematic Review,'' Cancers (Basel), p. 7 (Feb. 19, 2022), *https://pmc.ncbi.nlm.nih.gov/articles/PMC8870548/.*

[472] *See, e.g.,* Adam H. Fox, et al., ''Turnaround Time of Comprehensive Genomic Profiling in Lung Cancer and Other Solid Tumors,'' JCO Oncology Practice (Jun. 18, 2026), *https://ascopubs.org/doi/10.1200/OP-25-01191?url_ver=Z39.88-2003&rfr_id=ori:rid:crossref.org&rfr_dat=cr_pub%20%200pubmed.*

[473] *See, e.g.,* Xiao Wang, et al. ''Molecular Biomarker Testing Patterns and Turnaround Time in US Patients With Advanced Non–Small Cell Lung Cancer,'' Journal of the National Comprehensive Cancer Network (Oct. 10, 2025), *https://pmc.ncbi.nlm.nih.gov/articles/PMC13268203/.*

[474] *See* 79 FR 7290, 7295 (Feb. 6, 2014); *see also* ''Is a clinical laboratory required to provide an individual with access to a test report that is not yet complete?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #2067 (June 24, 2016), *https://www.hhs.gov/hipaa/for-professionals/faq/2067/is-a-clinical-laboratory-required-to-provide/index.html.*

[475] *See* 45 CFR 171.102 (definition of ''Actor'').

[476] Whether a practice that is likely to interfere with access, exchange, or use of EHI meets the statutory or regulatory definition of information blocking is a fact-specific determination. *See* 45 CFR 171.103. *See also* 85 FR 25642, 25649, 25808 (May 1, 2020); 89 FR 1192, 1384 (Jan. 9, 2024); ''When a state or federal law or regulation, such as the HIPAA Privacy Rule, requires EHI be released by no later than a certain date after a request is made, is it safe to assume that any practices that result in the requested EHI's release within that other required timeframe will never be considered information blocking?,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Jan. 2021), *https://healthit.gov/faq/when-state-or-federal-law-or-regulation-such-hipaa-privacy-rule-requires-ehi-be-released-no;*''How would any claim or report of information blocking be evaluated?,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Feb. 2022), *https://healthit.gov/faq/how-would-any-claim-or-report-information-blocking-be-evaluated/.*

information about their APIs that can be used by individuals to access certain information using a personal health application.[477] The Cures Act directed the Secretary to require, as a condition of certification and maintenance of certification for the ONC Health IT Certification program, that the developer of certified technology allows health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.[478] To achieve such access, exchange, or use without special effort, ONC issued regulations that require certified APIs, and the health care ecosystem in which they are deployed, to be standardized, transparent, and pro-competitive.[479] Where a developer of certified API technology institutes an authenticity verification process for API users, the developer must complete that process within 10 business days and subsequently register and enable the application for production use within 5 business days.[480] Accordingly, when regulated entities adopt health IT that includes certified API technology, individuals can more easily access their ePHI and covered entities can more easily respond to right of access requests.

To further encourage the use of ONC-certified and other secure, interoperable health IT with the goal of providing individuals with timelier access to their PHI, this final rule requires that access be provided ''as soon as practicable,'' but in no case later than 15 calendar days after receipt of the request. It clarifies that the Department will deem fewer than 15 calendar days to be practicable where Federal or state law requires such access to be provided more quickly. Accordingly, where other Federal regulations, such as the Interoperability and Patient Access Final Rule,[481] the Interoperability and Prior Authorization Final Rule,[482] and the Quality Payment Program,[483] require a covered entity to provide an individual with access to PHI in fewer than 15 days, the Department deems the shorter time period to be ''practicable'' and expects that covered entities will comply with such other law.[484] Thus, a failure to comply with such other law also could result in a violation of the timeliness requirements at 45 CFR 164.524(b)(2)(i) and 164.524(d)(5)(ii)(A). Where there is no specific law requiring access in fewer than 15 calendar days, covered entities still must provide individuals with access to their health information as soon as practicable (*i.e.,* in less than 15 calendar days if practicable). Furthermore, where regulated entities that are subject to the information blocking regulations engage in a practice that delays fulfilling access requests, such practice could constitute an interference under the information blocking regulations, even if the requests are fulfilled within the 15-calendar-day period required by this final rule.[485]

The Department strongly encourages covered entities to take advantage of technologies that enable individuals to have faster or even immediate access to the requested information, adoption of which would, in turn, make such expedited access ''practicable.''

Comment: Several commenters expressed concern that covered entities often take more than the permitted time to let individuals know that their request is incomplete and then reset the ''clock'' when the individuals submit an updated request.

Response: The time period for responding to a request for access begins on the date that a covered entity receives the request, and a covered entity must respond within 15 calendar days of receiving it. This 15-calendar-day period includes, for example, the time that it takes a covered entity to obtain any additional information from the individual or personal representative that it needs to act upon a request and the time that it takes a covered entity to obtain pertinent information from a business associate or forward the request to the business associate for action. It also includes the time that it takes to verify an individual or personal representative's identity, and in the case of a personal representative, their authority to obtain access to the requested PHI. Where a request is sent directly to a business associate and the business associate agreement provides that the business associate is responsible for responding to such requests, the 15-calendar-day period begins when the business associate receives the request from an individual.

If the covered entity is unable to act on a request within 15 calendar days of receiving the request, it may extend the deadline for up to an additional 30 calendar days by providing the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request. This written statement describing the extension must be provided within the standard (*i.e.,* pre-extension) deadline of 15 calendar days. A covered entity may extend the deadline only once for any given access request.

Comment: Several commenters expressed concern that the proposal would be burdensome for health plans for a variety of reasons, including that they offer multiple products, requests often require coordination across business associates, the PHI requested may span a long period of time, and they have multiple electronic information systems that maintain PHI. One commenter requested that the Department provide health plans with a longer implementation period for this proposal because it would require administrative and technological changes to implement a new process for responding to access requests.

Response: We are adopting a modified version of our proposal that requires covered entities to respond to a request for access as soon as practicable, but no later than 15 calendar days after receipt of the request, with the possibility of one 30-calendar-day extension. To the extent that a particular request meets the conditions for a one-time extension, the total amount of time permitted for acting on the request is 45 calendar days from receipt of the individual's request, which we believe is sufficient for most

[477] *See* 45 CFR 170.404(a)(1).

[478] Sec. 3001(c)(5) of the PHSA, as amended by sec. 4002(a) of the 21st Century Cures Act, Public Law 114–255, 130 Stat. 1159–60 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–11(c)(5)(D)(iv); 45 CFR 170.404(a)(1).

[479] *See* 84 FR 7424, 7477 (Mar. 4, 2019); 85 FR 25642, 25739–40 (May 1, 2020).

[480] *See* 45 CFR 170.404(b)(1).

[481] *See* 42 CFR 422.119, 431.60, 438.242, 457.730, 457.1233; 45 CFR 156.221; 85 FR 25510 (May 1, 2020).

[482] *See* 42 CFR 422.119, 431.60, 438.242, 457.730; 45 CFR 156.221; 89 FR 8758 (Feb. 8, 2024).

[483] *See* 42 CFR 414.1375; 90 FR 49266, 49654–64, 49868–49903 (Nov. 5, 2025); *see also* ''Promoting Interoperability: Traditional MIPS Requirements,'' *supra* note 246; ''APM Performance Pathway,'' *supra* note 246.

[484] *See generally* ''When would a delay in fulfilling a request for access, exchange, or use of EHI be considered an interference under the information blocking regulation?,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Mar. 2021), *https://healthit.gov/faq/when-would-delay-fulfilling-request-access-exchange-or-use-ehi-be-considered-interference-under/.*

[485] *See generally* 45 CFR part 171; *see also* ''When a state or federal law or regulation, such as the HIPAA Privacy Rule, requires EHI be released by no later than a certain date after a request is made, is it safe to assume that any practices that result in the requested EHI's release within that other required timeframe will never be considered information blocking?,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Jan. 2021), *https://healthit.gov/faq/when-state-or-federal-law-or-regulation-such-hipaa-privacy-rule-requires-ehi-be-released-no.*

requests today even without significant changes in covered entities' policies and procedures. Additionally, to comply with other laws, many covered entities already have implemented patient or health plan member portals and other solutions for providing individuals with access to their PHI in an electronic form and format quickly and easily. Thus, we do not believe that covered entities need additional time to implement this requirement.

The effective date of the final rule is 60 days after publication for all regulated entities. Regulated entities have an additional 180 days until the compliance date to establish and implement policies, procedures, and practices to achieve compliance with any new or modified standards. Regulated entities are permitted to comply earlier than the compliance date, but the Department will not take action against them for noncompliance with the finalized requirements that occur before the compliance date. Thus, regulated entities have 240 days to develop and implement policies and procedures for responding to such requests.

5. Addressing the Form and Format of Access

a. Current Rule

Section 164.524(c)(2) includes the requirements for the form and format of a covered entity's response to an individual's request for access to their PHI. Section 164.524(c)(2)(i) requires a covered entity to provide an individual with access to the individual's PHI in the form and format requested by the individual, if it is readily producible in the requested form and format. Where the covered entity cannot provide PHI in the requested form and format, 45 CFR 164.524(c)(2)(i) requires the covered entity to provide the individual with a readable hard copy or such other form and format as agreed to by the covered entity and individual. If the covered entity maintains the PHI electronically, 45 CFR 164.524(c)(2)(ii) requires a covered entity to provide the individual with access to the information in the requested electronic form and format, if it is readily producible in that form and format, or if not, in a readable electronic form and format as agreed to by the covered entity and individual.

The Department interprets the phrase ''readily producible in that form and format'' as referring to (1) how PHI is produced to the individual (or person designated by the individual to receive an electronic copy of the PHI in an electronic health record), and (2) the format of the PHI that is transmitted (*e.g.,* the type of electronic file, etc.). When an individual requests access to PHI in a particular form or format, the question for the covered entity is whether or not the entity is able to readily produce the copy in that format—which is a matter of capability, not willingness.[486] Thus, if a covered entity has the capability to readily produce the requested format, it is not permissible for the covered entity to deny the individual access to that format because the entity would prefer that the individual receive their PHI in a different format or follow other procedures for accessing records that are more customarily relied upon by the entity.[487]

For example, where an individual requests a paper copy of PHI maintained by the covered entity either electronically or on paper, it is expected that the covered entity will be able to provide the individual with the paper copy requested.[488] Where an individual requests an electronic copy of PHI that a covered entity maintains only on paper, the covered entity is required to provide the individual with an electronic copy if it is readily producible electronically (*e.g.,* the covered entity can readily scan the paper record into an electronic format).[489] In the event that an individual requests an electronic copy of PHI and a covered entity maintains PHI electronically, a covered entity is not required to purchase new software or equipment in order to accommodate every possible individual request.[490] However, the covered entity in this circumstance must have the capability to provide some form of electronic copy of PHI maintained electronically.[491] Where an individual declines to accept any of the electronic formats readily producible by the covered entity, the covered entity may satisfy the request for access by providing the individual with a readable hard copy of the PHI.[492]

The Privacy Rule also includes requirements that address whether and when covered entities can provide individuals with summaries or explanations of their requested PHI. Section 164.524(c)(2)(iii) permits a covered entity to provide the individual with a summary of the requested PHI in lieu of copies, or an explanation of the PHI to which access has been provided, if the individual has agreed in advance to such summary or explanation, and to the fees imposed, if any, by the covered entity to cover the costs of preparing the summary or explanation.

b. Proposed Rule

In the 2021 Privacy Rule NPRM, the Department proposed to modify the requirements for covered entities responding to requests for access to PHI in an electronic form and format. Specifically, the Department proposed to add a new subparagraph (iii) to 45 CFR 164.524(c)(2) that would deem PHI to be ''readily producible'' in a form and format where another applicable Federal or state law requires the entity to provide the access in the particular electronic form and format requested by the individual. To accommodate this new paragraph and address the requirements of the right of access to direct, we also proposed to redesignate 45 CFR 164.524(c)(2)(iii) as 45 CFR 164.524(c)(2)(iv) and 164.524(d)(4).

Additionally, we proposed to require at 45 CFR 164.524(c)(2)(iv)(B) and 164.524(d)(4)(ii) that when a covered entity offers a summary to an individual, or a person designated by the individual, in lieu of copies of the requested PHI, it must inform the individual that they retain the right to obtain a complete copy of the PHI. These proposed requirements would not apply when the covered entity offers a summary because it is denying the individual's request made pursuant to the right of access (including the right of access to direct) on unreviewable or reviewable grounds. For example, a covered entity would not be required to inform an individual that they retain the right to obtain a complete copy of their PHI where the covered entity denies the individual's request for access to PHI because the requested PHI was obtained from someone (other than a health care provider) under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.[493] In such

[486] *See* ''When an individual exercises her HIPAA right to get an electronic copy of her PHI, can the individual choose the electronic format of the copy?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #2056 (May 30, 2025), *https://www.hhs.gov/hipaa/for-professionals/faq/2056/when-an-individual-exercises-her-hipaa-right/index.html.*

[487] *Id.*

[488] *See* 78 FR 5566, 5633 (Jan. 25, 2013).

[489] *See* ''If an individual requests an electronic copy of the individual's PHI that the covered entity maintains only on paper, is the covered entity required to scan the paper records to create an electronic copy of the PHI for the individual?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #2055 (June 24, 2016), *https://www.hhs.gov/hipaa/for-professionals/faq/2055/if-an-individual-requests-an-electronic-copy/index.html.*

[490] *See* 78 FR 5566, 5633 (Jan. 25, 2013).

[491] *Id.*

[492] *Id.*

[493] *See* 45 CFR 164.524(a)(2)(v).

circumstances, the covered entity would be required to implement the specified procedures for such denial.[494]

c. Overview of Comments

Commenters expressed mixed views on these proposals, with most commenters expressing concern or opposition. Some commenters asserted that the proposal to deem ePHI readily producible in a particular form and format in certain circumstances would increase costs for health care providers because it would require changes to their EHRs. Many commenters expressed opposition to the Department's proposal because they believed that it would require covered entities to use secure, standards-based APIs to fulfill requests for access. In contrast, a few commenters expressed support for this proposal because they believed that it would require covered entities to use secure, standards-based APIs to fulfill requests for access.

A few commenters expressed support for the Department's proposals to require that covered entities inform individuals that they retain their right to request access to their PHI (including their right of access to direct) if they do not agree to receive the summary (or to direct the summary to the person designated by the individual) in lieu of a copy of the PHI.

Commenters expressed the need for transparency about the information personal health apps collect on individuals, and what the developers do with that information, and urged the Department to protect individuals' health information from exploitation. These commenters expressed concern that app developers that are not regulated entities may misuse individuals' health information. Many commenters who expressed opposition to providing individuals with a copy of their PHI through a personal health app pursuant to the individual's right of access recommended that the Department require covered entities or an app itself to notify individuals that their information is not protected by HIPAA under such circumstances.

d. Final Rule

The Department is finalizing the proposals to: (1) add a new 45 CFR 164.524(c)(2)(iii); (2) redesignate existing 45 CFR 164.524(c)(2)(iii) as 45 CFR 164.524(c)(2)(iv) and 164.524(d)(4) without modification; and (3) add new 45 CFR 164.524(c)(2)(iv)(B) and 164.524(d)(4)(ii). New paragraph (iii) of 45 CFR 164.524(c)(2) provides that if other Federal or state law requires an entity (which may include a business associate acting on behalf of a covered entity) to implement a technology or policy that has the effect of providing an individual with access to their PHI in a particular electronic form and format, such form and format would be deemed ''readily producible'' for the purposes of compliance in fulfilling requests for such PHI under 45 CFR 164.524(c)(2)(i) and (ii).

The Department believes that aligning the Privacy Rule with other applicable laws facilitates individual access and care coordination, and eases burdens on covered entities and individuals. The Department also believes that these modifications increase transparency about the obligations of covered entities to provide individuals with copies of their PHI. Moreover, we believe that these modifications will result in a more complete understanding of the right of individuals to access their PHI.

Further, we clarify that PHI is readily producible in a form and format where a covered entity makes PHI available in that form and format to other persons (*e.g.,* regulated entities), and where the level of risk to the security of the covered entity's ePHI and electronic information systems (or the business associate's electronic information systems when the ePHI is maintained or transmitted by the business associate for, or on behalf of, the covered entity) is no greater than it is when providing the PHI to such other persons in that same form and format. For example, where a covered entity (or a business associate acting for, or on behalf of a covered entity) provides ePHI to another covered entity through a secure, standards-based API that also is capable of transmitting ePHI to a personal health app without increasing the risk to the security of the covered entity's ePHI or electronic information systems, we consider the ePHI to be readily producible to the individual through their personal health app. Further, where a covered entity transmits a copy of PHI through a personal health app, we interpret this as a transmission to the individual. In other words, the Department interprets a request by an individual to receive a copy of their PHI through a personal health app as an exercise of their right to obtain a copy, rather than an exercise of the right of access to direct (discussed below).

A covered entity is not required to provide an individual with a copy of the individual's PHI to or through a personal health app if a copy is not readily producible to or through such application. In other words, this final rule does not independently require the implementation of technology or policies by covered entities for the purpose of gaining the ability to provide individuals with a copy of their PHI to or through a personal health app. Rather, it requires that covered entities use technology or policies that are required by other Federal or state laws, or that they have otherwise implemented, to provide individuals with copies of their PHI to or through personal health apps where individuals request copies in such form and format.

Relatedly, we encourage covered entities to provide individuals with an electronic copy of their ePHI in another standards-based interoperable electronic format if the requested ePHI is not readily producible in the requested electronic form and format. Where the ePHI is not available in another standards-based interoperable electronic form and format, we encourage covered entities to provide individuals with their ePHI in a machine-readable electronic form and format. This approach aligns with the Manner Exception in the information blocking regulations.[495] Only if the ePHI is not producible in a machine-readable electronic form and format should covered entities offer individuals a copy of their ePHI solely in a human-readable electronic form and format—unless the individual requests the copy in such form and format.

Additionally, 45 CFR 164.524(c)(2)(iv)(B) and 164.524(d)(4)(ii) require that, when a covered entity offers a summary in lieu of a copy of PHI, it must inform the individual that the individual retains the right of access, including the right of access to direct if they do not agree to receive the summary. To fully comply with the access provisions, a covered entity remains obligated to ensure that it is the individual, and not the covered entity, who decides whether a summary is an acceptable substitute for a copy or copies of the requested PHI.

e. Responses to Public Comments

Comment: A few commenters expressed support for the proposal because they believed that it would clarify that ''readily producible'' includes access through secure APIs and personal health apps.

In contrast, many commenters expressed opposition to the Department's assertion that ''readily producible'' could include the use of implemented secure, standards-based APIs to fulfill access requests if a Federal or state law requires an entity to implement a technology or policy that

[494] *See* 45 CFR 164.524(d) (redesignated as 45 CFR 164.524(e) in this final rule).

[495] *See* 45 CFR 171.301.

would have the effect of providing an individual with access to their PHI in that form and format. A few commenters expressed opposition to the proposal because they believed that such a requirement would exceed the Department's authority under HIPAA and would require reliance upon or changes to other Federal or state laws. These commenters additionally asserted that aligning the Privacy Rule with other laws or policies in this manner could undermine the ability of the Department to exercise enforcement discretion, causing conflicts or requiring modification to the Privacy Rule when such other laws are modified.

Some of these commenters asserted that API technology was not mature and would continue to evolve. According to commenters, this lack of maturity could harm patient care because API technology was not able to fully integrate into other technologies, delaying the ability of covered entities to respond to individuals' requests for ePHI or diverting resources from clinical initiatives. Several commenters expressed opposition to this proposal because they believed that it would require physicians to implement API technology. These commenters asserted that such a requirement would increase costs and burdens for health care providers, especially for small providers, for various reasons, including the complexity of integrating API technology with legacy systems.

Several commenters expressed opposition to the proposal because they believed that the proposed modification would increase the burden on covered health care providers.

Other commenters recommended that the Department modify the proposal to clarify that a covered entity would not have to provide access to ePHI in the form or format requested if an exception to information blocking applies.

Response: The Department believes that providing individuals with easy and prompt access to their PHI empowers them to make informed decisions about their health care, and that supporting the adoption of new technologies that enable such access is essential. The Privacy Rule generally is technology neutral; accordingly, we do not specifically require covered entities to adopt APIs or other technology that enables access through personal health apps. Additionally, we recognize that not all covered entities have implemented technology, such as secure, standards-based APIs that are consistent with ONC's certification criteria and with their Security Rule obligations, to enable access to requested PHI through personal health apps. However, where a covered entity has chosen, or is required by other Federal or state law, to implement such technology or participate in TEFCA or the CMS Aligned Networks to enable access to requested PHI,[496] we will deem that PHI to be readily producible in that form and format for purposes of the right of access. We recognize that even where covered entities have implemented such technology or elected to participate in networks that enable the electronic exchange of PHI, not all PHI will be readily producible in the requested electronic form and format. For example, today, not all images can be exchanged electronically. Where an individual requests a copy of PHI that includes such images to be sent to their personal health app, the Department would not deem such images to be readily producible through the personal health app. Instead, the covered entity would be required to produce the PHI that is readily producible in that form and format through a personal health app and to provide the individual with the balance of the PHI in a mutually agreed upon form and format.

The provision deeming ePHI to be readily producible in a form and format where other Federal or state law requires that ePHI be available in the particular form and format only implicates covered entities that are subject to such other laws (*e.g.,* the Interoperability and Patient Access Final Rule).[497] This provision does not require modifications to other Federal or state laws, nor does it affect the ability of the Secretary to exercise enforcement discretion. Where an exception to or exclusion from a Federal or state law applies to a covered entity, the covered entity would not be obligated under such law to provide access using a particular form or format that otherwise would be required by the law. However, if that form or format is readily producible for the covered entity, the covered entity is still required to provide ePHI in that form or format if requested by the individual under the Privacy Rule.

We clarify that requiring all personal health apps to complete a registration process before the covered entity transmits ePHI to the individual and/or their personal representative through such apps, would not constitute a denial of access in the form and format requested, provided that the registration process does not exclude or prevent a personal health app that is capable of securely connecting to the secure, standards-based API from so connecting.[498] Additionally, as discussed above, negotiations about the form and format of an individual's request do not extend the amount of time that covered entities have to respond to requests for access. Accordingly, a covered entity's decision to require personal health apps to register through the process described above cannot be used as a basis to exceed the timeliness requirements for requests made pursuant to the right of access. This holds true regardless of whether the request was to provide the individual with their PHI through a personal health app or to transmit it to a person designated by the individual pursuant to the right of access to direct.

Comment: A few commenters expressed concern about potential risks to the privacy and security of identifiable health information in personal health apps. A few commenters urged the Department either to work with private sector entities to develop a privacy and security trust framework or to warn individuals that APIs and health apps currently lack sufficient regulatory and technology-based privacy and security guardrails. One commenter asserted that the proposal would facilitate the development of a national privacy framework that would ensure that health care data obtained by third-party apps is held to high privacy and security standards. One commenter asserted that the Department should limit the ability of personal health apps to be used by others for financial gain. Another commenter recommended that developers of personal health apps be required to provide individuals with transparency about their data collection and use policies.

Response: As health IT proliferates and matures, the Department must take steps, where possible within its statutory authority, to require that regulated entities implement corresponding privacy and security measures.[499] However, as we have

[496] *See* Security Rule, 45 CFR part 160 and subparts A and C of part 164.

[497] *See* 85 FR 25510 (May 1, 2020).

[498] HIPAA does not grant authority to the Secretary to impose security standards on a personal health app that is not a covered entity or a business associate. However, the information blocking regulations, at 45 CFR 171.203, provide an exception to what is considered information blocking when the actor's practice that is likely to interfere with the access, exchange, or use of EHI is implemented to protect the security of EHI and meets the other requirements of that provision. An actor whose practices met the security exception at all relevant times would not be subject to an enforcement action for information blocking. *See* 85 FR 25642, 25649 (May 1, 2020).

[499] For example, in 2025, the Department proposed significant modifications to the Security

Continued

explained elsewhere in this final rule, a personal health app or its developer, by definition, is not acting on behalf of or at the direction of a regulated entity, and therefore would not be subject to the privacy and security obligations of the HIPAA Rules. At the same time, a covered entity must provide an individual with access to their PHI in the form and format requested by the individual, if it is readily producible in such form and format.[500] As discussed above, we are adopting the proposal to clarify that a requested form and format would be deemed readily producible for purposes of compliance with the Privacy Rule if other Federal or state law requires an entity to implement a technology or policy that has the effect of providing an individual with access to their PHI in a particular electronic form and format (*e.g.,* if a Federal law required the provision of access via secure, standards-based API).

Whether a particular mode of transmission or transfer is readily producible is based on the capabilities of the covered entity and the level of security risk that the mode of transmission or transfer may introduce to the PHI on the covered entity's electronic information systems.[501] A covered entity is not expected to tolerate unacceptable levels of risk to the security of the PHI on its systems when responding to requests for access under the Privacy Rule. Whether the individual's requested mode of transfer or transmission presents such an unacceptable level of risk to the covered entity's ePHI or its electronic information systems is informed by the covered entity's Security Rule risk analysis and risk management measures.[502] We believe that, generally, when a covered entity determines its electronic information systems' ability to transmit PHI or to provide read access to PHI through a personal health app, the risk to the security of ePHI in their electronic information systems is low. At the same time, a covered entity remains responsible for maintaining awareness of and protecting ePHI in the face of new security vulnerabilities and threats to the confidentiality, integrity, and availability of ePHI. Determining whether a covered entity that is subject to the information blocking regulations is compliant with the Security Rule and has met the conditions of the Security Exception of the information blocking regulations requires separate analyses.[503]

Whether a particular mode of transmission or transfer is readily producible is not based on the level of privacy or security risks to the PHI once it has left the covered entity's electronic information systems. Thus, under the individual right of access, an individual may request a covered entity to transmit their ePHI to a personal health app in an unsecure manner or through an unsecure channel.[504] For instance, an individual may request that their unencrypted ePHI be transmitted to an app as a matter of convenience. With respect to such apps, the covered entity may consider informing the individual of the potential risks involved when the individual makes the request.[505]

The Department acknowledges that not all covered entities have implemented secure, standards-based APIs to enable individuals to access their ePHI using personal health apps. The Department believes that email generally is considered readily producible by all covered entities (except in the limited case where email cannot accommodate the file size of requested images), and transmitting PHI in such a manner does not present unacceptable security risks to the electronic information systems of covered entities, even though there may be security risks to the PHI while in transit (*e.g.,* where an individual has requested to receive their PHI by, and accepted the risks associated with, unencrypted email).[506]

Comment: A few commenters expressed support for the proposal to require a covered entity to inform the individual who requests copies of PHI that the individual retains the right of access to direct a copy of ePHI in an electronic health record to a designated person and does not have to agree to a summary in lieu of access. One commenter expressed concern that the proposal could limit the ability of health care providers to restrict the access of parents or guardians to certain PHI. This commenter asserted that the proposal would conflict with certain state laws because they believed that the proposal would require the disclosure of a minor's full record, even where state law directs covered entities to provide parents/guardians with a summary of the minor's records.

Response: The Department proposed and is finalizing without modification the proposal to require that when a covered entity offers the individual a summary of their PHI in lieu of providing access, the covered entity must inform the individual that the individual retains the right to obtain a copy of the requested PHI (or to direct an electronic copy of PHI in an electronic health record to a person designated by the individual) if they do not agree to the summary.

The Privacy Rule establishes the right of an individual, or a personal representative acting on the individual's behalf, to access the individual's PHI.[507] The Privacy Rule provides that, if under applicable law, a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under the HIPAA Rules, with respect to PHI relevant to such personal representation.[508] In most cases, a parent is the personal representative of an unemancipated minor child and can exercise the minor child's rights with respect to PHI, because the parent usually has the authority to make health care decisions about their minor child.[509] Accordingly, the Privacy Rule generally gives the parent the right to access the minor child's medical records as the minor child's personal representative, unless one of the limited exceptions applies. This final rule does not change anything with respect to the exceptions or the grounds for a denial of access.[510] We believe that this modification is necessary to ensure that individuals remain aware of their rights and the obligations of covered entities with respect to their PHI.

Rule to strengthen protections for ePHI. *See* 90 FR 898 (Jan. 6, 2025).

[500] 45 CFR 164.524(c)(2) and (3).

[501] This discussion refers to covered entities because the Privacy Rule imposes the obligation to provide an individual with access to their PHI on covered entities. However, the concepts discussed herein apply equally to business associates that, on behalf of covered entities and pursuant to their business associate agreements, furnish individuals with access to their PHI.

[502] *See* 45 CFR 164.524(c)(2) and (3); 164.308(a)(1).

[503] *See* 45 CFR 171.303.

[504] *See* 45 CFR 164.524(a)(1), (c)(2)(ii), and (c)(3); *see also* ''Can a covered entity refuse to disclose ePHI to an app chosen by an individual because of concerns about how the app will use or disclose the ePHI it receives?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #3012 (Apr. 18, 2019), *https://www.hhs.gov/hipaa/for-professionals/faq/3012/can-a-covered-entity-refuse-to-disclose-ephi.html.*

[505] *See* 85 FR 25642, 25814 (May 1, 2020) (discussing how a covered entity that is also an actor may provide individuals with such information).

[506] *See* 90 FR 898, 969 (Jan. 6, 2025) (discussing risks associated with a request for access in a manner that does not support encryption, such as unencrypted email).

[507] 45 CFR 164.524.

[508] 45 CFR 164.502(g)(3)(i).

[509] *See* Letter to Colleagues from OCR Director Paula M. Stannard, *supra* note 354.

[510] 45 CFR 164.502(g), 164.524(a)(3) and (4), and 164.524(d)(2) and (3).

6. Addressing the Individual Right of Access to Direct Copies of PHI to a Person Designated by the Individual

a. Issues To Address

Section 13405(e)(1) of the HITECH Act expanded the individual right of access, codified at 45 CFR 164.524, to include the right of an individual to direct an electronic copy of their PHI in an electronic health record to a person designated by the individual, provided that the direction is clear, conspicuous, and specific.[511] Under the 2013 Omnibus Rule, which implemented certain provisions of the HITECH Act, the individual's (or their personal representative's) request to exercise the right of access to direct must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.[512]

The 2013 Omnibus Rule also expanded the right of access to direct to encompass all PHI in a designated record set, regardless of whether the PHI is in an electronic health record.[513] The court in *Ciox* held that the Department had exceeded its authority under the HITECH Act and vacated the Department's expansion of the right beyond electronic copies of PHI in an electronic health record. Thus, the Department is revising the Privacy Rule to ensure that section 13405(e) of the HITECH Act is implemented consistent with the court's interpretation of the statute in *Ciox.*

b. Proposed Rule

The Department proposed to create a separate set of provisions, within the Privacy Rule section on the right of access, to address the individual's right of access to direct a covered health care provider to transmit an electronic copy of PHI in an electronic health record to a person designated by the individual. We proposed to require a covered health care provider to respond to an individual's request to exercise this right when the request is clear, conspicuous, and specific and to permit the request to be made orally or in writing (including electronically). Additionally, the Department proposed that only covered health care providers would be responsible for fulfilling an individual's request under the right of access to direct because the Department did not believe that other covered entities would have an electronic health record as we proposed to define it.

The Department also proposed to extend the right of access to direct to require a covered health care provider or health plan (the ''Requestor-Recipient''), at an individual's direction, to submit an individual's access request for their ePHI to another covered health care provider (the ''Discloser''), requesting that the Discloser transmit ePHI maintained by or on behalf of the Discloser in its electronic health record to the Requestor-Recipient. We proposed that this requirement would apply when an individual was an existing or prospective new patient or a current member (or dependent) of the Requestor-Recipient, and would be limited to directing electronic copies of PHI in an electronic health record back to the Requestor-Recipient.

c. Overview of Comments

Many commenters expressed opposition to the Department's proposal to limit the right of individuals to direct a copy of PHI to a designated person to only electronic copies of PHI in an electronic health record because they believed that it would eliminate individuals' right of access to direct non-electronic copies of PHI and PHI that is not in an electronic health record. Some commenters expressed concerns that the right of access to direct had been misused by other persons and that individuals sometimes were unaware of what PHI was being disclosed under this right, to whom, and for what purpose. Several commenters expressed support for limiting an individual's right of access to direct as proposed because they believed that it would ease compliance.

d. Final Rule

We are finalizing many of our proposals for 45 CFR 164.524(d), with modification, as described below. Consistent with the HITECH Act, the final rule adopts, with modification, the proposal to require a covered entity to transmit an electronic copy of PHI in an electronic health record to the person designated by the individual if directed to do so by an individual. While we do not believe that the definition of an electronic health record is relevant to all covered entities, we recognize that there are some circumstances where a covered entity other than a covered health care provider may have an electronic health record (*e.g.,* where a health plan is integrated with a health care provider and maintains PHI in the same electronic information systems as the health care provider). In such circumstances, both the health plan and the health care provider would be required to respond to requests made pursuant to the right of access to direct. Accordingly, the regulatory text reflects that the right of access to direct may apply to all covered entities that are subject to the right of access.[514]

As required by the HITECH Act, consistent with the court's decision in *Ciox,* the scope of this right is limited to requests for electronic copies and to PHI in an electronic health record. Thus, requests for a non-electronic copy of PHI or for PHI that is not in an electronic health record do not meet the conditions for the right of access to direct. Instead, in such circumstances, in order for the covered entity to transmit the requested PHI to another person, an individual would need to provide a covered entity with a valid authorization to disclose the requested PHI to that other person, absent an applicable Privacy Rule permission.

Section 13405(e) of the HITECH Act places the right of access to direct within 45 CFR 164.524, which contains the standard for the right of access. Thus, the final rule adopts a revised version of the proposed standard for the right of access to direct—also placing it within the section of the Privacy Rule that addresses the right of access—that more closely mirrors the standard for the individual right of access at 45 CFR 164.524(a) and incorporates the limitations of the right of access into the right of access to direct. Through these revisions, we clarify that, consistent with the HITECH Act and the *Ciox* decision, the right of access to direct is limited to PHI about the individual that is both in an electronic health record and in a designated record set. PHI that is in an electronic health record but not in a designated record set (*e.g.,* patient safety work product), or that is in a designated record set but not in an electronic health record (*e.g.,* paper records), is not subject to the right of access to direct. We also clarify that this right, like the broader right of access, excepts both psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, from the PHI in an electronic health record that an individual is entitled to direct to a person designated by the individual. Similarly, we clarify that, for purposes of the right of access to direct, an ''electronic copy'' has the same meaning as we interpret the term under the broader right of access.[515] The

[511] *See* sec. 13405(e) of the HITECH Act, 123 Stat. 264 (Feb. 17, 2009) (codified at 42 U.S.C. 17935(e)).

[512] 45 CFR 164.524(c)(3)(ii).

[513] *See* 78 FR 5566, 5631 (Jan. 25, 2013).

[514] Health care clearinghouses are not subject to the same individual access requirements as health plans and covered health care providers. *See* 45 CFR 164.500(b)(1).

[515] 78 FR 5566, 5631–34 (Jan. 15, 2013).

requirements of the individual right of access with respect to denials and timing also are mirrored in the right of access to direct. Thus, requests made pursuant to the right of access to direct can be denied for the same reasons as a request made pursuant to the individual right of access and must be addressed within the same amount of time, as discussed below.

Additionally, we eliminate references to a ''third party'' and replace them with the statutory language of ''a person designated by the individual.'' Not only does this language mirror the HITECH Act more closely, but it also emphasizes the purpose of the right—to strengthen individuals' control over disclosures of their PHI.

We are not finalizing the proposal to require a covered entity to respond to individuals' requests made pursuant to the right of access to direct when such requests are made orally. We are persuaded by public comments that implementing the proposed requirement for covered health care providers to respond to oral requests made pursuant to the right of access to direct would be difficult, would increase burdens on covered entities because of the work associated with verifying the accuracy of the request, and would increase the likelihood of miscommunication and erroneous responses to requests, leading to potential breaches of unsecured PHI (*e.g.,* misdirected records). Instead, we are finalizing the implementation specification at 45 CFR 164.524(d)(5) to more closely mirror the implementation specification at 45 CFR 164.524(b) by including both: (1) instructions for how a covered entity is to identify requests made pursuant to the relevant right; and (2) the amount of time that a covered entity has to act on such requests.

Consistent with the HITECH Act, the final rule adopts a new 45 CFR 164.524(d)(5)(i) that instructs a covered entity to permit an individual to direct an electronic copy of PHI about the individual in an electronic health record to a person designated by the individual where the request is clear, conspicuous, and specific. This section also clarifies that a covered entity is permitted to require an individual to make such a request in writing, provided that it informs the individual of such a requirement. For purposes of the right of access to direct, consistent with new 45 CFR 164.524(b)(1)(ii), ''in writing'' means that the request itself serves as documentation of the individual's exercise of the right of access to direct, including when the request is submitted electronically or on paper.

Individuals who request that a covered entity provide them or a person that the individual designates with access to their PHI are not required to execute a HIPAA authorization. As discussed above, a request to direct an electronic copy of PHI in an electronic health record to a person designated by the individual is sufficient when it is clear, conspicuous, and specific. Because a HIPAA authorization requires more information than is necessary or that may be relevant for individuals to exercise their access rights, including their right of access to direct,[516] requiring the execution of a HIPAA authorization may create impermissible obstacles to the exercise of this right. Where it is unclear, based on the form of a request, whether the request is an effort by the individual to exercise their right of access to direct or merely the individual's authorization to disclose PHI as requested by a third party, covered entities may seek clarification from the individual about whether the request was a direction from the individual or a request from the third party. The instructions about the amount of time a covered entity has to respond to a request made pursuant to the right of access to direct are now in 45 CFR 164.524(d)(5)(ii), mirroring the instructions for timeliness under the individual right of access at 45 CFR 164.524(b)(2). A covered entity's decision to require individuals to execute HIPAA authorizations for all requests for disclosures does not extend the amount of time that it has to respond to a request made pursuant to the right of access, including the right of access to direct. This is true even if the covered entity needs to contact an individual who requests an electronic copy of their PHI in an electronic health record to clarify whether the individual is intending to exercise their right of access to direct.

To eliminate redundancy, we are finalizing the proposal to consolidate the instructions to covered entities about how to address individual requests for a review of a denial of access at 45 CFR 164.524(e)(4) and clarifying that similar instructions apply where an individual requests a review of a denial of the right of access to direct for a reviewable ground. Accordingly, where a covered entity denies, on a reviewable ground, a request made pursuant to the individual right of access, including the right of access to direct, the covered entity must designate a licensed health care professional who was not directly involved in the denial to review the decision to deny access and promptly refer the request to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether to deny the access request based on the standards for a reviewable ground for a denial. The covered entity must promptly provide written notice of the determination of the designated reviewing official and take any other required actions to carry it out.

The Department is not finalizing the proposal to require covered health care providers and health plans, at an individual's direction, to submit an individual's request made pursuant to the right of access to direct to another covered health care provider (the ''Discloser''), requesting that the Discloser transmit ePHI maintained by or on behalf of the Discloser in its electronic health record to the Requestor-Recipient. We are persuaded by public comments that the proposal would increase the burden on covered entities and be difficult to implement. The disclosures contemplated by the proposal already are permitted under the Privacy Rule (*e.g.,* for treatment purposes). Thus, the Department's decision not to finalize this proposal does not preclude covered entities from assisting an individual by submitting an access request for PHI to another covered entity on the individual's behalf, nor would it preclude the other covered entity from sending the requested PHI to the covered entity who assisted the individual in making the request.

e. Response to Public Comments

Comment: Several commenters expressed concern that the proposal to limit the right of access to direct to electronic copies of PHI in an electronic health record would decrease the utility of this right by decreasing the amount of PHI available to a person designated by the individual. According to commenters, this would limit the ability of individuals to meaningfully participate in their health care and to determine who has access to their information. A few commenters asserted that limiting the right of access to direct to PHI in an electronic health record would not address requests to direct to a designated person non-electronic PHI or PHI in health IT systems other than an EHR, thus requiring a covered health care provider to obtain an authorization before complying with such requests. A few commenters asserted that it would be difficult to distinguish between requests from an individual to direct an electronic copy of PHI in an electronic health record to a designated person from requests an individual makes that require an authorization.

[516] *See* 45 CFR 164.508(c).

Response: The Department is finalizing its proposal with minimal modifications, as described above. The court in *Ciox* held that the HITECH Act created a limited right of access to direct and the Department could not expand that right. Therefore, the final rule limits the right of access to direct PHI to an electronic copy of PHI in an electronic health record. The definition of electronic health record further limits the application of the right of access to direct because the HITECH Act specifies that an electronic health record is an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. As discussed above, we interpret such clinicians to include health care providers that have direct or indirect treatment relationships with individuals. Also as discussed above, we do not believe that the definition of an electronic health record applies to all covered entities, but we recognize that it may apply to more than covered health care providers. Thus, we are not limiting the right of access to direct to only covered health care providers. Furthermore, as explained above, we do not interpret PHI in an electronic health record as limited to PHI in a particular software or application. Rather, we interpret it to include all PHI that is in an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

As a process matter, to ensure compliance with the Privacy Rule, covered entities may wish to assume that a clear, conspicuous, and specific request made by an individual to transmit an electronic copy of PHI about the individual in an electronic health record to a person designated by the individual is a request made pursuant to the right of access to direct. Covered entities are encouraged to contact the individual making the request if there are any questions or concerns about the request, including about the authority of the person designated by the individual to have access to the PHI.

A request for PHI that is not in an electronic health record, or a request for a copy in a non-electronic format, would not meet the conditions of the right of access to direct. Thus, such requests should be treated as requests made pursuant to an authorization, provided that the request meets the requirements for a valid authorization at 45 CFR 164.508. Where such requests do not meet the requirements for a valid authorization, the Department encourages covered entities to consider whether another provision of the Privacy Rule would permit the disclosure, and if not, to contact individuals to explain the limitations of the right of access to direct and obtain the information that is needed for the request to constitute a valid authorization.

Comment: Many commenters asserted that disclosures to personal health apps should be treated as requests made pursuant to the right of access to direct, rather than either of the following: (1) a request made pursuant to the individual right of access, or (2) a request for disclosure pursuant to valid authorization.

Response: As explained above, we interpret a personal health app to be equivalent to the individual and a request from an individual to receive their PHI in a personal health app to constitute an individual request to obtain a copy of their PHI in a particular electronic form and format. In other words, when employed by the individual (or their personal representative), a personal health app, as defined in this final rule, is a technology or tool used by the individual (or their personal representative); the personal health app is not a person designated by the individual to receive PHI. Thus, when an individual requests that a covered entity transmit the individual's PHI to a personal health app, we interpret the request as being made pursuant to the individual right of access at 45 CFR 164.524(a), rather than a request made pursuant to the right of access to direct at 45 CFR 164.524(d). Where an individual requests that a covered entity transmit a copy of their PHI in an electronic health record to an app that is not offered by or on behalf of another regulated entity, and does not meet the definition of personal health app (because, for example, the information in the app is not managed, shared, and controlled by or primarily for the individual), we would interpret such request as being made pursuant to the right of access to direct (where the request meets the applicable requirements). As discussed above, the processes and technology that a covered entity implements will enable it to differentiate between the different types of apps that transmit requests for PHI through the covered entity's API.

Comment: Some commenters asserted that the right of access to direct is abused by third parties for commercial purposes. According to some commenters, in some cases, fraudulent requests are submitted to covered entities purportedly on behalf of individuals, creating additional burden for regulated entities because they must verify that the request was initiated by the individual. Some commenters recommended that the Department limit the scope of the proposal, or issue guidance to clarify its application, to specific categories of persons, purposes, or PHI; or limit the liability of health care providers when a request is for disclosure in certain circumstances. A few commenters asserted that Congress intended for section 13405(e) of the HITECH Act to facilitate the disclosure of PHI only for health care purposes and urged the Department to limit the right of access to direct to apply only where the person designated by the individual is a health care provider, social service organization with whom PHI may be shared for care coordination, or caregiver. One commenter expressed concern about their ability to comply with the proposal while also complying with other laws that restrict the disclosure of certain PHI (*e.g.,* state laws that limit the disclosure of records about an individual's mental health).

Many commenters expressed concern that the proposal would result in the disclosure of sensitive information to entities that are not regulated under the HIPAA Rules. Some commenters expressed concern that such disclosures would pose risks to the privacy and security of PHI. One commenter asserted that the proposal would impose an administrative burden and raise liability concerns for health care providers if the PHI is disclosed to a designated person and then used or disclosed inappropriately.

Several commenters requested that the Department either modify the Privacy Rule or issue guidance to clarify covered entities' obligations under the proposed right of access to direct in an environment where PHI is increasingly transmitted electronically and to a wider pool of recipients.

Response: As discussed above, Congress has enacted several laws that direct the Department to empower individuals by ensuring that they have access to and the ability to share their PHI. For example, as enacted by Congress, section 13405(e) of the HITECH Act provides individuals, as part of the right of access, the right of access to direct a covered entity to transmit an electronic copy of their PHI in an electronic health record to a person designated by the individual. The statute placed no limitations on the ability of the individual to choose the person to whom they direct electronic copies of their PHI in an electronic health record. In this final rule, the Department seeks to implement this right, as directed by Congress. Thus,

consistent with the HITECH Act and the Privacy Rule's longstanding right of access provisions, the purpose of an individual's request for access and/or the designated person to whom they choose to direct an electronic copy are not relevant factors when a covered entity responds to an individual's access request, including a request under the right of access to direct. Accordingly, a covered entity cannot deny an individual's request under the right of access to direct based solely on the covered entity's opinion of the person that the individual designates or the purpose(s) for which the individual requests the disclosure. For example, a covered entity may not deny an individual's request made pursuant to the right of access to direct merely because the covered entity does not agree with the individual's decision to direct a copy of their PHI to an attorney or other person. Prior to disclosing PHI, a covered entity is required to verify the identity of a person requesting PHI and the authority of that person to have access to PHI if the identity or authority of such person is not known to the covered entity. Elsewhere in this final rule, we finalize a prohibition against imposing an unreasonable identity verification requirement on an individual attempting to exercise the right of access and provide examples of both reasonable and unreasonable measures of identity verification. For example, it would be reasonable for a covered entity that receives a request made pursuant to the right of access to direct to contact the individual to verify that they intended to direct the copy to the particular person.

Comment: Many commenters recommended that all requests made pursuant to the right of access to direct should be in writing. Many commenters expressed opposition to the proposal to allow oral requests, with several commenters asserting that the proposal would be inconsistent with the HITECH Act because oral requests are not ''conspicuous.'' Some commenters expressed concern that the proposal could lead to increased risks to individual privacy, as well as fraud and abuse. Some commenters asserted that the proposal would pose an administrative burden or implementation challenge and provided examples, such as developing new processes for accepting, documenting, and tracking such requests, changing workflows, and training staff on the new processes.

Some commenters expressed concern about their ability to verify the identity of an individual making an oral request. A few commenters recommended that the Department impose limitations on oral requests, such as allowing individuals to make oral requests only in person except where making the request in person would present an undue burden for the individual or in urgent situations, provided that the request is later reduced to writing. A few commenters recommended that health care providers be permitted to verify the identity of individuals making oral requests. A few commenters stated that covered entities should have the flexibility to determine whether to accept oral requests for access.

Some commenters requested that the Department create a safe harbor to shield covered entities from liability for erroneous disclosures that may result from responding to an oral request for access. One commenter asserted that the proposal could create a conflict with state laws that require providers of behavioral health care to adopt additional due diligence practices, such as obtaining written consent from the individual, before disclosing PHI.

Several commenters requested that the Department provide guidance on how to operationalize this proposal and examples of what would constitute ''clear, conspicuous, and specific'' requests.

Response: As explained above, based on public comments, we are not finalizing the proposal to require covered entities to accept oral requests made pursuant to the right of access to direct. Instead, consistent with the HITECH Act, we require that the request be clear, conspicuous, and specific. We also are adopting language that permits a covered entity to require that the request be in writing, provided that it informs individuals of such requirement, consistent with the modification that we are making at 45 CFR 164.524(b)(1)(ii), which includes the clarification of what constitutes a request in writing.[517]

For example, we would consider a request to be clear, conspicuous, and specific if the individual sends an email to a covered health care provider requesting that the provider send to the individual's family member an email containing a report interpreting diagnostic images where the report is maintained in the provider's electronic health record, provided that the request included the family member's name and email address.[518] We would not consider this request to be clear, conspicuous, and specific if it did not contain the family member's name or email address. As another example, we would consider a request to be clear, conspicuous, and specific where the individual sends a message through a personal health app to a covered health care provider requesting that the provider send the individual's PHI in the provider's electronic health record to a file-sharing application used by the individual's attorney, provided that the message included the attorney's name and specific information about how and where to send the PHI. We would not consider this request to be clear, conspicuous, and specific if it did not include information about how to send the individual's PHI to the attorney's file-sharing application.

Where a verbal request meets the requirements of clear, conspicuous, and specific, a covered entity is permitted, but not required, to accept the request. For example, where an individual, in a discussion, tells the receptionist that they would like to have their PHI in an electronic health record emailed to a particular family member and the individual dictates the family member's email address or provides the email address in writing to the receptionist, such request could be considered clear, conspicuous, and specific. For such verbal requests, the covered entity would be responsible for adopting reasonable safeguards to document the request in writing to protect the information that is disclosed. For example, a reasonable safeguard would not need to require the covered entity to confirm that the individual provided the correct email address of the designated person, but it would require reasonable procedures to ensure that the covered entity correctly typed the email address.[519]

Comment: Several commenters expressed support for the proposal to require covered entities and health plans, at the individual's direction, to submit an individual's access request to another covered entity. A few commenters expressed support for this proposal because it would facilitate care coordination and access. One commenter requested guidance about how this access pathway would work in relation to the pathway for individuals to obtain access through a personal health app.

Many commenters expressed opposition to the proposal to require covered health care providers and plans, at an individual's direction, to submit to another covered entity the individual's request to transmit an electronic copy of

[517] *See* 45 CFR 164.524(b)(1).

[518] *See infra* for a discussion of reasonable measures that covered entities may implement to verify the identity of a person, including an individual who seeks to exercise the right of access to direct.

[519] *See* 78 FR 5566, 5635 (Jan. 25, 2013).

PHI in an electronic health record to a person designated by the individual. Some commenters asserted that the proposal would be burdensome or impracticable for health care, create additional paperwork, obligate health care providers to gather PHI that they do not need, potentially cause confusion, and unnecessarily delay responses to requests. A few commenters asserted that the proposal was unnecessary because the interoperability rules and standards designed to enable automated workflows already address the issue.

Several commenters asserted that the proposal would increase the risks to privacy, security, and health care delivery because of the amount of PHI that the Requestor-Recipient would be collecting. A few commenters expressed concern that the proposal would create a conflict with state laws on record collection and retention. Commenters suggested ways to address these risks, such as modifying the proposal to allow the Requestor-Recipient to exercise reasonable judgment when deciding whether to respond to the request, using a number of factors; requiring that the individual be a patient of the Discloser (as opposed to a former patient or prospective new patient); and permitting the Discloser to deny requests from a Requestor-Recipient when the Discloser determines, using professional judgment, that fulfilling the request is not in the best interests of the individual.

A few commenters requested that the Department clarify which party would be responsible for reporting the Discloser's failure to provide an electronic copy of the individual's PHI or to comply with timeliness requirements. A few commenters expressed concerns about the logistics of and liability for managing the PHI of prospective patients. One commenter asserted that the proposal would shift the burden of collecting PHI to health care providers, requiring them to mediate between an individual and multiple Disclosers, and expressed concern about the ability of small and rural health care providers, in particular, to perform this function.

Several commenters recommended that the Department clarify the circumstances under which a covered entity would be permitted to deny requests by an individual to submit the individual's access request to another covered entity on the individual's behalf and the processes for issuing denials. Several commenters requested that the Department provide additional information about how to determine when a request provides sufficient information to constitute a valid request. A few commenters requested that the Department clarify that covered entities would be permitted to make the requested disclosures only if consistent with applicable law.

Response: We are not finalizing the proposal to require covered health care providers and health plans (''Requestor-Recipient''), at an individual's direction, to submit to another covered entity (''Discloser'') the individual's request to transmit an electronic copy of the individual's PHI in an electronic health record. We are persuaded by the comments asserting that such a requirement likely would create unreasonable administrative burdens without meaningfully contributing to the Department's efforts to facilitate information sharing among entities in the health care system.[520] However, this does not preclude covered entities from assisting an individual by submitting an access request to another covered entity on the individual's behalf.

7. Adjusting Permitted Fees for Access to PHI and ePHI

a. Current Rule

The Privacy Rule allows covered entities to charge a reasonable, cost-based fee to fulfill access requests from individuals for copies of their PHI. Section 164.524(c)(4) limits the allowable fees to the costs of: (1) labor for copying (whether the PHI is in paper or electronic form); (2) supplies for creating the paper copy or electronic media if requested; (3) postage; and (4) preparing any agreed-upon summary or explanation of the requested PHI.

The labor portion of allowable fees for copying includes only labor for creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, after the PHI that is responsive to the request has been identified, retrieved or collected, and compiled and/or collated, and is ready to be copied.[521] Examples of allowable labor costs include, but are not limited to, costs associated with the following:

- Photocopying PHI that is on paper.
- Scanning PHI that is on paper into an electronic format.
- Converting electronic information in one format to a format requested by or agreed to by the individual.
- Transferring (*e.g.,*uploading, downloading, attaching, burning) ePHI from a covered entity's electronic information system to a web-based portal (where the PHI is not already maintained in or accessible through the portal), portable media, email, app, personal health record, or other manner of delivery of the PHI.
- Creating and executing a mailing or email with the responsive PHI.

Importantly, we recognized in the 2013 Omnibus Rule that covered entities would continue to improve their technological capabilities over time and that the costs of producing an electronic copy would be negligible.[522]

The labor portion of allowable fees for copying does not include costs associated with reviewing the request for access; searching for and retrieving the PHI, which includes locating and reviewing the PHI in the medical or other record; or segregating or otherwise preparing the PHI that is responsive to the request for a copy. Additionally, a covered entity may not pass on the administrative or other costs associated with outsourcing the function of responding to individual requests for access (*e.g.,* the cost of using a business associate to act on individual requests for access).[523]

b. Proposed Rule

The Department proposed to modify the provisions addressing access fees to establish a fee structure with two elements based on the type of access request.[524] The first proposed element described categories of access for which covered entities would not be permitted to charge a fee, and the second described the allowable costs that could be included when an access fee is permitted.[525]

[520] For example, a covered entity must disclose PHI to a person designated by the individual pursuant to the right of access to direct, where applicable. *See* 45 CFR 164.524(d). Additionally, a covered entity is permitted to assist that individual by submitting an access request for PHI to another covered entity on the individual's behalf. *See* 45 CFR 164.524(d)(5)(i). As discussed in Sec. III.B.1, the Department also has announced efforts to enforce the information blocking regulations and to modernize the nation's digital health ecosystem. *See* ''HHS Announces Crackdown on Health Data Blocking,'' *supra* note 7; ''White House, Tech Leaders Commit to Create Patient-Centric Healthcare Ecosystem,'' *supra* note 4.

[521] *See* ''What Labor Costs May a Covered Entity Include in the Fee That May Be Charged to Individuals to Provide Them with a Copy of Their PHI?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #2025 (June 24, 2016), *https://www.hhs.gov/hipaa/for-professionals/faq/2025/what-labor-costs-may-a-covered-entity-include/index.html.*

[522] 78 FR 5632, 5635 (Jan. 25, 2013).

[523] *See* ''May a Covered Entity That Uses a Business Associate to Act on Individual Requests for Access Pass on the Costs of Outsourcing This Function to Individuals When They Request Copies of Their PHI?,'' Office for Civil Rights, U.S. Department of Health and Human Services (June 24, 2016), *https://www.hhs.gov/hipaa/for-professionals/faq/may-a-covered-entity-that-uses-a-business-associate-to-act/index.html.*

[524] 86 FR 6446, 6464 (Jan. 21, 2021).

[525] *Id.* at 6464–65.

The Privacy Rule does not permit fees to be charged for inspection of PHI by the individual who is the subject of the PHI. The Department believes that a covered entity does not incur labor costs for copying and is unlikely to incur more than *de minimis* costs for supplies when providing the individual with the opportunity to inspect PHI in person. The same is true when an individual who, while inspecting their PHI, takes notes, or uses other personal devices or resources to memorialize, record, or otherwise capture the PHI. Likewise, the Department believes that there are circumstances in which a covered entity can provide an individual with access to PHI using technology without the involvement of their workforce members. We refer to such technologies as ''internet-based methods.'' When an individual uses an internet-based method to obtain access to their PHI, the covered entity likely incurs no allowable labor costs or expenses. For example, where an individual requests or agrees to access their PHI available through the View, Download, and Transmit (VDT) functionality of the CEHRT, we believe there are no labor costs and no costs for supplies to enable such access.[526] Thus, for example, a covered health care provider cannot charge an individual a fee when it fulfills an individual's HIPAA access request using the VDT functionality of the provider's CEHRT. Accordingly, at 45 CFR 164.524(c)(4)(ii), the Department proposed to specify two situations that would always be free of charge: (1) when an individual inspects PHI in person; and (2) when an individual uses an internet-based method to view or obtain a copy of their ePHI, including access through the covered entity's certified health IT or by a personal health app connecting to a secure, standards-based API, consistent with applicable Federal or state law.[527]

The Department proposed that access requests by an individual for an electronic or non-electronic copy of PHI through a non-internet-based method would remain subject to the individual access fee limitations of a reasonable, cost-based fee.[528] Accordingly, we proposed to modify 45 CFR 164.524(c)(4)(i) to permit a covered entity to charge a reasonable, cost-based fee, provided that the fee includes only the following costs:

- Labor for copying the PHI requested by the individual in electronic or non-electronic (*e.g.,* paper, film) form.
- Supplies for making non-electronic copies.
- Actual postage and shipping for mailing non-electronic copies.
- Preparing an explanation or summary of electronic or non-electronic PHI, if agreed to by the individual, when an individual requests an electronic or non-electronic copy of PHI about the individual through a non-internet-based method.

As explained above, the fee would not be permitted to include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by state law. Pursuant to the HITECH Act, which limits the fees that a covered entity may impose for providing an individual with an electronic copy of PHI in an electronic health record to the covered entity's labor costs in responding to a request, covered entities would not be permitted to charge individuals for cost of electronic media or postage for providing electronic copies of PHI by any method.[529]

Additionally, we proposed at 45 CFR 164.524(d)(6) to permit covered entities to charge a reasonable, cost-based fee for a request made pursuant to the right of access to direct where the electronic copy would be provided using a method other than an internet-based method, provided that the fee includes only the following costs for labor: (1) copying the PHI requested by the individual in an electronic form; and (2) preparing of an explanation or summary of the ePHI, if agreed to by the individual.[530]

Finally, the Department solicited public comment on whether covered entities should be prohibited from charging fees for copies of PHI when requested to support applications for public benefits or when copies are directed to certain types of entities, such as those conducting clinical research.

c. Overview of Comments

Most commenters expressed general support for prohibiting fees for in-person and internet-based methods of accessing PHI. However, several commenters expressed opposition to prohibiting fees for in-person inspection and internet-based methods of access because they believed that there are costs to covered entities for providing access through either method. In response to the Department's comment solicitation related to public benefits, many commenters urged the Department to prohibit covered entities from charging a fee for a copy of PHI where the purpose of the request is to support an application for public benefits.

d. Final Rule

Consistent with section 13405(e) of the HITECH Act, this final rule adopts the proposal to modify the access fee provisions at 45 CFR 164.524(c)(4)(i) to provide that, where a covered entity is permitted to charge a reasonable, cost-based fee for responding to a request for PHI made pursuant to 45 CFR 164.524(a), the fee can include only the following costs:

- Labor for copying the PHI requested by the individual in electronic or non-electronic (*e.g.,* paper, film) form.
- Supplies for non-electronic copies.
- Actual postage and shipping for mailing non-electronic copies.
- Preparing an explanation or summary of electronic or non-electronic PHI, if agreed to by the individual when an individual requests an electronic or non-electronic copy of PHI about an individual.

Covered entities remain subject to the current limits on access fees for access requests by an individual for a non-electronic copy of PHI. This would include only labor for copying PHI in non-electronic form, supplies for creating the non-electronic copy, actual postage for mailed copies, and the costs of preparing a requested summary or explanation of the PHI. Additionally, they may charge reasonable, cost-based fees for access requests by an individual for an electronic copy of PHI through a method other than an internet-based method, limited to the costs of labor for making electronic copies of the PHI (*e.g.,* copying PHI onto electronic media) and preparing a summary or explanation as agreed to by the individual.

Additionally, this final rule adopts the proposal to modify 45 CFR 164.524(c)(4)(ii) to prohibit fees for in-person inspection and use of an internet-based method to view or obtain a copy of ePHI maintained by or on behalf of a covered entity. This change is consistent with section 13405(e) of the HITECH Act and the modification that we are making in this final rule to 45 CFR 164.524(c)(4)(i) to limit the fees that individuals may be charged for

[526] 45 CFR 170.315(e)(1); *see* 85 FR 25642, 25691 (May 1, 2020); 80 FR 62602, 62658 (Oct. 16, 2015); *see also* ''Quality Payment Program: Merit-Based Incentive Payment System (MIPS) Promoting Interoperability Performance Category Measure—2023 Performance Period,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (last accessed Mar. 16, 2026), *https://qpp.cms.gov/docs/pi_specifications/Measure%20Specifications/2025-MIPS-Promoting-Interoperability-Measure-Provide-Patients-E-Access-to-Their-Health-Info.pdf.*

[527] 86 FR 6446, 6465 (Jan. 21, 2021).

[528] *Id.*

[529] *See* sec. 13405(e) of the HITECH Act.

[530] 86 FR 6446, 6465 (Jan. 21, 2021).

copies of their PHI to the costs described above. As discussed above, the Department believes that a covered entity does not incur labor costs for copying and is unlikely to incur more than *de minimis* costs for supplies when providing an individual with the opportunity to inspect, that is, review their PHI, rather than providing them with a copy.[531] Where the individual requests a copy of their PHI from the covered entity during an in-person inspection, the request should be viewed as an exercise of the individual's right to obtain a copy, subject to the fee limitations of that right, rather than the continued exercise of the individual's right to inspect their PHI.

Similarly, because we intend the term ''internet-based method'' to refer to internet-based processes for responding to requests for access automatically (*e.g.,* using VDT in a patient or health plan member portal, or a personal health app connection via a certified API technology), the Department anticipates that there will not be more than *de minimis* labor costs for copying the PHI that an individual requests using an internet-based method. We do not intend for the term internet-based method to include methods that provide an individual with their PHI, pursuant to the right of access, through the internet where there are labor costs for copying associated with the provision of the PHI in the form and format requested by the individual (*e.g.,* where a PDF is emailed to the individual at the request of the individual). Additionally, we do not anticipate that there will be supplies used to make non-electronic copies, or postage or shipping costs for mailing non-electronic copies, where an individual obtains access through the right of access to inspect or through an internet-based method.

Accordingly, this final rule supersedes the Department's previous interpretation of how to calculate the fees for copies of PHI provided in response to requests made pursuant to the right of access, including the explanation of the three methods for calculating this fee: actual costs, average costs, or a flat fee of $6.50, as provided in the 2016 guidance. Instead, in this final rule, we explain how covered entities are to calculate a reasonable, cost-based fee. Specifically, covered entities are permitted to charge individuals for the following costs in response to a request for access:

- Labor for copying the requested PHI.
- Supplies for creating a non-electronic copy of the requested PHI, where requested.
- Postage, where the individual has requested that a non-electronic copy, or a summary or explanation, be mailed.
- Preparing an explanation or summary of the PHI, if agreed to in advance by the individual.

The final rule provides covered entities with a ceiling of what can be charged for copies of PHI provided pursuant to the right of access, rather than a floor. Nothing in this final rule prevents regulated entities from charging individuals less than the maximum fee permitted under this final rule, and as discussed below, other laws may limit such fees even further. In particular, the Department encourages covered entities to consider the financial circumstances of the individual requesting the copy of PHI when determining whether it would be appropriate to charge the individual the maximum fee permitted by the Privacy Rule.

The modification to not permit fees for access when such access is provided through an internet-based method aligns with the Fees Exception to information blocking regulations, which does not protect an actor's practice of charging an individual (or their personal representative) a fee that is based in any part on electronic access to an individual's EHI[532] (*e.g.,* ePHI) by the individual or their personal representative.[533]

We are not addressing the proposal to limit the fees that a covered entity is permitted to charge in response to a request made pursuant to the right of access to direct in this final rule. We will continue to monitor the landscape with respect to the fees charged by covered entities for copies of PHI provided in response to a request made pursuant to the right of access to direct.

e. Responses to Public Comments

Comment: A few commenters expressed concern about the proposal to prohibit fees for in-person inspection of PHI, asserting that permitting individuals to inspect their PHI in-person would require a commitment of resources by covered entities, including staff and space. A few commenters requested that the Department establish limits on the number of paper copies that covered entities are required to provide for free. Other commenters expressed support for the proposal to prohibit covered entities from charging fees for access through patient portals but asserted that there may be costs for providing electronic copies of PHI when such access is through an internet-based method other than a patient portal. For example, a few commenters stated that resources generally are required to collect and merge records that are maintained in different electronic formats into a single record.

Response: As discussed elsewhere, we are not finalizing the proposal to modify the right to inspect. However, the right of an individual to inspect their PHI is a longstanding provision that remains in the Privacy Rule as part of the right of access, and nothing in this rule will increase costs to covered entities for providing such access. As discussed above, we do not believe that a covered entity incurs labor costs for copying PHI, or more than *de minimis* costs for supplies for creating a copy, when an individual exercises their right to inspect; thus, we are adopting our proposal not to permit a covered entity to impose a fee for such access.

While the Privacy Rule permits a covered entity to charge a fee in other circumstances, the Department encourages covered entities to provide individuals who request access to their information with copies of their PHI free of charge wherever possible. Providing individuals with access to their health information is a necessary component of delivering and paying for health care, and providing access to PHI for free is particularly vital in circumstances where the financial situation of an individual requesting access makes it difficult or impossible for the individual to afford the fee.

The Department believes that prohibiting fees for in-person inspection and internet-based methods of access is appropriate because we expect that such methods of access will generate at most nominal costs for which covered entities are permitted to charge individuals under the Privacy Rule, as modified by section 13405(e) of the HITECH Act. As discussed above, the Privacy Rule does not permit a covered entity to charge a fee for reviewing a request for access; searching for and retrieving the PHI, which includes locating and reviewing the PHI in the medical or other record; or segregating or otherwise preparing the responsive PHI, whether in electronic or non-electronic form. However, we emphasize that the requirement to provide free access does not apply to circumstances where the individual is using an online portal to submit a request for copies of PHI to be

[531] Such *de minimis* costs may include the cost of copying where the covered entity decides to make a copy to help fulfill an individual's request to inspect their PHI.

[532] *See* 45 CFR 171.102 (definition of ''Electronic health information'').

[533] *See* 45 CFR 171.302(a)(1)(ii) and (b)(2); 85 FR 25642, 25879–88 (May 1, 2020).

sent to him or her in a manner that would require the covered entity to incur costs for labor for copying, supplies, or postage that could be the basis for a reasonable, cost-based fee.

Comment: A few commenters expressed opposition to the Department's proposal to limit fees for providing PHI on portable electronic media to individuals to labor costs only. According to the commenters, covered entities should be permitted to charge individuals fees that cover any reasonable costs of providing access, including labor, supplies, media, or postage.

Response: We are finalizing the proposal to limit the fee that a covered entity is permitted to charge an individual for providing access to PHI on portable electronic media to labor costs only, consistent with a plain reading of section 13405(e) of the HITECH Act, as discussed above.[534] Covered entities are permitted to include, as part of a reasonable, cost-based fee, labor costs for copying PHI in an electronic health record to another electronic format (such as a PDF) or onto electronic media (*e.g.,* CD, USB drive), if requested by the individual or their personal representative.

Comment: Many commenters who receive access requests stated that they receive almost no requests for access via internet-based methods because almost all of the requests that they receive require manual processing. One commenter asserted that not all health care providers have the ability to electronically exchange PHI, which, according to the commenter, means that the proposal would lead to higher costs for those providers for providing access via internet-based methods.

Response: The Department interprets the term internet-based method to apply to the use of technology that relies on the internet, such as patient and health plan member portals, personal health apps, and APIs, as well as similar successor technologies, to obtain a copy of PHI without requiring a member of the covered entity's workforce to invest labor in making such a copy. As explained in the 2021 Privacy Rule NPRM, the Department does not intend to require covered entities to provide free access where the individual simply is using an online portal to submit a request for copies of PHI to be sent to the individual in a manner that would require the covered entity to incur allowable costs for supplies, postage, or labor for copying. The submission of an access request through an electronic method, or a request for electronic delivery of a copy, does not by itself mean that the individual is using an internet-based method for which no fee may be charged. Instead, as discussed above, the Department intends the term ''internet-based method'' to refer to automated processes for transmitting electronic copies. It does not include circumstances that involve labor for making copies on the part of a member of the covered entity's workforce.

One example of an internet-based method is using certain functionality of certified health IT to obtain copies of PHI (*e.g.,* using VDT in a patient or health plan member portal or a personal health app connection via a certified API technology). However, using certified health IT or certain functionality of the certified health IT is not a requirement for obtaining an electronic copy of PHI using an internet-based method. Providing an individual with a copy of ePHI that is in the USCDI through a personal health app that connects to a covered entity's secure, standards-based API is another example of an internet-based method. By contrast, an individual's request that a covered entity provide such individual with an electronic copy of PHI, that is not ePHI, through their personal health app, would not be a request to obtain PHI through an internet-based method because it would require a member of the covered entity's workforce to copy the PHI into an electronic form and format.

As discussed elsewhere in this final rule, the Privacy Rule does not require a covered entity to provide an individual with their PHI in a particular electronic form and format. However, the Privacy Rule does require a covered entity to provide an individual with their PHI in the electronic form and format requested by the individual if the requested PHI is readily producible in that form and format. Thus, if the individual requests that a copy of their PHI be sent to them using an internet-based method (*e.g.,* VDT or personal health app through a secure, standards-based API) and the requested PHI is available in that requested form and format, the covered entity must provide it to the individual (or their personal representative) in that form and format for free.

Comment: A few commenters recommended that the Department align its fee proposals with other Federal regulations, such as the information blocking regulations and the Interoperability and Patient Access Final Rule, while taking into consideration the financial implications for individuals and regulated entities. A few commenters requested guidance on how to apply the Privacy Rule's limitations on fees in states that also have laws that limit the fees that covered entities are permitted to charge for disclosures of PHI.

Response: The information blocking regulations are designed to operate in a manner consistent with the framework of the Privacy Rule and other laws providing privacy rights for patients, but are separate and distinct from such statutes and regulations. The information blocking regulations exclude from the definition of information blocking certain fees that an actor[535] elects to charge for the access, exchange, or use of EHI. The Fees Exception is available for fees for individual access to their EHI when its conditions are met as specified in the exception.[536] However, as ONC has explained, an actor's practice of charging an individual, their personal representative, or another person designated by the individual for electronic access to the individual's EHR would be inherently suspect under an information blocking review.[537] CMS's Interoperability and Patient Access Final Rule also includes certain fee limitations.[538]

With respect to state law, Congress provided that standards, requirements, and implementation specifications adopted under HIPAA would supersede any contrary provision of state law, with certain limited exceptions, such as for state privacy laws that are contrary to and more stringent than the corresponding Federal standard, requirement, or implementation specification.[539] Accordingly, unless a specific exception applies, a state law that is contrary to the Privacy Rule is preempted by the Federal requirements.

HIPAA excepts from its general preemption authority contrary provisions of state law that impose requirements, standards, or implementation specifications that are more stringent than those of the Privacy Rule.[540] Under the HIPAA Rules, with respect to the rights of an individual who is the subject of the PHI, more stringent laws include state laws that permit greater rights of access (*e.g.,* state law provides stricter limits on the fees that a covered entity is permitted to

[534] Sec. 13405(e) of the HITECH Act (codified at 42 U.S.C. 17935(e)).

[535] 45 CFR 171.102 (definition of ''Actor'').

[536] *See* 45 CFR 171.302.

[537] 85 FR 25642, 25792 (May 1, 2020); *see also* 85 FR 25886–87 (May 1, 2020).

[538] *See* 85 FR 25510 (May 1, 2020).

[539] *See* Health Insurance Portability and Accountability Act of 1996, sec. 264(c)(2) of Public Law 104–191, 110 Stat. 2033 (codified at 42 U.S.C. 1320d–2 note); 45 CFR 160.203(b).

[540] *See* 45 CFR 160.203(b).

charge for providing an individual with a copy of their PHI).[541] Thus, HIPAA does not override state laws that provide individuals with greater rights of access to their health information than the Privacy Rule does.[542] This includes state laws that: (1) prohibit fees for providing individuals with copies of their PHI; or (2) allow only lesser fees than what the Privacy Rule would allow to be charged for copies. Additionally, where it is possible for regulated entities to comply with both the state or other Federal law and the Privacy Rule (*e.g.,* where a state or other Federal law provides stricter limits on the fees that a covered entity is permitted to charge for providing an individual with a copy of their PHI), there is no conflict between the laws, and no preemption of the state law.[543]

Comment: Many commenters asserted that individuals should not be charged for transfers of PHI between health care providers. One commenter asserted that this proposal would decrease the ability of health care providers to provide free responses to requests for PHI related to health care.

Response: The Privacy Rule does not expressly address fees for disclosures between covered entities, such as provider-to-provider exchanges.[544]

The Department does not intend to change how covered entities charge for disclosing records to other covered entities. It is the Department's understanding that there frequently is no charge for permitted disclosures of PHI to another covered entity for core health care activities such as TPO. Furthermore, in some circumstances, other Federal or state laws may limit or restrict such charges.[545] The finalized provision is not intended to cause covered entities to begin charging fees for such disclosures; rather, its purpose is to recognize individuals as the center of their own health care and empower individuals to identify persons that they wish to have electronic copies of their PHI in an electronic health record.

Comment: Several commenters recommended that covered entities should be limited to charging indigent individuals who request their PHI to support an application for disability benefits $10.50 for electronic records and $20–$30 for paper records.

One commenter expressed support for providing copies of PHI for free, on a cost basis, or for $6.50 to individuals, providers, and personal representatives. A few commenters stated that charging $6.50 for anyone requesting copies of PHI would cause hospitals and medical offices to lose revenue.

One commenter requested that the Department establish a set fee for copies of PHI that is reasonable and cost-based to alleviate uncertainty, but asserted that $6.50 was insufficient because it was unusual to be asked to produce only ePHI. Instead, the commenter urged the Department to set a separate flat rate fee for copies of PHI that is non-electronic and to allow covered entities to charge either $6.50 or the separate fee for PHI that is not electronic where the request includes both ePHI and PHI that is not ePHI.

Some commenters expressed support for a flat rate of $6.50 for individuals, especially for electronic records. A few commenters expressed support for providing covered entities with the option of charging either the flat rate or using other methods to calculate fees. One commenter stated that it charged a flat rate of $6.50 for patients' right of access. According to the commenter, for requests that involve both ePHI and PHI that is not electronic, it charged a workers' compensation rate for paper records, a reduced half rate for electronic records, or, when applicable, a state-specific fee schedule.

A few commenters expressed opposition to the $6.50 rate because they believed that the amount was too low, unreasonable, or arbitrary. According to one commenter, retrieving records could take many hours or days, and the flat rate did not cover even half of the commenter's hourly rate for such record retrieval.

A few commenters stated that the $6.50 flat rate is too high for providing electronic records, which incurs little to no cost, or for requests for only one page, for example. One commenter noted that the flat rate would also be too low for someone requesting many pages.

Response: As explained above, in 2016, in response to requests for clarification, the Department issued guidance on how to calculate the limited fees that covered entities were permitted to charge individuals to provide them with a copy of their PHI. The guidance explained that covered entities could use any of three methods for calculating this fee: actual costs, average costs, or a flat fee of $6.50; and explained each option in detail. In the 2021 Privacy Rule NPRM, we sought comments on how covered entities were calculating allowable access fees and whether the Department should specify one or more of the methods included in the 2016 guidance, or another method, in regulatory text as the exclusive acceptable method(s) of calculating access fees.

Consistent with section 13405(e) of the HITECH Act, we are finalizing the proposal to permit covered entities to charge for requests made pursuant to 45 CFR 164.524(a), in certain circumstances, a reasonable, cost-based fee that includes only the cost of the following:

- Labor for copying the requested PHI.
- Supplies for creating a non-electronic copy of the requested PHI, where requested.
- Postage, where the individual has requested that a non-electronic copy, or a summary or explanation, be mailed.
- Preparing an explanation or summary of the PHI, if agreed to by the individual.

A covered entity is not permitted to impose a fee where an individual inspects PHI about themselves or accesses ePHI maintained by or on behalf of the covered entity using an internet-based method, such as a personal health app or patient or health plan member portal.

Accordingly, this final rule supersedes the Department's previous interpretation of how to calculate the fees for copies of PHI provided in response to requests made pursuant to the right of access, including the explanation of the three methods for calculating this fee: actual costs, average costs, or a flat fee of $6.50, as provided in the 2016 guidance. The rule explains how covered entities are to calculate a reasonable, cost-based fee. It provides covered entities with a ceiling of what can be charged for copies of PHI provided pursuant to the right of access, rather than a floor. Nothing in this final

---

[541] *See* 45 CFR 160.202 (definition of ''More stringent'' at paragraph (2)).

[542] *See* 45 CFR 160.202; 160.203.

[543] *See also* ''A State law requires that a health care provider give individuals one free copy of their medical records but HIPAA permits the provider to charge a fee. Does HIPAA override the State law?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #2032 (June 24, 2016), *https://www.hhs.gov/hipaa/for-professionals/faq/2032/a-state-law-requires-that-a-health-care-provider-give-individuals/index.html.*

[544] Covered entities generally are prohibited from selling PHI. *See* 45 CFR 164.502(a)(5)(ii). Unless otherwise specified in 45 CFR 164.502(a)(5)(ii), covered entities are limited to charging a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for a permitted purpose or a fee otherwise expressly permitted by other law.

[545] For example, Arizona prohibits a health care provider or contractor from charging fees to another health care provider for the purpose of providing continuing care to the patient to whom the medical record pertains. *See* Ariz. Rev. Stat. 12–2295(B)(1). As another example, in Maine, a health care entity may not require any fee for the transfer of any medical records related to a patient between health care entities unless the fee is disclosed to the patient and is directly related to the actual transfer costs. *See* 22 Me. Rev. Stat. 1718–E (Prohibition on fees for transferring a patient or a patient's medical records).

rule prevents regulated entities from charging individuals less than the maximum fee permitted under this final rule, and as discussed above, other laws may limit such fees even further.

The Department encourages covered entities to consider the financial circumstances of the individual requesting the copy of PHI when determining whether it would be appropriate to charge the individual the maximum fee permitted by the Privacy Rule. Ensuring individuals' access to their PHI is not solely about ensuring that they have the ability to request and obtain their health information in the form and format that they want in a timely manner; it is also about ensuring that such access is affordable. When the fee for obtaining access exceeds an individual's ability to pay that fee, the right of access may be rendered meaningless. A 2018 Government Accountability Office (GAO) report on challenges associated with individual access found that ''high fees can adversely affect patients' access to their medical records.'' [546] According to a patient advocate interviewed by the GAO, some patients cancel their requests when they learn of the potential costs.[547] Another advocate highlighted the inability of patients to afford the fees for access to their medical records, even where such fees are permitted under the Privacy Rule or applicable state law, particularly in situations where seriously ill patients have accumulated voluminous medical records.[548] Charging fees in these circumstances may be particularly concerning when fulfilling an individual's access request imposes minimal or no burden on a covered entity. For example, when PHI generally is available electronically, a covered entity may incur minimal or no costs in providing access to the requested PHI, yet the fees charged to individuals may still be unaffordable relative to their financial circumstances. In such cases, the fees charged may create a barrier to an individual's exercise of the right of access. Thus, affordability may affect an individual's ability to meaningfully exercise the right of access.

While we are not adopting a prohibition in this rule against charging a fee to an individual (or their personal representative) who seeks a copy of their PHI to support the individual's application for public benefits, we will continue to monitor the landscape with respect to access to PHI for these purposes and consider ways to facilitate applications for public benefits. Public benefit programs or government-funded assistance programs, such as Medicaid, Supplemental Nutrition Assistance Program (SNAP), Social Security Disability Insurance (SSDI), Supplemental Security Income (SSI), VA benefits, and housing assistance, generally provide individuals with limited means assistance with paying for basic living expenses (*e.g.,* food, health care, housing, utilities).[549] Individuals seeking records to support an application for such benefits may have limited financial resources and may be unable to afford fees for copies, particularly where their medical records are lengthy.[550] In such cases, fees may create a barrier to an individual's exercise of the right of access. Although we are not adopting a prohibition in this final rule, the Department encourages covered entities to consider individuals' financial circumstances and to limit fees where possible when a copy of PHI is requested to support an application for public benefits.

Separate requirements to provide individuals with notice of fees for copies of PHI provided pursuant to the right of access and a valid authorization are discussed below.

Comment: Commenters requested that the Department provide guidance on fees that covered entities are permitted to charge for providing PHI under the right of access and via an authorization.

Response: Fees for disclosures pursuant to an authorization generally are limited to: (1) a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI pursuant to the authorization; or (2) a fee otherwise expressly permitted by other law.[551] (If the covered entity wishes to charge a higher fee, the authorization must state that the disclosure will result in remuneration to the covered entity as required by 45 CFR 164.508(a)(4).[552]) The chart below provides a summary of how different types of disclosures and recipients of the PHI affect the fees that the Privacy Rule permits covered entities to charge for copies of PHI provided in response to 45 CFR 164.524(a). As explained above, we are not addressing allowable fees for copies provided to a person designated by an individual pursuant to 45 CFR 164.524(d).

[546] ''Medical Records: Fees and Challenges Associated with Patients' Access,'' GAO–18–386, Government Accountability Office, p.14 (May 2018), *https://www.gao.gov/assets/gao-18-386.pdf.*

[547] *Id.*

[548] *Id.*

[549] *See* ''Government benefits,'' U.S. General Services Administration (last accessed Mar. 3, 2026), *https://www.usa.gov/benefits.*

[550] For example, to obtain SSDI, individuals must be: (1) unable to engage in any substantial gainful activity because of a medically determinable physical or mental impairment; or (2) aged 55 or older, blind, and unable to work as a result. *See* 42 U.S.C. 416(i)(1); 42 U.S.C. 423(d)(1)(B). For 2026, to be eligible for SSDI, individuals cannot earn more than $1,690 per month from work, or $2,830 per month if the individual is blind. *See* ''Substantial Gainful Activity,'' U.S. Social Security Administration (last accessed Jan. 20, 2026), *https://www.ssa.gov/oact/cola/sga.html.* To qualify for SSI, individuals must meet all three of the following conditions: (1) be aged 65 or older or have a disability; (2) have an income that is less than the statutorily established threshold; and (3) have resources of less than the statutorily established threshold. *See* 42 U.S.C. 1382. Today, the income limit is generally $2,019 from work each month for individuals. *See* ''Who can get SSI,'' U.S. Social Security Administration (last accessed Jan. 20, 2026), *https://www.ssa.gov/ssi/eligibility.* The limit increases for couples and for children. *Id.*

[551] 45 CFR 164.502(a)(5)(ii)(B)(viii).

[552] 45 CFR 164.502(a)(5)(ii)(A).

Relevant Provision of the Privacy Rule	Type of Disclosure	Recipient of PHI	Allowable Fee
Right to inspect 45 CFR 164.524(a)	In-person inspection	Individual (or personal representative)	Free
Right of access 45 CFR 164.524(a)	Internet-based method of receiving copies of PHI (*e.g.*, using VDT, or a personal health app connection via a secure, standards-based API)	Individual (or personal representative)	Free
Right of access 45 CFR 164.524(a)	Non-internet-based method of receiving an electronic copy of PHI, in response to an access request (*e.g.*, by sending PHI copied onto electronic media through the U.S. Mail or via certified export functionality)[a]	Individual (or personal representative)	Reasonable, cost-based fee, limited to costs of labor for: (1) making copies
Right of access 45 CFR 164.524(a)	Non-electronic copy of PHI	Individual (or personal representative)	Reasonable, cost-based fee, limited to costs of: (1) labor for making copies; (2) supplies for copying; and (3) actual postage and shipping
Right of access 45 CFR 164.524(a)	Summary or explanation agreed to by the individual	Individual (or personal representative)	Reasonable, cost-based fee, limited to costs of: (1) labor for making copies; (2) supplies for copying; and (3) actual postage and shipping; and (4) preparing the summary or explanation as agreed to by the individual

8. Notice of Access and Authorization Fees

a. Issues To Address

As discussed above, the Privacy Rule allows covered entities to charge fees for copies of PHI in certain circumstances. Where a covered entity intends to charge an individual the limited fee that is permitted under the Privacy Rule, the covered entity should inform the individual in advance and should negotiate any details that will affect the form and format of the PHI that is produced in response to a request for access. Failure to provide advance notice of a fee may serve as a barrier to access because it deprives the individual of the opportunity to decide whether they need all of the requested PHI, or whether they can accomplish their purpose with only a subset of that PHI, particularly if the cost of the requested PHI is prohibitive. However, the Privacy Rule does not require a covered entity to provide an individual with advance notice of such fees, meaning that individuals and others often are surprised when they are charged fees for such copies that are significantly higher than they expect, and in some cases, can afford. In such circumstances, disputes could be avoided if the covered entity provided the individual with advance notice of any fees and the opportunity to modify their request. The Department has received anecdotal reports that individuals often lack clarity about the charges for copies of their PHI and that fee practices vary across covered entities.

b. Proposed Rule

To address these concerns and promote transparency and uniform application of the fee limitations, the Department proposed a new section at 45 CFR 164.525(a) that would require a covered entity to provide an individual with advance notice of approximate fees for copies of PHI under the right of access and with a valid authorization. Proposed 45 CFR 164.525(a)(1) would require covered entities to post a fee schedule on their website, if they have one, and make the fee schedule available to individuals at the point of service and upon request. It also would require the notice to include all types of access that are available free of charge and include a fee schedule specifying the standard fees for all of the following:

- Copies of PHI provided to individuals under the individual right of access, with respect to all readily producible electronic and non-electronic forms and formats for such copies.
- Copies of PHI about an individual in an electronic health record and directed to persons designated by the individual, with respect to all readily producible electronic forms and formats for such copies.
- Copies of PHI sent to a specified recipient with the individual's valid authorization, with respect to all available forms and formats for such copies.

The Department also proposed at 45 CFR 164.525(a)(2) to require that covered entities provide an individualized estimate to an individual of the approximate fees to be charged for the requested copies of PHI, upon request. Additionally, the Department proposed at 45 CFR 164.525(a)(3) to require covered entities to provide, upon an individual's request, an itemization of the charges for labor for copying, supplies, and postage, as applicable, which would constitute the total fee charged to the individual for copies of PHI.

c. Overview of Comments

Commenters expressed mixed views on these proposals. Many commenters asserted that advance notice of applicable fees would promote transparency, reduce the potential for unanticipated fees, and assist individuals in making decisions regarding their requests for copies of PHI. Generally, these commenters also stated that requiring information about standard fees to be publicly available would facilitate understanding of and compliance with the Privacy Rule's fee limitations.

Some commenters expressed opposition to all or parts of the proposal because they believed that it would pose a significant burden for covered entities and would be infeasible to implement. Some commenters also recommended that the Department clarify when itemized statements would be required and whether covered entities would be permitted to charge for the preparation of individualized estimates or itemized statements.

d. Final Rule

The Department finalizes proposed 45 CFR 164.525, with modifications discussed below, to require covered entities to provide advance notice of fees for copies of PHI requested under the right of access, including the right of access to direct, and for copies of PHI requested pursuant to a valid authorization. We are not finalizing the proposals to require that covered entities provide individualized estimates and itemized statements upon request. Specifically, the Department is finalizing 45 CFR 164.525 to require a covered entity to post a fee schedule on its website, if it has a website, and to make the fee schedule available to individuals at the point of service. As explained in the 2021 Privacy Rule NPRM, the Department expects that a covered entity will make their fee schedule available upon request, in paper or electronic form, at the point of service or at an office that is responsible for releasing medical records, and, as applicable, to provide such information verbally (*e.g.,* over the telephone). Making the fee schedule available at the point of service or a medical records office and upon request could include, for example, any of the following: posting the fee schedule on the wall, leaving paper copies on a table in the waiting room, keeping a copy at the reception desk to show an individual who requests it, printing a copy to give to an individual who requests it—or, if the individual requests an electronic copy of the fee schedule, emailing a copy to the individual. For covered entities, the point of service also could include a customer service call center that handles requests for records, or any location at which PHI is made available for individuals to inspect, as required under 45 CFR 164.524(a).

The Department also is adopting the proposal to require that the notice identify all types of access that are available free of charge and include a fee schedule specifying the standard fees that may be charged for copies of PHI provided under 45 CFR 164.524(a), for electronic copies requested pursuant to the right of access to direct at 45 CFR 164.524(d), and for disclosures pursuant to a valid authorization under 45 CFR 164.508. The standard fees included in the fee schedule are the charges associated with components of the fees for copies provided pursuant to the right of access and a valid authorization and how the covered entity uses those charges to determine the total fee. For example, to the extent that a covered entity charges fees for the following costs, the fee schedule must contain the covered entity's charge for labor for making a paper copy of an individual's PHI in response to a right of access request, the costs of any supplies that may be used to make non-electronic copies of the requested PHI, postage fees for mailing the non-electronic copy, any charges associated with preparing an explanation or summary of an individual's PHI when agreed to by the individual, as applicable, and explain that those charges are added together to determine the total fee.[553] Fees for labor may be displayed on the fee schedule as hourly charges.

The fee schedule also must list information about the circumstances in which covered entities are required to provide copies of PHI for free. Covered entities are encouraged to provide individuals with a fee schedule that is easy to understand and enables them to identify the most appropriate mechanism for requesting PHI. The Department recommends that, where possible, covered entities inform individuals, in advance, about average costs for copies of PHI that are commonly requested; however, this final rule does not require covered entities to do so.

The Department believes that requiring covered entities to make a fee schedule publicly available and accessible at the point of service is consistent with the goal of this Administration to increase pricing transparency in health care.[554] We believe that making the fee schedule publicly available and accessible at the point of service will increase individuals' awareness of potential charges for obtaining copies of their PHI, including when directing electronic copies of their PHI pursuant to the right of access to direct, and assist individuals in making decisions about the scope of their requests for copies of their PHI. The Department also believes that providing individuals with notice of a covered entity's standard fees in advance will promote consistency in how information about permissible fees

[553] 45 CFR 164.524(c)(4).

[554] *See, e.g.,* E.O. 14221, 90 FR 11005 (Feb. 28, 2025).

is made available. Additionally, we believe that readily available information about access fees will promote compliance with the Privacy Rule because covered entities will seek to avoid posting fee schedules that demonstrate noncompliance with the Privacy Rule's fee limitations or publicly misrepresent their business practices. Publicly posting information about fees also will empower individuals to insist on covered entities' compliance with such limitations.

The Department expects that this requirement will provide greater predictability regarding costs for copies of PHI and reduce the likelihood that individuals will encounter surprise charges, thereby supporting individuals' access to and use of their PHI. The Department also expects that the implementation of the requirement to post a general fee schedule will not impose substantial new operational burden because many covered entities already provide such a fee schedule and we assume that covered entities have a fee schedule for their own internal use, even if they do not post it publicly. Additionally, implementation of this requirement generally will be limited to making the covered entity's fee schedule available in a format that is understandable for individuals and others.

Finalizing these provisions does not give a covered entity the ability to withhold or deny an individual access to their PHI on the grounds that the individual has not paid the bill for health care services that the covered entity provided to the individual. As discussed elsewhere in this final rule, the ability of an individual to access their PHI is essential to the primary goals of HIPAA and the HITECH Act, one of which is a health care system that ensures the best possible outcomes for individuals in a manner that limits administrative burdens. The right of access ensures that individuals have an opportunity to identify and correct errors in their PHI [555] and fosters trust, transparency, and understanding between the individual and their health care providers.[556] This is why covered entities are permitted to make disclosures in certain circumstances, but are required to make disclosures when a request is made by the individual pursuant to the right of access. Covered entities may deny an access request only under one of the narrow exceptions specifically enumerated in the Privacy Rule.[557] None of the exceptions permit a covered entity to withhold or deny an individual's request made pursuant to the right of access because the individual has not paid for health care services provided to them by the covered entity.

The Department is not adopting the proposals to require individualized estimates or itemized statements of charges. We find persuasive the comments asserting that these proposals would require substantial operational changes and costs, as discussed below. The Department has determined that requiring a publicly available fee schedule provides an appropriate level of transparency and additional requirements are not warranted at this time, given the potential burden that they would impose.

e. Responses to Public Comments

Comment: Several commenters expressed support for the proposal because they believed that it would support price transparency and clarify applicable fees.

Some commenters expressed opposition to the proposal because they believed that it would be difficult or burdensome for health care providers to implement the requirements. One commenter asserted that the proposals to divide the right of access into the right of access and the right of access to direct would make it challenging for workforce members to identify which fee provisions apply, making it difficult to provide individualized fee estimates.

Several commenters raised concerns about the proposed requirements to provide individualized fee estimates and itemized statements. One commenter asserted that the proposals to require individualized estimates and itemized bills would be administratively burdensome and urged the Department to provide additional time to implement this proposal, if adopted. One commenter recommended that the access timeframes be tolled when an individual requests an individualized estimate.

A few commenters requested that the Department provide greater specificity about the circumstances in which covered entities would be required to provide an itemized statement of charges. One commenter recommended that covered entities be permitted to charge individuals a reasonable, cost-based fee for preparation of the advance estimate of fees and itemized bill.

Response: As discussed above, the Department is finalizing the proposal to require covered entities to post a fee schedule on their website, if they have one, that contains information about the standard fees for copies of PHI provided pursuant to the right of access to inspect and obtain a copy, the right of access to direct, and a valid authorization. We are also finalizing the proposal to require covered entities to make the fee schedule available to individuals at the point of service and upon request. We believe that this will promote transparency and clarify the fees that covered entities are permitted to charge for copies of PHI, in addition to assisting individuals in understanding the potential costs for copies of PHI, and will support compliance with the Privacy Rule's existing fee limitations. The Department expects that because many covered entities already maintain and provide fee schedules for copies of PHI, implementation of this requirement will require limited effort beyond making such schedules of standard fees publicly available.

The Department anticipates that the requirement to make a general fee schedule publicly available and accessible at the point of service will promote administrative efficiency. Standard fee schedules reduce the need for workforce members to respond to ad hoc inquiries regarding permissible charges and to provide repeated explanations of applicable fees.

At the same time, we are persuaded by commenters that expressed concern about the administrative and financial burdens associated with the proposed requirements to provide individualized fee estimates and itemized statements upon request. We find convincing the comments asserting that the implementation of these requirements would require substantial workflow changes and resources to enable workforce members to make request-specific determinations regarding the applicable fee provisions and to provide individualized calculations for each access or authorization request. Accordingly, the Department is not finalizing the proposals to require individualized estimates and itemized statements upon request.

The requirement to make a fee schedule publicly available and accessible at the point of service does not require covered entities to make request-specific determinations or apply different fee limitations on a case-by-case basis, meaning that it can be implemented without the level of operational burden that would be imposed by the proposal to require individualized estimates and itemized

[555] The Privacy Rule provides individuals with the right to request that a covered entity amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set. *See* 45 CFR 164.526.

[556] 65 FR 82462, 82605–07 (Dec. 28, 2000).

[557] 45 CFR 164.524(a)(3) and (4); *see also* 65 FR 82556 (Dec. 28, 2000).

statements upon request. Thus, the Department concludes that the implementation timeframe provided is sufficient and does not warrant extension.

Because the Department believes that providing individuals with access to their PHI is an important component of delivering and paying for health care, we continue to encourage covered entities to waive permissible fees for copies of PHI or provide flexibility in payment (*e.g.,* delaying charges or accepting payment in installments, without delaying the provision of copies) for individuals who are unable to pay upfront or at all because of an emergency or a demonstrated financial hardship.

9. Modifying the General Rules for Required Disclosures of PHI by Business Associates

a. Current Rule

Section 164.502(a)(4)(ii) requires a business associate to disclose PHI to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under 45 CFR 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of their PHI.

b. Proposed Rule

The Department proposed to add language to 45 CFR 164.502(a)(4)(ii) to clarify when a business associate must disclose PHI and to whom. Specifically, the proposed modification would clarify that a business associate is required to provide access to PHI directly to the individual (or the individual's personal representative),[558] or a person designated by the individual (subject to the limitations of the right of access to direct), if the business associate agreement provided that the business associate would provide such direct access. We explained that the proposed clarification was consistent with preamble to the 2013 Omnibus Rule [559] and subsequent guidance [560] and was not intended to be a substantive change.

c. Overview of Comments

Most commenters expressed support for this proposal. According to a few commenters, the proposed modification would clarify the role of a business associate with respect to requests for access, particularly considering the increasing maintenance of PHI by business associates. One commenter explained that the proposed modification would clarify the relationship between covered entities and business associates without creating unnecessary burden for either party. Another commenter asserted that the proposal would simplify business associate agreements and improve relationships between covered entities and business associates. A few commenters expressed opposition to the proposal because they believed that it would be inconsistent with the Cures Act and the requirements of the information blocking regulations.

d. Final Rule

The Department adopts the proposed revision of 45 CFR 164.502(a)(4)(ii) without modification, codifying our longstanding interpretation of this provision.[561]

While a covered entity is directly responsible for providing individuals access to their health information, a business associate may disclose PHI for purposes of the right of access to the individual (or personal representative) or the individual's designee when the terms of the business associate agreement expressly permit or require the business associate to disclose PHI on behalf of a covered entity for purposes of fulfilling an individual's right of access. The business associate agreement controls whether the business associate must disclose PHI either to the individual or individual's designee, or to the covered entity. This final rule clarifies that regulated entities should address in their business associate agreements which party is responsible for disclosing the requested PHI to an individual or their designee for purposes of the right of access.

Longstanding guidance explains that business associate agreements should specify whether the business associate is allowed to disclose PHI directly to an individual or an individual's designee to satisfy the covered entity's obligations.[562] For example, for a business associate to provide access directly to an individual, the covered entity must include in its business associate agreement that the business associate can do so. The sample provisions for a business associate agreement on the Department's website long have included a sample element that specifically addresses the issue clarified by this modification.[563]

A person who meets the definition of a business associate [564] must comply with the provisions of the HIPAA Rules that are applicable to business associates, regardless of whether they have executed the required business associate agreement with the entity using its services.[565] The existence or absence of a business associate agreement between a covered entity and a person does not determine whether the person is a business associate of that covered entity. If a business associate agreement has not been executed, a business associate still would be responsible for disclosing PHI to the covered entity, which would provide the PHI to the individual. In all cases, the covered entity remains ultimately responsible for ensuring that the requested PHI is provided to the individual or individual's designee to fulfill the right of access.[566]

The modification to 45 CFR 164.502(a)(4)(ii) does not allow regulated entities to use contractual arrangements to avoid other legal obligations to provide individuals with access to their health information, which may include PHI.[567] If there are other applicable laws that require a disclosure of PHI by a business associate, the business associate would need to comply with that law and ensure that any agreements which they enter into are consistent with those legal obligations.[568]

Furthermore, records that meet the definition of designated record set and are held by a business associate for or

[558] For purposes of 45 CFR 164.502(a)(4)(ii), an ''individual'' also includes the individual's ''personal representative,'' with limited exceptions. *See* 45 CFR 164.502(g) and 164.524(a)(3)(iii).

[559] *See* 78 FR 5566, 5598–99 (Jan. 25, 2013).

[560] *See* ''Direct Liability of Business Associates,'' *supra* note 113.

[561] *Id.*

[562] *See* ''Does the HIPAA Privacy Rule require a business associate to provide individuals with access to their protected health information or an accounting of disclosures, or an opportunity to amend protected health information?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #246 (Dec. 19, 2002), *https://www.hhs.gov/hipaa/for-professionals/faq/246/do-business-associates-have-obligations/index.html; see also* ''Direct Liability of Business Associates,'' *supra* note 113.

[563] ''Business Associate Contracts,'' Office for Civil Rights, U.S. Department of Health and Human Services (Jan. 25, 2013), *https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.*

[564] 45 CFR 160.103 (definition of ''Business associate'').

[565] *See* 78 FR 5566, 5598–99 (Jan. 25, 2013).

[566] *Id.* at 5600.

[567] *See* 85 FR 25642, 25811 (May 1, 2020) (explaining that while the information blocking regulations do not require actors that are also covered entities or business associates to violate their business associate agreements or associated service level agreements, they also do not permit such agreements to be used in a discriminatory manner by an actor to forbid or limit disclosures that otherwise would be permitted by the Privacy Rule).

[568] *See* ''Does the HIPAA Privacy Rule preempt state laws?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #399 (Mar. 12, 2003), *https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html.*

on behalf of a covered entity are part of the covered entity's designated record set.[569] Accordingly, a covered entity may not avoid its access obligations on the basis that its business associate maintains the requested PHI.

e. Responses to Public Comments

Comment: Several commenters expressed support for the proposed modification. According to a few commenters, it would clarify the role of a business associate with respect to requests for access. A few commenters asserted that the proposed modification would clarify the relationship between covered entities and business associates with minimal burden.

One commenter asserted that changing the process for requesting access to PHI to permit individuals to make such requests of business associates directly would be burdensome for individuals and covered entities.

A few commenters expressed opposition to the proposal because they believed that it would be inconsistent with section 4006 of the Cures Act, which requires the Secretary to consult with ONC and promote policies that ensure the accessibility of ''electronic health information,'' and with the information blocking regulations. One commenter recommended that we ensure that the Department's approach to individual access and business associate responsibilities for providing individual access is consistent across components of the Department. One commenter expressed concern that some business associate agreements prohibit business associates from disclosing PHI in response to individual requests for access to anyone other than the person that is the source of the data (*e.g.,* generally, the covered entity that engaged the business associate); this commenter recommended that the Department educate health care providers on how to leverage HIEs for individual access requests.

Response: As discussed above, we are finalizing the modification as proposed and consistent with our longstanding interpretation of this provision. This clarification does not create a new requirement under the Privacy Rule for business associates to respond directly to requests from individuals. Rather, it clarifies the two ways for a business associate to fulfill the regulatory requirement to disclose PHI as necessary for a covered entity to satisfy its obligations under the right of access: (1) provide the PHI to the covered entity; or (2) where the business associate agreement specifies, provide the PHI directly to the individual or the individual's designee.

Section 4006(b) of the Cures Act amended the HITECH Act to clarify that a business associate is permitted to provide an individual with access or a copy of PHI about the individual if the individual requests such access or copy from the business associate (or in the case where an individual exercises their right of access to direct, to grant or transmit such access or copy to a person designated by the individual).[570] Thus, the HITECH Act did not expressly require the business associate to make such disclosure, so there is no conflict with the revision that we are making in this final rule.

The Privacy Rule permits a business associate to use or disclose PHI only as permitted or required by its business associate agreement pursuant to 45 CFR 164.504(e)[571] or as required by law.[572] Accordingly, under the Privacy Rule, a business associate can make disclosures directly to individuals or their designees to fulfill a right of access request only if the business associate agreement permits or requires it. The Privacy Rule does not require that a business associate agreement permit or require a business associate to respond directly to requests for access, and the obligation for ensuring that responses are provided to such requests remains with the covered entity, regardless of any delegation made as part of the business associate agreement. However, not permitting a business associate to respond directly to requests for access may be a violation of another law. For example, a practice of a business associate that is also an actor[573] may implicate the information blocking regulations where the practice involves not responding to or fulfilling requests for access, exchange, or use of EHI,[574] if such access, exchange, or use of EHI is restricted by contracts or agreements and such restrictions are considered an interference.[575]

The information blocking regulations were designed to operate in a manner that is consistent with the Privacy Rule and other laws providing privacy rights for patients. Foremost, the definition of information blocking excludes practices that are ''required by law,'' including under the Privacy Rule (or other Federal or state law). However, if an actor is permitted to provide access, exchange, or use of EHI under the Privacy Rule (and other applicable laws), then the information blocking regulations may be implicated with respect to the actor's practice that is likely to interfere with access, exchange, or use of EHI unless an exception applies to the practice.[576]

B. Reducing Identity Verification Burden for Individuals Exercising the Right of Access

1. Issues To Address

Section 164.514(h) of the Privacy Rule requires, with limited exceptions, that a covered entity take reasonable steps to verify the identity of a person requesting PHI before disclosing the PHI to ensure that unauthorized persons do not obtain an individual's PHI.[577]

The Privacy Rule does not mandate any particular method of verification (*e.g.,* viewing an individual's driver's license at the point of service). Instead, it generally leaves the type and manner of the verification to the discretion and professional judgment of the covered entity, provided that the verification processes and measures do not create barriers to, or unreasonably delay, the individual from obtaining access to their PHI. Verification may be done verbally or in writing. In many circumstances, the type of verification may depend on how the individual is requesting and/or receiving access, such as in person, by phone (if permitted by the covered entity), by faxing or emailing the request

[569] *See* 65 FR 82462, 82489 (Dec. 28, 2000); 45 CFR 164.501 (definition of ''Designated record set'').

[570] 42 U.S.C. 17935(e)(2) (as amended by sec. 4006(b) of Pub. L. 114–255, 130 Stat. 1183 (Dec. 13, 2016)).

[571] 45 CFR 164.504(e) contains the standard and implementation specifications for business associate contracts, commonly referred to as business associate agreements.

[572] 45 CFR 164.502(a)(3); *see* 45 CFR 164.103 (definition of ''Required by law''). For example, the Privacy Rule does not relieve a business associate of its obligations to disclose PHI to a plan sponsor to the extent that such disclosure is required by section 408 of the Employee Retirement Income Security Act of 1974 (ERISA), where applicable.

[573] 45 CFR 171.102 (definition of ''Actor'').

[574] 45 CFR 171.102 (definition of ''Electronic health information'').

[575] 85 FR 25642, 25811–12 (May 1, 2020). Similarly, a practice of a covered entity that is also an actor may implicate the information blocking regulations where the practice results in the inability of a business associate to respond to or fulfill requests for access, exchange, or use of EHI, if such access, exchange, or use of EHI is the result of restrictions in contracts or agreements and such restrictions are considered an interference. As explained by ONC, the actions and processes (*e.g.,* negotiations) of the actors in reaching the business associate agreement and associated service level agreements would need to be reviewed to determine whether there was any action taken by an actor that is party to the agreement that was likely to interfere with the access, exchange, or use of EHI and whether the requisite intent requirement was met. *Id.*

[576] *Id.* at 25812.

[577] Disclosures made pursuant to 45 CFR 164.510 are excepted from this requirement. 45 CFR 164.514(h)(1)(i).

on the covered entity's supplied form, by secure online portal, or by other means. For example, if the covered entity requires that access requests be made on its own supplied form, the form could ask for basic information about the individual that would enable the covered entity to verify that the person requesting access is the subject of the information requested or is the individual's personal representative, provided that use of the form does not create a barrier to or unreasonably delay the individual from obtaining access to the individual's PHI. For covered entities providing individuals with access to their PHI through patient or health plan member portals, such portals already should be set up with appropriate authentication controls, as required by 45 CFR 164.312(d), to ensure that the person seeking access is the individual who is the subject of the PHI (or their personal representative).[578]

However, the Department continues to receive complaints and anecdotal accounts indicating that some covered entities are imposing burdensome requirements for identity verification on individuals seeking to obtain their PHI pursuant to the individual right of access. For example, some covered entities require individuals to receive their PHI in person, or even to obtain (at potentially added expense) a notarization on a written request, to exercise their right of access.

2. Proposed Rule

To address these barriers to an individual's access to their health information, the Department proposed to modify 45 CFR 164.514(h) by adding paragraph (2)(v) to expressly prohibit a covered entity from imposing unreasonable identity verification measures on an individual (or their personal representative) exercising a right under the Privacy Rule.[579]

In addition, the Department proposed to clarify that unreasonable verification measures are measures that cause an individual to expend unnecessary effort or expense when a less burdensome verification measure is practicable for the particular covered entity. The Department proposed to include in regulatory text examples of what is considered an unreasonable verification measure, including but not limited to: requiring individuals to obtain notarization of requests to exercise their Privacy Rule rights or requiring individuals to provide proof of identity in person when a more convenient method for remote verification is practicable for the covered entity.[580]

The Department explained that it would consider the entity's fulfillment of its Security Rule obligations in assessing whether a verification measure is practicable. As part of the assessment, we would consider the covered entity's size, complexity, and capabilities; technical infrastructure, hardware, and software security capabilities; the costs of security measures related to verification and of implementing measures that may be more convenient for individuals; and the probability and criticality of potential risks to ePHI in the covered entity's electronic information systems.[581]

As discussed above, we also proposed to clarify that a covered entity that implements a requirement for individuals to submit a request for access, including a request to direct an electronic copy of PHI in an electronic health record to a person designated by the individual, in writing, pursuant to 45 CFR 164.524(b)(1), would not be permitted to do so in a way that imposes unreasonable burdens on individuals. The Department proposed the change to ensure that individuals do not have to expend unnecessary effort or expense when other verification measures are practicable for the covered entity.

Consistent with the proposed verification provisions above, the Department also proposed to expressly prohibit a covered entity from imposing unreasonable measures for submitting a request for access, including the right of access to direct, in writing; the proposal provided that measures would be unreasonable if they impede the individual from obtaining access when a measure that is less burdensome for individuals is practicable for the particular covered entity. To help define ''unreasonable measures'' for covered entities, the Department proposed to include and compare, in regulatory text, non-exhaustive specific examples of reasonable and unreasonable measures that some covered entities have imposed (as described in public comments or individuals' complaints submitted to the Department) or may be likely to impose.

3. Overview of Comments

Most commenters expressed support for the proposed prohibition against imposing unreasonable identity verification measures. Some commenters asserted that the proposal would facilitate individuals' access to their PHI and provide covered entities with sufficient flexibility to determine appropriate identity verification measures. Several commenters cautioned the Department against enumerating specific methods or examples of appropriate measures for identity verification, while others urged the Department to preserve flexibility for covered entities to select verification measures appropriate to their operational environments. A few commenters expressed concern that limiting the available measures for identity verification could increase the risk to the privacy and security of PHI. Several comments requested clarification regarding identity verification for personal representatives.

Most commenters expressed support for the proposal to prohibit covered entities from imposing unreasonable measures on individuals making access requests, stating that it would strengthen the individual right of access. Many commenters reported that some covered entities refuse to receive requests submitted by email or only receive requests made through online portals even in circumstances when an individual could not reasonably use those systems. A few commenters expressed concern that allowing greater flexibility in request submission could increase administrative burden and requested that the Department clarify whether covered entities may continue to require requests in writing.

4. Final Rule

The Department is finalizing a modified version of the proposal to prohibit a covered entity from imposing unreasonable identity verification measures or imposing unreasonable measures that impede the submission of requests for access, including the right of access to direct. Specifically, the final rule adds paragraph (2)(v) of 45 CFR 164.514(h) to prohibit covered entities from imposing unreasonable verification measures that would impede an individual from exercising a right under the Privacy Rule. An unreasonable measure is one that causes an individual to expend unnecessary effort or resources when a less burdensome verification measure is practicable for the covered entity.

The Department is not finalizing in regulatory text examples of unreasonable measures. Instead, consistent with comments urging flexibility and to avoid establishing prescriptive limitations on reasonableness that may become outdated as technology evolves, the Department provides in this preamble a

[578] *See* 45 CFR 164.312(d).

[579] *See* 86 FR 6446, 6470–71 (Jan. 21, 2021).

[580] *See* 86 FR 6446, 6534 (Jan. 21, 2021).

[581] *See* 45 CFR 164.306(b)(2); 86 FR 6446, 6470 (Jan. 21, 2021).

non-exhaustive list of examples of measures that we currently consider unreasonable to illustrate how the standard applies.

As we discussed in the proposed rule, unreasonable identity verification measures include, but are not limited to, requiring an individual to do any of the following: (1) provide proof of identity in person when a method for remote verification is practicable for the covered entity and more convenient for the individual; (2) provide a ''wet'' signature when a signature is required and an electronic signature is valid under applicable law;[582] or (3) obtain notarization of the individual's signature on a written request to exercise their right of access, including the right of access to direct. Notarization requirements also may be unreasonable if imposed on a personal representative requesting access on an individual's behalf, in circumstances when the covered entity has sufficient documentation to verify the identity and authority of the personal representative or when a less burdensome verification measure is practicable.

As another example, we also would consider it to be unreasonable for a covered entity to refuse to accept a request for access from a personal health app where: (1) the request is made, using TEFCA, to a covered entity that participates in TEFCA; and (2) the covered entity has performed both of the following actions:

- Verifies, using technology that performs signature validation, that the cryptographically signed token[583] attached to the request was issued by a credential service provider[584] (CSP) that is certified to perform digital identity verification consistent with IAL2 and AAL2 as set forth in the most recent version of NIST Special Publication (SP) 800–63[585] (''SP 800–63'').
- Ensures that the demographic information verified by the CSP and included in the cryptographically signed token is consistent with the demographic information for the individual in the designated record set maintained by or for the covered entity.

Accordingly, a covered entity can meet its obligations under 45 CFR 164.514(h)(1) where the person requesting the disclosure of PHI is an individual seeking to exercise their right of access in the circumstances described above.

The same is true where the request is sent through CMS Aligned Networks to a covered entity that is a participant in the networks from a patient facing app that: (1) is a personal health app and (2) connects to the networks as a participant in the Medicare App Library.

The Department also is finalizing a modified version of the proposal to prohibit a covered entity from imposing measures that impede access requests.[586] The final rule clarifies that a covered entity may not impose measures that impede the individual from obtaining access when a measure that is less burdensome for the individual is practicable for the entity. The final rule also reiterates that a covered entity may require an individual to submit a request for access in writing, provided that it informs the individual of such a requirement, and clarifies that a request submitted electronically or on paper may satisfy such a requirement because the request itself serves as documentation of the individual's exercise of the right of access.[587]

Although the Department is not finalizing in regulatory text a list of examples of measures that impede access, we reaffirm the examples provided in the 2021 Privacy Rule NPRM and provide additional examples to assist regulated entities in understanding what we consider to be measures that impede an individual's access to their PHI. For example, requiring individuals to complete a form with only the limited information needed for the entity to provide access would be considered reasonable because it requests only the information necessary for verification and does not require the individual to expend unnecessary effort. In contrast, requiring individuals to fill out a form with the extensive information contained in a HIPAA authorization form may impose an unreasonable burden on individuals.

In addition, while we encourage covered entities to provide individuals with the option to submit access requests through patient and health plan member portals and other electronic methods (*e.g.,* email, personal health apps, through an HIN), it generally would be unreasonable for a covered entity to require that requests for access be made only through a particular electronic method when it would be practicable for the covered entity also to accept such requests in-person or through other electronic methods.[588] Unreasonable measures also include applying onerous or infeasible registration requirements for personal health apps (or other apps that are not being provided on behalf of or at the direction of the covered entity) that would create a barrier to or unreasonably delay registration beyond what is necessary for compliance with the Security Rule, such as requiring a person who does not meet the definition of a business associate to enter into a business associate agreement with the covered entity. Another example of an unreasonable measure would be preventing an individual's personal health app from registering with an endpoint (*e.g.,* API) that the covered entity makes public where the registration of such endpoint would not pose an unacceptable level of risk to the ePHI in the covered entity's (or its business associate's) electronic information systems, as informed by the covered entity's risk analysis.[589]

As explained in the 2021 Privacy Rule NPRM, under the Privacy Rule's requirements for individual access,

[582] *See* 78 FR 5566, 5633 (Jan. 25, 2013); ''How do HIPAA authorizations apply to an electronic health information exchange environment?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #554 (Dec. 15, 2008), *https://www.hhs.gov/hipaa/for-professionals/faq/554/how-do-hipaa-authorizations-apply-to-electronic-health-information/index.html;* ''How may the HIPAA Privacy Rule's requirements for verification of identity and authority be met in an electronic health information exchange environment?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #569 (Dec. 15, 2008), *https://www.hhs.gov/hipaa/for-professionals/faq/569/how-may-hipaas-requirements-for-verification-of-identity-be-met-electronically/index.html.*

[583] *See* NIST definition of ''token,'' Glossary, Computer Security Resource Center, National Institute for Standards and Technology, U.S. Department of Commerce, *https://csrc.nist.gov/glossary/term/token.*

[584] Generally, a credential service provider is an entity that performs digital identity verification. *See* NIST definition of ''credential service provider,'' Glossary, Computer Security Resource Center, National Institute for Standards and Technology, U.S. Department of Commerce, *https://csrc.nist.gov/glossary/term/credential_service_provider/.*

[585] The current and most recent version is SP 800–63–4. *See* ''Digital Identity Guidelines,'' National Institute of Standards and Technology, U.S. Department of Commerce (Aug. 26, 2025), *https://pages.nist.gov/800-63-4/.* For information on CSP certification, *see* ''International Identity Assurance Program,'' Kantara Initiative, *https://kantarainitiative.org/us-identity-certification-program/.* As of this publication, no CSPs are certified as meeting the requirements of SP 800–63–4. Accordingly, covered entities may rely on a cryptographically signed token CSP that is certified to perform digital identity verification consistent with IAL2 and AAL2 as set forth in NIST SP 800–63–3 until such time as there are CSPs certified to NIST SP 800–63–4.

[586] *See* new 45 CFR 164.524(b)(1)(iii).

[587] *See* new 45 CFR 164.524(b)(1)(ii).

[588] *See* new 45 CFR 164.514(h)(2)(v).

[589] *See* 45 CFR 164.308(a)(1). As discussed above, we believe that, generally, when a covered entity is in control of its electronic information systems' ability to transmit PHI or to provide read access to PHI through a personal health app, the risk to the security of ePHI in their electronic information systems is low. At the same time, a covered entity remains responsible for maintaining awareness of and protecting ePHI in the face of new security vulnerabilities and threats to the confidentiality, integrity, and availability of its ePHI.

covered entities generally must allow every application that wants to register with the API to provide access for an individual the ability to do so, assuming that it is practicable for the covered entities and absent any Security Rule concerns.[590] Therefore, a regulated entity that makes available a secure, standards-based API but denies registration, and therefore individual access, to an individual's personal health app, may be in violation of the Privacy Rule's requirements for the provision of individual access. For example, a health care provider may not prevent an app from registering solely because the app does not have a business associate relationship and agreement with the covered entity or because the app offers another service to individuals that competes with a service that the health care provider (or one of its business associates) offers.

As another example, it would be unreasonable for a covered entity that participates in TEFCA to refuse to accept an individual's request for access made through a personal health app that is a TEFCA IAS Provider, even though the request is not made on the covered entity's specific form, where both of the following conditions are met:

- The request meets the requirements at 45 CFR 164.524.
- The covered entity is able to verify the individual's identity consistent with its obligations at 45 CFR 164.514(h)(i), including by verifying the signature on and the demographic information in a cryptographically signed token as described above.

The same is true where the scenario relies upon CMS Aligned Networks and the covered entity and personal health app have the requisite relationship.

The final rule does not require covered entities to adopt particular methods of verification, nor does it require covered entities to implement the measure for verification that is least burdensome for an individual in every circumstance, if it is impracticable for the covered entities to do so. Covered entities retain discretion to select verification measures that are appropriate to their operational environment, provided that the measure does not impose unreasonable burdens on an individual's exercise of the right of access. Covered entities are encouraged to offer individuals multiple options for verifying their identity when the individual requests access.

[590] The Cures Act Final Rule provides exceptions to information blocking that are aligned with the HIPAA Rules to prevent harm, for privacy and security. This discussion is consistent with those provisions. *See* 85 FR 25642 (May 1, 2020).

5. Responses to Public Comments

Comment: Some commenters expressed support for the proposal to prohibit covered entities from imposing unreasonable measures for identity verification. Several commenters expressed support for the proposal because it would clarify the requirements while retaining flexibility for covered entities to determine the particular method of verification. Some commenters recommended that the Department require implementation of specific methods of identity verification and authentication. A few commenters expressed support for the proposal and urged the Department to require that identity verification be streamlined through patient portals and that requests for information be limited to the information needed to securely verify identity.

A few commenters expressed support for the proposal because they believed that it would facilitate individuals' access to their PHI by addressing obstacles that disproportionately burden members of minority groups and historically disadvantaged communities, including individuals with limited financial means or disabilities and caregivers for such individuals.

Response: The final rule adopts the proposal to prohibit a covered entity from imposing unreasonable identity verification measures. The Department declines to require specific methods for identity verification and authentication. Because of the varied circumstances of individuals and covered entities, a given measure for verifying an individual's identity or requesting access, such as using an online portal, may be convenient for some individuals and burdensome for others, and practicable for some covered entities but not for others. Given this variability, the Department declines to require that covered entities implement any particular measure or analyze and adopt the least burdensome measure possible for each individual.

Comment: Many commenters provided examples of what they considered to be reasonable or unreasonable measures and requested that the Department provide additional examples of reasonable or unreasonable measures. A few commenters recommended that the Department adopt a framework for evaluating the reasonableness of identity verification measures, while one commenter requested that the Department clarify that ''reasonableness'' would be determined based on a covered entity's business and operational environment. A few commenters recommended that the Department ensure that covered entities are able to match a patient's identity with their information.

Response: As discussed above, the Department is not including examples in regulatory text to avoid creating an impression of a complete list of reasonable or unreasonable measures of identity verification. Rather, we provide a non-exhaustive list of examples in preamble above. The standard for identity verification generally requires a covered entity (or a business associate on behalf of the covered entity) to verify the identity of a person requesting PHI and the authority of any such person to have access to PHI under the Privacy Rule, if the identity or authority of such person is not known to the covered entity. As we explained in the 2021 Privacy Rule NPRM, practicability considerations encompass those related to an entity's fulfillment of its Security Rule obligations, discussed above.[591]

Comment: One commenter stated that the identity verification standard should be the same whether access to PHI is requested by an individual or a personal representative, while another commenter recommended that the Department permit covered entities to employ different standards for identity verification for individuals and personal representatives.

Response: The Privacy Rule generally requires a covered entity to treat a person who has the authority under applicable law to act on behalf of an individual in making decisions related to health care as the individual's personal representative with respect to PHI relevant to such personal representation, with limited exception.[592] The final rule does not prescribe separate standards for identity verification for individuals and personal representatives, nor does it alter the existing requirement under 45 CFR 164.514(h) that a covered entity must verify the identity of a person requesting PHI and the authority of any such person to have access to PHI, if their identity (and authority) is not already known to the covered entity. The Department acknowledges that verification considerations may differ when a personal representative requests access to PHI on behalf of an individual. For example, a health care provider can require a copy of a power of attorney if a person represents that they have a health care power of attorney, or can ask questions to determine that an adult acting for a minor child has the requisite relationship to the child, provided that

[591] *See* 45 CFR 164.306(b)(2); 86 FR 6446, 6470 (Jan. 21, 2021).

[592] *See* 45 CFR 164.502(g).

such measures do not impose an unreasonable burden on the exercise of the individual's rights under the Privacy Rule.[593] However, it would be unreasonable for a covered entity to adopt procedures for identity verification that would unnecessarily delay the covered entity's response to a request for access made by an individual's personal representative where alternative procedures would enable the verification of the personal representative's identity and authority in a more timely manner. Additionally, requiring personal representatives to repeatedly submit documentation already on file, mandating in-person appearances when remote verification is practicable, or refusing to accept legally valid documentation submitted electronically may, depending on the circumstances, constitute unreasonable measures that interfere with the individual's right of access as exercised through a personal representative.

Comment: Some commenters expressed opposition to this proposal because they viewed it as burdensome or unclear. Several commenters urged the Department not to impose restrictions on the ability of covered entities to determine the type and manner of identity verification. One commenter recommended that the Department prohibit covered entities from requiring extensive validation protocols.

Response: As discussed above, the Department is finalizing a modified version of the proposal that does not include examples in the regulatory text of what is considered unreasonable to avoid establishing prescriptive limitations on reasonableness or creating the impression that specific methods of identity verification are required. By removing examples from the regulatory text and instead addressing them in this preamble, the final rule provides covered entities with the flexibility to adopt verification methods that evolve with technological and operational changes, while still making clear that they cannot employ identity verification measures that are unreasonable.

Comment: Some commenters expressed opposition to the proposal because they believed that it would lead to breaches of PHI. For example, commenters posed examples of malicious actors creating technology that is able to impersonate individuals or covered entities being unable to verify the identity of a minor's guardian. One commenter expressed concern that relaxing identity verification measures could lead to increased identity theft, fraud, or misidentification, while another commenter recommended that the Department clarify that a covered entity is permitted to reject a request if it is unable to verify a person's identity.

Response: The final rule does not require covered entities to relax identity verification requirements. Nothing in this final rule changes a covered entity's obligation under 45 CFR 164.514(h) to take reasonable steps to verify the identity and authority of a person requesting PHI before disclosing the PHI to help ensure that unauthorized persons do not obtain an individual's PHI.[594] Rather, the final rule prohibits covered entities from imposing measures that impede access requests or imposing unreasonable identity verification measures. Covered entities remain responsible for assessing security risks and are not required to adopt verification methods that would increase the likelihood of identity theft, fraud, or misidentification, nor are they required to fulfill an access request when they cannot verify the identity of the person making the request.

C. Amending the Definition of Health Care Operations To Clarify the Scope of Care Coordination and Case Management

1. Current Rule

The Privacy Rule expressly permits covered entities to use and disclose PHI, without an individual's valid authorization, for treatment and certain health care operations, among other important purposes.[595] The definitions of both ''treatment'' and ''health care operations'' include some care coordination and case management activities.[596]

As explained in preamble to the 2000 Privacy Rule, certain activities may be considered either health care operations or treatment, depending on whether the activities are population-wide or individual-specific activities, and if individual-specific, whether the communication with an individual occurs on behalf of a health care provider or a health plan.[597] For example, a telephone call by a nurse in a doctor's office to an individual to discuss follow-up care would be a treatment activity; however, the same activity performed by a nurse working for a health plan would be a health care operation.[598]

2. Proposed Rule

Despite the guidance in the 2000 Privacy Rule, we have received anecdotal reports that some covered entities have interpreted the definition of ''health care operations'' to include only population-based care coordination and case management, which would have the effect of excluding individual-level care coordination and case management by health plans.[599] In addition, some covered entities have expressed uncertainty about the ability of health care providers to disclose PHI to health plans for individual-level care coordination and case management without an individual's authorization.

Thus, the Department proposed to amend the definition of ''health care operations'' at 45 CFR 164.501 to clarify that it encompasses all care coordination and case management by health plans, whether individual-level or population-based. The Department explained that, as drafted, the placement of commas separating the list of activities following the term ''population-based activities'' permitted the interpretation that the term ''population-based activities'' modifies (*i.e.,* places a condition on) all of the activities listed between the semi-colons, including case management and care coordination, although the Department has not applied that interpretation to the definition of health care operations. Accordingly, the Department proposed to change the commas into semi-colons in paragraph (1) of the definition of ''health care operations'' at 45 CFR 164.501 to clearly convey that the activities listed are each separate types of health care operations.

3. Overview of Comments

Many individuals and organizations commented on the proposal to clarify the definition of ''heath care operations.'' Most commenters expressed general support for the proposal because they believed that the changes would clarify the scope of health care operations. They also believed that the proposed modifications would facilitate the sharing of PHI to support care coordination and case management.

Some commenters expressed opposition to the proposal because they believed that it would permit the use and disclosure of PHI for individual-

[593] *See* 65 FR 82462, 82547 (Dec. 28, 2000).

[594] *See* 45 CFR 164.514(h).

[595] *See* 45 CFR 164.506; 45 CFR 160.103 (definitions of ''Disclosure'' and ''Use'').

[596] *See* 45 CFR 164.501 (definitions of ''Treatment'' and ''Health care operations'').

[597] 65 FR 82462, 82627 (Dec. 28, 2000).

[598] *Id.*

[599] This final rule describes such activities as ''population-based'' and ''individual-level'' care coordination and case management, respectively.

level care coordination and case management without requiring an individual's authorization, thereby excluding individuals from the process of care coordination.

4. Final Rule

This final rule adopts the proposed clarification of the definition of ''health care operations'' to facilitate the intended range of care coordination and case management activities. The Department generally has interpreted the existing definition to permit health care providers to disclose PHI to health plans for individual-level care coordination and case management without an individual's authorization. However, covered entities have expressed uncertainty about the extent to which the definition applies to activities such as case management and care coordination by health plans or as part of value-based health care models. Therefore, it is necessary for the Department to expressly confirm that health care operations encompasses all care coordination and case management activities by health plans and covered health care providers, whether individual-level or population-based. Changing the punctuation in the definition accomplishes this goal, thereby improving the likelihood that covered entities will use and disclose PHI accordingly.

5. Responses to Public Comments

Comment: Many commenters expressed support for this proposal because it would facilitate both individual-level and population-based care coordination and case management. Several commenters asserted that the proposal would provide certainty to covered entities that are hesitant to disclose PHI for care coordination and case management without an individual's authorization. One commenter stated that clarifying the definition would decrease the burden for workforce members who previously requested individual authorizations for these disclosures. Another commenter suggested that the Department issue guidance to address this concern, rather than notice and comment rulemaking.

Several commenters expressed support for the Department's goal but recommended further revisions. For example, one commenter recommended that the Department add the phrase ''individual-level or population-based'' in front of the words ''case management and care coordination'' to provide additional clarity.

Response: The Department believes that the clarification that we are finalizing here addresses any uncertainty regarding whether PHI may be used or disclosed for individual-level care coordination and case management without an individual's authorization and reduces the burden of obtaining an individual's authorization when not required. This revision to the definition sufficiently clarifies the intended range of care coordination and case management, so it is not necessary to modify it further.

Comment: A few commenters who expressed support for the clarification to the definition of health care operations recommended that the Department define or provide greater clarity regarding the activities included in ''care coordination'' and ''case management'' to allow for more consistent interpretation of the terms. Some commenters requested that the Department explicitly include coordination of social services such as supportive housing for an individual with a disability, in the definition of health care operations.

Response: We decline to define ''care coordination'' and ''case management'' in this final rule. Both terms refer broadly to a set of activities aimed at promoting cooperation among people involved in caring for individuals, including family members, caregivers, and community-based organizations. Rather than proposing limiting definitions, the Department has, instead, provided an extensive discussion and a non-exhaustive list of examples of the types of activities it considers to be care coordination and case management activities.[600]

The Department also declines to include coordination of social services in the definition of ''health care operations'' in this final rule. Instead, to address questions about whether the Privacy Rule permits disclosures to social services organizations for care coordination and case management, the Department is adding a provision at 45 CFR 164.506(c)(6) to expressly permit disclosures of PHI for individual-level care coordination and case management that constitute treatment or health care operations, to certain types of organizations that provide health and human services.[601]

Comment: Some commenters expressed concern that the proposal would increase the ability of covered entities to use and disclose PHI for care coordination and case management without individual authorization. A few commenters expressed opposition to the Department's proposed clarification because they believed that it would exclude individuals from the process of care coordination. One commenter asserted that the proposal would expand access to individual-level PHI without accompanying safeguards and controls to protect an individual's privacy.

Response: This clarification does not expand the authority of covered entities to use or disclose PHI without a valid authorization. As we explained in the 2021 Privacy Rule NPRM, the Department has become aware that some covered entities may be interpreting the definition of health care operations in a manner that is inconsistent with the Department's intent. Thus, the Department does not consider this clarification to be a substantive modification because the final rule does not alter our interpretation of the definition. Rather, the modification to the definition merely clarifies the ability of covered entities to use and disclose PHI for individual-level care coordination and case management. For example, health plans may use and disclose PHI for individual-level care coordination and case management, and covered entities may disclose PHI to health plans for these purposes.

The Department appreciates commenters' concerns about protecting individuals' privacy and emphasizes that covered entities must apply the requirements of the minimum necessary standard for uses and disclosures of PHI for the purpose of health care operations. Additionally, individuals have a right to request restrictions on uses or disclosures for TPO under 45 CFR 164.522(a).[602]

---

[600] *See supra* at sec. III.A.3.

[601] The permission would be consistent with existing OCR guidance addressing these types of disclosures by covered health care providers. *See* ''Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes? For example, can a health care provider refer a homeless patient to a social services agency, such as a housing provider, when doing so may reveal that the basis for eligibility is related to mental health?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #3008 (Jan. 4, 2018), *https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html.*

[602] *See* 45 CFR 164.522(a)(1)(ii). Although covered entities must allow individuals to request restrictions of the use or disclosure of their PHI for TPO, covered entities generally are not required to agree with the requested restrictions, with limited exception. Specifically, covered entities are required to accept an individual's request to restrict the disclosure of PHI about the individual to a health plan if: (1) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise requirement by law; and (2) the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has

Comment: A few commenters expressed concern that the proposal could have unintended adverse consequences if implemented in conjunction with the proposal to modify the minimum necessary standard. For example, one commenter asserted that removing the minimum necessary standard for health care operations for care coordination and case management could allow health plans to gain unfettered access to a physician's EHR and empower health plans to make decisions about an individual's health care.

Response: The Department is not finalizing the proposed exception to the minimum necessary standard for health care operations uses and disclosures of PHI related to individual-level care coordination and case management, as discussed below. Retaining the current minimum necessary standard addresses concerns that the modification to the definition of health care operations weakens individuals' privacy protections. Therefore, covered entities who engage in care coordination and case management as health care operations must limit the PHI that they use or disclose to the minimum necessary to accomplish the intended purpose of the use or disclosure.

D. Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-Level Care Coordination and Case Management

1. Current Rule

Section 164.502(b) requires covered entities to use, disclose, and request only the minimum amount of PHI necessary for the purposes of TPO, except for disclosures to or requests by a health care provider for treatment, where the minimum necessary requirement does not apply.

The Department has long considered care coordination to be part of an individual's treatment and interpreted the Privacy Rule to permit health care providers to disclose PHI in support of an individual's health care to service providers who may not be covered entities and who may not be health care providers.[603] Health plans also coordinate an individual's care when managing and paying for health plan benefits; however, these activities are considered health care operations activities (and therefore subject to the minimum necessary standard) because most health plans do not provide treatment.[604]

2. Proposed Rule

The Department proposed to create an exception to the minimum necessary standard for disclosures to, or requests by, a health plan or covered health care provider for care coordination and case management. The proposed exception would apply only to individual-level activities for care coordination and case management activities. In conjunction with the proposal to clarify that the definition of health care operations includes individual-level care coordination and case management described above, this proposed exception would permit health plans to request, use, and disclose PHI without limitation for such health care operations, including disclosures to persons who are not covered entities and who are not health care providers. For covered health care providers, the proposal would specify that the existing exception for disclosures to, or requests by, a health care provider for treatment includes case management and care coordination. The proposed exception would relieve covered entities from the requirement to make determinations about the minimum information necessary when the request is from, or the disclosure is made to, a covered health care provider or health plan to support individual-level care coordination and case management activities.

3. Overview of Comments

Commenters were evenly split in their views of the proposal. Commenters who expressed support for this proposal asserted that it would facilitate care coordination, improve outcomes, and provide clarification, while commenters who expressed opposition did so because they believed that it would decrease an individual's privacy.

4. Final Rule

This final rule does not adopt the proposed exception to the minimum necessary standard for individual-level care coordination and case management. The Department is persuaded by public comments that asserted that providing an exception to the minimum necessary standard for certain health care operations would erode individuals' confidence in the privacy of their PHI and their willingness to fully engage with the health care system. Additionally, we believe that other modifications that we are making in this final rule, such as modification to the definition of health care operations, will facilitate the ability of health plans to perform beneficial individual-level care coordination and case management activities.

5. Responses to Public Comments

Comment: Many commenters who expressed support for this proposal asserted that it would facilitate care coordination, improve outcomes, and clarify that disclosures of all PHI, rather than the minimum necessary, is permissible to health care providers and health plans for the purpose of individual-level care coordination and case management. Some commenters provided examples of the types of activities that they believed that this proposal would facilitate. According to one commenter, the proposal would eliminate concerns about determining the purpose of certain requests that could be for either treatment or health care operations. One commenter asserted that this proposal would not alter the practice of covered entities to request the minimum PHI necessary to accomplish their purpose. A few commenters expressed their belief that the proposal would reduce the administrative burden on covered entities. One commenter expressed support for the proposal because they believed that it would reduce impediments to the disclosure of PHI using HIEs. Another commenter asserted that the proposal would enable covered entities to transition from providing care on a fee-for-service basis to providing care based on value.

Response: The Department agrees with commenters that it is important for the Privacy Rule to permit the disclosure of PHI to facilitate care coordination and improve health care outcomes. However, we have determined that such aims can be achieved by means other than creating a new exception to the minimum necessary standard. Specifically, elsewhere in this rule, we are finalizing

paid the covered entity in full. *See* 45 CFR 164.522(a)(1)(vi).

[603] *See* ''Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes? For example, can a health care provider refer a homeless patient to a social services agency, such as a housing provider, when doing so may reveal that the basis for eligibility is related to mental health?,'' *supra* note 601.

[604] Managed care organizations generally integrate both the delivery and financing of health care, as opposed to most health plans, which solely pay for health care. Therefore, managed care organizations may operate as both health plans and health care providers. *See* Julie J. Welch, ''Managed Care: The Dominant Paradigm in US Healthcare,'' Journal of The American Health Information Management Association (Nov. 21, 2024), *https://journal.ahima.org/Portals/0/archives/AHIMA%20files/Managed%20Care_%20The%20Dominant%20Paradigm%20in%20US%20Healthcare.pdf;* Samuel R. Falkson, et al., ''Health Maintenance Organization,'' in StatPearls (StatPearls Publishing 2026) (updated Mar. 6, 2023), *https://www.ncbi.nlm.nih.gov/sites/books/NBK554454.*

our proposals to modify the definition of health care operations and to expressly permit the disclosure of PHI to social services agencies, community-based organizations, HCBS providers,[605] and other similar entities. We are not convinced that excepting, from the minimum necessary standard, disclosures for individual-level care coordination and case management when performed for the purpose of health care operations would provide sufficient benefits to outweigh the interests of individuals in limiting the PHI that is shared with health plans.

Comment: Many commenters expressed opposition to the proposal because of concerns that it would decrease an individual's privacy. Relatedly, several commenters asserted that the proposal would deter individuals from seeking treatment or erode individuals' trust in their health care providers. Several commenters expressed opposition to the proposal because they believed that increasing disclosures of PHI for care coordination or case management could harm individuals in a variety of ways, such as increased disclosures to entities that are not regulated under HIPAA, denials of public benefits, discrimination, and breaches. A few commenters asserted that PHI should not be disclosed for care coordination or case management without an individual's consent. According to a few commenters, obtaining an individual's authorization before disclosing PHI for care coordination or case management does not prevent or delay the provision of health care to an individual.

Several commenters expressed opposition to the proposal because it would permit health plans to have access to more PHI than they currently are able to obtain. Several commenters expressed opposition to the idea that health plans need access to more than the minimum necessary PHI for care coordination and case management. Several commenters asserted that the proposal would lead to an increase in coverage denials by health plans. One commenter expressed opposition to this proposal because they believed that it would lead to an increase in requests from health plans for the disclosure of PHI, leading to an increase in burden on health care providers.

Response: The Department agrees with the comments expressing concern that allowing health plans to have access to more than the minimum PHI necessary to accomplish their purpose likely would raise concerns for individuals, whether warranted or not, thereby eroding trust in the health care system. We also agree that, where the Privacy Rule permits disclosures of PHI beyond the minimum necessary for a particular purpose, there is the potential for an increase in the risk of unintended adverse consequences (*e.g.,* more PHI exposed in the event of a breach), regardless of who receives the PHI. At the same time, we recognize that health plans need a certain amount of PHI to perform routine functions, such as case management, care coordination, medical review, auditing, and provider credentialing. Therefore, in light of commenters' concerns, the Department believes that existing restrictions on the use and disclosure of PHI (*e.g.,* the prohibition on the use of genetic information for underwriting purposes, limitations on the use and disclosure of psychotherapy notes) strike an appropriate balance of protecting individuals' privacy interests while permitting uses and disclosures of PHI that are needed for health plans' legitimate purposes, including payment and health care operations. Accordingly, we are not finalizing our proposal to provide an exception to the minimum necessary standard for requests by or disclosures to health plans for individual-level activities for care coordination and case management.

Comment: A few commenters expressed concerns about the potential for health plans to use the proposed exception to gain access to large amounts of PHI to create de-identified data sets for sale and potential re-identification. According to these commenters, this would make PHI available for a variety of applications without authorization from individuals. These commenters urged the Department to implement protections to prevent the disclosure of such de-identified datasets and the re-identification of PHI before finalizing this proposal.

Response: As discussed above, the Department is not finalizing the proposed exception to the minimum necessary standard. With respect to concerns about re-identification of de-identified data, the de-identification standard requires that the information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.[606] In other words, PHI is not de-identified under the Privacy Rule if there is a reasonable basis to believe that it can be re-identified.

Comment: Several commenters expressed concerns about whether health care providers would be able to deny a request for PHI from health plans when the request meets the requirements of the permission for health care operations and the proposed exception to the minimum necessary standard, given the requirements of the information blocking regulations. One commenter recommended that the Department clarify how the information blocking regulations and the HIPAA Rules work in concert to ensure appropriate oversight and enforcement of the information blocking regulations.

Response: As discussed above, the Department is not finalizing the proposed modification to the minimum necessary standard because we do not believe that it is a necessary or effective mechanism to facilitate the ability of covered entities to support individual-level care coordination and case management. The information blocking regulations exclude from the definition of information blocking reasonable and necessary practices that advance the privacy interests of individuals.[607] For example, the information blocking regulations accommodate circumstances where the Privacy Rule requires that certain preconditions (*e.g.,* the minimum necessary standard) be met before permitting the use or disclosure of PHI.[608] For more information about the interaction of the information blocking regulations with the HIPAA Rules and other laws protecting individuals' privacy interests, see the discussion of the Privacy Exception in the Cures Act Final Rule.[609]

E. Clarifying the Scope of Covered Entities' Abilities To Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management That Constitutes Treatment or Health Care Operations

1. Current Rule

Section 164.506 of the Privacy Rule sets forth the circumstances in which a covered entity is permitted to use and disclose PHI for TPO. Under 45 CFR 164.506(a), covered entities are permitted to use or disclose PHI without an individual's authorization for TPO,

[605] *See generally* 42 CFR part 441, subparts G, J, K, and M.

[606] *See* 45 CFR 164.514.

[607] *See* 85 FR 25642, 85 FR 25845–59 (May 1, 2020).

[608] *See* ''Would it be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to comply with federal privacy laws that require certain conditions to have been met prior to disclosure?,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, IB FAQ #48 (Apr. 2023), *https://healthit.gov/faq/would-it-be-information-blocking-if-actor-does-not-fulfill-request-access-exchange-or-use-ehi/.*

[609] 89 FR 1192, 1351–52 (Jan. 9, 2024).

subject to the applicable conditions and other requirements of the Privacy Rule. Section 164.506(b)(1) of the Privacy Rule permits, but does not require, covered entities to obtain an individual's consent to use or disclose PHI for TPO.[610]

The implementation specifications for using and disclosing PHI for TPO are in 45 CFR 164.506(c) of the Privacy Rule. Under 45 CFR 164.506(c)(1), a covered entity may use or disclose PHI for its own TPO. Sections 164.506(c)(2) and (c)(4) permit a covered entity to disclose PHI for the treatment activities of another health care provider and for specified health care operations of another covered entity, respectively, when the applicable conditions are met.

The Privacy Rule's definitions of both treatment and health care operations expressly include care coordination and case management activities.[611] Consistent with these definitions, the Department previously explained that a covered health care provider may disclose PHI for treatment purposes without an individual's authorization when coordinating or managing an individual's care with third parties that provide services related to the individual's health, including public- or private-sector entities that provide health-related social and community-based services.[612] For example, a covered health care provider is able to make a disclosure to a provider of HCBS[613] to treat an individual who is older or has a disability if it is for the coordination or management of that individual's treatment by the health care provider.[614] As another example, a health care provider may disclose to a senior center or adult day care provider the minimum PHI necessary to help coordinate health-related services for an individual, such as arranging for a home aide or helping the individual with their prescribed at-home or post-discharge treatment protocol. Likewise, the Privacy Rule also would permit the disclosure of PHI to facilitate care coordination and case management as part of a health plan's health care operations, such as when a health plan discloses to a senior wellness center the minimum PHI necessary where the individual is enrolled in the plan's wellness program. For example, if an individual plan member enrolls in a health plan's diabetes management program, the health plan may disclose only the minimum necessary amount of PHI to a senior center that is administering the wellness program for care coordination purposes, such as the member's demographic information and relevant diagnosis. The health plan would not be permitted to disclose PHI beyond the minimum necessary, such as unrelated diagnoses and other nongermane health information.

Section 164.502(b) contains the minimum necessary standard, which governs how much PHI a covered entity is permitted to disclose based on the purpose of the request, and the exceptions to that standard.[615] Disclosures to, or requests by, a health care provider for treatment purposes are excepted from the minimum necessary standard.[616] If a disclosure for treatment is made to an entity that is not a health care provider, this exception to the minimum necessary standard does not apply, and the covered entity must limit the disclosure to the minimum PHI necessary to accomplish the intended purpose of the use or disclosure. Disclosures for health care operations are likewise subject to the minimum necessary standard, unless an exception applies.

2. Proposed Rule

The Department long has interpreted the Privacy Rule as permitting a covered entity to use or disclose an individual's PHI without authorization for many care coordination and case management activities, even where such disclosure is to a third party that is not subject to the HIPAA Rules. However, as discussed in the 2021 Privacy Rule NPRM, we have become aware that some covered entities are uncertain about whether the Privacy Rule permits disclosures of PHI for these purposes to certain third parties without an individual's authorization and are requiring authorizations for such disclosures.

To address this uncertainty, the Department proposed to clarify that the Privacy Rule permits covered entities to disclose PHI to social services agencies, community-based organizations, HCBS providers, and similar third parties that provide health or human services to specific individuals for individual-level care coordination and case management, either as a treatment[617] activity of a covered health care provider or as a health care operations[618] activity of a covered health care provider or health plan. The Department proposed to make this clarification by adding paragraph 45 CFR 164.506(c)(6) that would identify such entities as permissible recipients of PHI for these purposes. The Department proposed to limit the scope of this permission to disclosures by covered entities for individual-level care coordination and case management that constitute treatment or health care operations, rather than including population-based activities, to ensure that the disclosures made under this permission would be akin to disclosures for treatment, which individuals expect to occur without the need to provide an authorization or consent.

3. Overview of Comments

Most commenters expressed support for the Department's proposal to expressly permit disclosures of PHI to third parties for individual-level care coordination and case management that constitute treatment or health care operations because they believed that it would enhance the ability of health care providers and health plans to provide case management and care coordination for individuals. Commenters who expressed opposition to the proposal recommended that disclosures for individual-level care coordination and case management require an

[610] *See* 67 FR 53182, 53209–11 (Aug. 14, 2002) (explaining the differences between a consent that a covered entity chooses to obtain to use or disclose PHI for TPO, as compared to an authorization that is described in 45 CFR 164.508); *see also* ''What is the difference between ''consent'' and ''authorization'' under the HIPAA Privacy Rule?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #264 (Mar. 23, 2007), *https://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html.*

[611] 45 CFR 164.501 (definitions of ''Health care operations'' and ''Treatment'').

[612] *See* ''Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes? For example, can a health care provider refer a homeless patient to a social services agency, such as a housing provider, when doing so may reveal that the basis for eligibility is related to mental health?,'' *supra* note 601. However, the disclosure of patient information for treatment and other purposes may be subject to other laws, including 42 CFR part 2 for certain SUD patient records.

[613] *See, e.g.,* 42 CFR 440.180. HCBS provides opportunities for Medicaid beneficiaries to receive services in their own homes or communities. Some HCBS providers may be health care providers within the definition at 45 CFR 160.103, some provide only human services (*e.g.,* non-medical transportation services), and some provide both types of services. *See* ''Home- and Community-Based Services,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (May 6, 2026), *https://www.cms.gov/training-education/partner-outreach-resources/american-indian-alaska-native/ltss-ta-center/information/ltss-models/home-and-community-based-services.*

[614] *See* 45 CFR 164.506(c).

[615] *See* 45 CFR 164.502(b). Certain provisions of 45 CFR 164.514(d) also address the minimum necessary requirement.

[616] 45 CFR 164.502(b)(2)(i).

[617] 45 CFR 164.501 (definition of ''Treatment'').

[618] 45 CFR 164.501 (definition of ''Health care operations''). As discussed in detail above, this final rule includes a modification to the punctuation in paragraph (1) of the definition of health care operations to clarify that care coordination and case management are not limited to ''population-based activities.''

individual's authorization. A few commenters asserted that this proposal would increase the administrative burden on covered entities because they believed that it would lead to an increase in requests, additional contracts, and difficulties complying with other Federal and state laws. Some commenters expressed concerns about the ability of such organizations to safeguard the privacy and security of the information disclosed to them by regulated entities pursuant to this proposal, as well as their ability to use and redisclose such information because they generally are not subject to the HIPAA Rules.

4. Final Rule

The Department is finalizing its proposal to adopt 45 CFR 164.506(c)(6) without modification. This section clarifies that the Privacy Rule permits covered entities to disclose PHI, without an individual's authorization, to social service agencies, community-based organizations, HCBS providers, and similar third parties for individual-level care coordination and case management activities that constitute treatment or health care operations. This clarification will facilitate the treatment and health care operations of the disclosing covered entities in circumstances where a disclosure will serve the health care or health-related needs of individuals.

The Privacy Rule has long permitted disclosures of PHI to such entities for treatment or, in certain circumstances, health care operations.[619] Rather than changing the Department's interpretation of these permitted disclosures, this final rule adds express language at 45 CFR 164.506(c)(6) to provide greater clarity about the scope of these existing permissions. The inclusion of this language in regulatory text ensures that covered entities understand their ability to disclose PHI to coordinate and manage care for individuals across clinical and community-based settings without an individual's authorization, where the Privacy Rule permits such disclosures. This clarification is consistent with the Department's longstanding approach of permitting uses and disclosures of PHI for TPO without authorization to avoid interfering with the ability of individuals to access quality and effective health care, while continuing to protect individuals' privacy.[620]

This express permission to disclose PHI to third parties for care coordination and case management that constitute treatment or health care operations eliminates confusion about a covered entity's ability to make such disclosures to improve individuals' health care. For example, a covered health care provider may disclose the minimum necessary PHI of an individual, who is transitioning from a long-term care facility into community living, to a social service agency that arranges housing, day programs, and other health-related services that the individual may need upon discharge. The covered provider also may disclose the minimum necessary PHI, for example, to a community-based organization that facilitates transportation, life skills training, and nutrition services that are needed to support the individual's health care. Likewise, a health plan may disclose the minimum necessary PHI to a transition coordinator[621] to verify an individual's eligibility for certain services and streamline care coordination.

The Department is limiting the scope of this permission to disclosures by covered entities for individual-level care coordination and case management that constitute treatment or health care operations, rather than population-based activities. The limitation to individual-level activities in 45 CFR 164.506(c)(6) does not affect a covered entity's ability to make disclosures for population-based activities where such disclosures are otherwise permitted by 45 CFR 164.506(c)(1) or another applicable provision of this Privacy Rule. This limitation is intended to ensure that the scope of the permission at 45 CFR 164.506(c)(6) remains consistent with the privacy expectations of individuals. Covered entities remain subject to all applicable conditions and requirements of the Privacy Rule, including the minimum necessary standard, as applicable.

Nothing in this final rule alters an individual's right under 45 CFR 164.522(a) to request restrictions on a use or disclosure of PHI for TPO. While a covered entity generally is not required to agree to such restrictions, it must act in accordance with any restriction to which it does agree. In addition, although covered entities are not required to obtain an individual's authorization or consent for disclosures permitted under 45 CFR 164.506(c)(6), disclosures for individual-level care coordination and case management activities that constitute treatment or health care operations should remain consistent with the covered entity's NPP.

5. Responses to Public Comments

Comment: Some commenters expressed support for this proposal because they believed that it would remove barriers to care coordination and improve the quality of care. These commenters also asserted that it would reduce the burden on individuals and health care providers because it would reduce reliance on written authorizations where the Privacy Rule already permits disclosures without authorization.

Response: The Department is adopting the proposal to add an implementation specification for TPO to provide greater clarity regarding covered entities' ability to disclose PHI without an individual's authorization to social services agencies, community-based organizations, HCBS providers, and other similar third parties for individual-level care coordination and case management that constitute treatment or health care operations. This clarification reduces unnecessary administrative burdens that can delay or impede coordination of care by decreasing the need for consultations with legal or compliance offices about whether authorizations are required for these disclosures. The Department also expects that this clarification will facilitate and encourage greater wraparound support and more targeted care for individuals who need health-related social or supportive services. For example, if a health care provider refers an individual with diabetes to a food bank, the health care provider could disclose the minimum necessary PHI about the individual to the food bank to enable the food bank to provide appropriate dietary accommodation or nutrition support.

Comment: While many commenters expressed support for limiting the proposal to individual-level care coordination and case management that constitute treatment or health care operations, several commenters recommended that the Department

[619] 65 FR 82497, 82628 (Dec. 28, 2000).

[620] *See* 67 FR 53182, 53215 (Aug. 14, 2002).

[621] *See* Deficit Reduction Act of 2005, sec. 6071 of Public Law 109–171, 120 Stat. 102 (Feb. 8, 2006) (enacting the Money Follows the Person (MFP) demonstration project to transition Medicaid beneficiaries from long-term institutional care to home-and community-based settings). Pursuant to MFP, states have developed transition programs, and hired transition coordinators, to assist individuals. *See* Debra Lipson, et al., ''Implications of State Program Features for Attaining MFP Transition Goals,'' Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services (prepared by Mathematica Policy Research, Inc.) (June 2009), *https://www.cms.gov/Regulations-and-Guidance/Legislation/DeficitReductionAct/downloads/mfptransitiongoalsjun26.pdf. See, e.g.,* ''Transition Process,'' Colorado Department of Health Care Policy & Financing (2026), *https://hcpf.colorado.gov/transition-process* (explaining that, for Colorado Medicaid recipients transitioning out of a nursing facility back into the community, transition coordinators assist recipients in finding necessary community supports, create transition plans, and provide post-transition supports).

expand the proposal to permit disclosures of PHI to community-based organizations for population-level activities.

Response: The Department is limiting 45 CFR 164.506(c)(6) to disclosures for individual-level care coordination and case management activities that constitute treatment or health care operations. The Department believes that the limitation to individual-level activities will ensure that disclosures made pursuant to 45 CFR 164.506(c)(6) are consistent with the types of treatment and health care operations disclosures that individuals generally expect to occur without the need to provide an authorization and will protect individuals' privacy interests. Limiting the provision in this manner also preserves existing privacy protections and ensures that the scope of permissible disclosures remains tied to the care of a specific individual.

Comment: Some commenters recommended that the Department clarify the types of organizations to which covered entities would be permitted to disclose PHI, the circumstances in which such disclosures may be made, or the services contemplated, and provide examples. Some recommended that the types of organizations identified be interpreted broadly to allow for maximum flexibility. One commenter expressed concern that the proposal would restrict who is permitted to receive PHI for care coordination and case management.

Response: Section 164.506(c)(6) permits disclosures to social services agencies, community-based organizations, HCBS providers, and similar third parties that provide health or human services to specific individuals for individual-level care coordination and case management that constitute treatment or health care operations. The Department believes that the plain regulatory language provides sufficient clarity to allow covered entities to determine whether a potential recipient of PHI falls within the scope of the provision. This approach preserves flexibility and avoids unintentionally excluding organizations that provide care coordination and case management services in a variety of settings. The Department believes that these categories of entities encompass organizations serving many types of individuals across communities, consistent with the purpose of facilitating individual-level care coordination and case management.

This provision does not restrict the ability of a covered entity to disclose PHI for care coordination and case management. Rather, this provision clarifies that an individual's authorization is not required for disclosures to third parties for individual-level care coordination and case management activities that constitute treatment or health care operations. A covered entity is still permitted, but not required, to obtain an individual's consent to disclose the individual's PHI for TPO.[622]

Comment: Commenters expressed mixed views about whether the proposal should be limited to circumstances in which a particular service or provider is identified in an individual's care plan or where a screening assessment has been conducted. Commenters who expressed opposition to such conditions generally did so because they believed that additional requirements or conditions would increase the administrative burden for health care providers or community-based organizations, while commenters who expressed support for imposing such conditions generally did so because they believed that it would be more protective of individuals' privacy. A few commenters recommended that disclosures be limited to circumstances where there is shared care planning between individuals and health care providers. Some commenters urged the Department to specify that a covered entity may make disclosures based on their good faith belief that the disclosure is in the best interests of the individual. Another commenter asserted that regulated entities should disclose PHI to a community-based organization only if the organization requests the disclosure.

Many commenters raised concerns about the potential negative effects of disclosures to certain types of organizations on health disparities. One commenter asserted that while they supported screening for social needs and documenting such needs in an individual's care plan, requiring documentation of such information in the individual's care plan would serve to further entrench inequities.

Response: The Department is not adopting additional conditions or prerequisites on disclosures permitted under 45 CFR 164.506(c)(6) that would impede timely coordination of services for individuals. The Privacy Rule already permits uses and disclosures of PHI for treatment and health care operations, subject to existing conditions and limitations, including the minimum necessary standard where applicable. The addition of 45 CFR 164.506(c)(6) removes uncertainty and eases care transitions. The Department believes that imposing additional conditions or prerequisites such as care plan documentation, screening assessments, or shared care planning would create barriers to care coordination and case management and increase the administrative burden for health care providers and community-based organizations.

Comment: Several commenters requested clarification of how the proposal would interact with other laws that regulate the use and disclosure of certain health information about individuals that also may be PHI, such as 42 CFR part 2 (''Part 2''), the information blocking regulations, and state laws. A few commenters requested that the Department expressly state that this provision would not require such disclosures and it would allow covered entities to implement consent processes where required by other laws. One commenter expressed support for this proposal to the extent that it would not affect the obligations of Part 2 programs.

Response: The Privacy Rule creates a Federal floor of protection for the privacy of PHI. It preempts state laws that are contrary to a standard, requirement, or implementation specification adopted under the Privacy Rule, with certain exceptions. As discussed above, Congress excepted from HIPAA's general preemption authority contrary provisions of state law that impose requirements, standards, or implementation specifications that are more stringent than those of the Privacy Rule.[623] If a provision of state or other Federal law provides greater privacy protection than a provision of the Privacy Rule, and it is possible for regulated entities to comply with both the state or other Federal law and the Privacy Rule (*e.g.,* where a state or other Federal law requires an individual's authorization for a disclosure that the Privacy Rule would permit without authorization), there is no conflict between the laws, and no preemption as to the state law. Accordingly, nothing in this final rule affects the obligations of covered entities to comply with applicable state or other Federal laws that restrict the disclosure of sensitive information, including information about SUD or other sensitive health issues, nor does it change the compliance obligations of covered entities subject to other Federal laws. For example, the permission in this section does not remove the obligations of covered entities that are also federally funded SUD treatment programs (*i.e.,* Part 2 programs) to

[622] 45 CFR 164.506(b).

[623] *See id.*

obtain patient consent when using or disclosing Part 2 records for treatment, payment, and health care operations purposes.

Similarly, 45 CFR 164.506(c) does not prevent or relieve covered entities from complying with the information blocking regulations. Section 3022(a)(1) of the PHSA generally defines information blocking as a practice that, except as required by law or specified by the Secretary pursuant to rulemaking, is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.[624] Section 3022(a)(1)(A) excludes from the definition of information blocking practices that are required by law, circumstances where one or more elements of the definition is not met, and circumstances where the practice is covered by one of the exceptions for reasonable and necessary activities.[625] For example, if a covered entity is required by a state or Federal law to satisfy a precondition (such as obtaining patient consent or authorization) before providing access to, exchanging, or using EHI, the covered entity may choose not to provide access to, exchange, or use such EHI if the precondition has not been satisfied under certain circumstances.[626]

Comment: Several commenters raised questions about the ability of social services agencies, community-based organizations, HCBS providers, and similar entities to exchange information electronically. Some commenters recommended that the Department provide support or guidance to facilitate electronic information exchange or compliance with HIPAA requirements for policies and procedures. Several commenters recommended that the Department provide resources to enable data segmentation. One commenter expressed concern that technical limitations of EHR systems may make it difficult for covered entities to limit the disclosures of PHI to the minimum necessary. Another commenter requested clarification that covered entities would be permitted to disclose PHI electronically, including through HIEs/HINs.[627]

Response: The Privacy Rule regulates the use and disclosure of PHI maintained in any form or medium. The Department does not prescribe specific means by which covered entities must use or disclose PHI and does not regulate the technical capabilities of entities that are not subject to HIPAA.

A covered entity may use an HIO, such as an HIE/HIN, to facilitate the exchange of PHI for individual-level care coordination and case management that constitute treatment or health care operations, provided that it has a business associate agreement with the HIO that requires the HIO to protect the information.[628] As discussed above, covered entities remain responsible for complying with the minimum necessary standard, as applicable, when disclosing PHI under 45 CFR 164.506(c)(6). However, some of the requests or disclosures to or through the HIO by a covered entity may not be subject to the minimum necessary standard, such as disclosures for the treatment activities of a health care provider. For electronic disclosures by a covered entity to and through an HIO that are subject to the minimum necessary standard, such as for a payment or health care operations purpose, the Privacy Rule would require that the minimum necessary standard be applied to that exchange and that the business associate agreement limit the disclosures by the HIO of, and requests for, PHI accordingly.[629]

Comment: Some commenters expressed concerns about the ability of social services agencies, community-based organizations, HCBS providers, or other similar third parties to safeguard the privacy and security of the information disclosed to them by covered entities pursuant to this proposal. A few commenters recommended that the Department specify that the disclosure of PHI should be limited to persons who have implemented appropriate privacy and security measures or that the Department provide guidance on how the information should be safeguarded after PHI has been disclosed. Several commenters expressed concerns about the ability of third parties to re-disclose an individual's PHI without limitation and urged the Department to take steps to limit re-disclosures of PHI by entities that are not regulated under HIPAA.

Some commenters expressed concerns about potential liability for covered entities if there is a breach after disclosure of PHI to such organizations. A few of these commenters recommended that the Department provide a safe harbor or assurances for covered entities that disclose PHI to social services agencies in the event of a subsequent improper use or disclosure, while another suggested that the Department provide a safe harbor for regulated entities that adopt software that assigns labels to PHI to govern how that PHI may be accessed, used, or disclosed.

Response: The Department declines to require that disclosures under 45 CFR 164.506(c)(6) be limited to entities that have implemented particular privacy or security measures. The Department also declines to establish a safe harbor or impose additional conditions related to the potential liability of covered entities based on actions taken by persons who receive PHI and are not regulated under HIPAA. A safe harbor is unnecessary because a covered entity is not liable for subsequent breaches or improper use of health information by the person who receives it, including a person who is not regulated under HIPAA. We have determined that imposing such conditions could impede timely and effective care coordination and case management because it would require covered entities to assess, verify, or monitor the privacy and security practices of a wide range of persons who are not regulated under HIPAA and may not have standardized or readily assessable frameworks to facilitate such reviews. Requiring covered entities to evaluate privacy or security practices of such persons could not only delay or deter necessary information sharing and

---

[624] *See* Public Law 114–255, 130 Stat. 1176 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–52).

[625] *See* 42 U.S.C. 300jj–52(a)(1) (excluding from the definition of ''information blocking'' practices that are likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI if they are ''required by law''); 85 FR 25642, 25794 (May 1, 2020) (explaining that ''required by law'' specifically refers to interferences that are explicitly required by state or Federal law); *see also* 89 FR 1192, 1351 (Jan. 9, 2024) (affirming that where applicable law prohibits access, exchange, or use of information, practices in compliance with such law are not considered to be information blocking and citing to compliance with the Privacy Rule as an example of an applicable law); *see also* ''Information Blocking Exceptions,'' Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Apr. 2024), *https://healthit.gov/wp-content/uploads/2024/04/IB_Exceptions_Fact_Sheet_508.pdf.*

[626] *See* ''Information Blocking Exceptions,'' *supra note* 625; *see also* ''Would it be information blocking if an act or does not fulfill a request to access, exchange , or use EHI in order to comply with federal privacy laws that require certain conditions to have been met prior to disclosure?,'' *supra note* 608.

[627] *See* 45 CFR 171.102 (definition of ''Health information network or health information exchange'').

[628] *See* 45 CFR 164.502(e) and 164.504(e); *see also* ''May a covered health care provider disclose electronic protected health information (PHI) through a health information organization (HIO) to another health care provider for treatment?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #541 (July 26, 2013), *https://www.hhs.gov/hipaa/for-professionals/faq/541/may-a-covered-health-care-provider-disclose-electronic-protected-health-information/index.html.*

[629] *See* ''How may the HIPAA Privacy Rule's minimum necessary standard apply to electronic health information exchange through a networked environment?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #545 (July 26, 2013), *https://www.hhs.gov/hipaa/for-professionals/faq/545/how-may-hipaas-minimum-necessary-standard-apply-to-electronic-information/index.html.*

create barriers to integrated care, but it also could increase the compliance burden for regulated entities.

Regulated entities remain subject to all applicable requirements of the Privacy and the Security Rules. This includes the obligation to implement reasonable safeguards, to limit disclosures to the minimum necessary PHI as applicable, and to determine whether a recipient is acting as a business associate, in which case a business associate agreement must be in place prior to disclosure.

Comment: Several commenters requested that the Department clarify whether covered entities would be required to enter into business associate agreements with the third parties contemplated in this proposal before making a disclosure. Some commenters recommended that the Department require covered entities to execute written agreements with third parties to limit their use or redisclosure of PHI. A few commenters expressed concern that requiring agreements would increase administrative burden and impede care coordination.

Response: Section 164.506(c)(6) does not impose any new requirements regarding business associate agreements. A covered entity is required to enter into a business associate agreement with a person or organization only when that person or organization meets the definition of a business associate.[630] As discussed above, there may be instances where disclosures for individual-level care coordination and case management that constitute treatment or health care operations under 45 CFR 164.506(c)(6) will be made to business associates engaged by a covered entity to provide health-related services on behalf of the covered entity. In those circumstances, a business associate agreement must be in place prior to the disclosure of PHI. In other circumstances, the person who receives the PHI will not be performing covered functions or activities for or on behalf of the covered entity; it will be providing services to the individual on its own behalf. In such cases, the person who receives the PHI does not meet the definition of a business associate, and a business associate agreement is not required.

Furthermore, the Department declines to require regulated entities to execute additional written agreements with third parties as a condition of disclosures under new 45 CFR 164.506(c)(6). Requiring such agreements would increase administrative burden and risk delaying or impeding care coordination and case management activities. Covered entities remain responsible for complying with the applicable conditions and requirements of the Privacy Rule, including determining whether a person who receives PHI is acting as a business associate and ensuring that a business associate agreement is in place when required.

Comment: A few commenters requested that the Department add definitions or further clarify certain terms related to the proposed permission. For example, some commenters requested a definition of ''social service agencies'' with examples of the types of services contemplated.

Response: The Department is not adopting any additional definitions or exclusions in connection with this provision. The Privacy Rule already defines the terms treatment and health care operations, and those definitions expressly encompass care coordination and case management activities. The Department believes that the robust description and discussion of other definitions for care coordination and case management above affords the regulated community sufficient information with which to determine whether a recipient is engaged in the contemplated activities. As discussed in the 2021 Privacy Rule NPRM, the third parties contemplated by this provision may include a range of organizations that provide health or human services to specific individuals. The third party receiving PHI under this provision does not have to be a health care provider and may instead provide health-related social or other supportive services, such as food or sheltered housing needed to address health risks and conditions. For example, a covered health care provider may disclose the minimum necessary PHI to a senior center or adult day care provider to coordinate health-related services as part of treatment, and a health plan may disclose the minimum necessary PHI to a senior wellness center to coordinate care for an enrolled individual as part of the plan's health care operations.[631]

The Department does not believe that adding definitions or enumerated lists of entities or services would improve clarity and is concerned that doing so could inadvertently limit the application of this provision in varied clinical and community contexts. Covered entities remain responsible for determining whether a disclosure falls within treatment or health care operations and whether the recipient is engaged in individual-level care coordination or case management activities.

Comment: Many commenters expressed concern about the potential risks of this proposal to an individual's privacy. Some commenters recommended that an individual's consent or authorization be required before disclosures to social services agencies and similar third parties for care coordination and case management are made or that individuals be given an opportunity to object to such disclosures. According to some commenters, disclosures of PHI without an individual's consent could alienate individuals, lead to lower engagement with care, or result in care avoidance. A few commenters recommended that covered entities be required to notify individuals of such disclosures in advance. One commenter asserted that it would be reasonable for a clinician to explain to the individual the disclosures that would be made and the implications of disclosing PHI to entities not regulated under HIPAA.

Response: While the Department appreciates commenters' concerns about protecting individuals' privacy interests, we decline to require consent, authorization, advance notice (other than what is required in an NPP),[632] or an opportunity to object as a condition of disclosures permitted under this provision. The Privacy Rule already permits disclosures without authorization for treatment and, in certain circumstances, health care operations, and this final rule clarifies the applicability of those existing permissions to disclosures that are made for these purposes to social services agencies, community-based organizations, HCBS providers, and similar third parties, consistent with longstanding guidance.

Section 164.506(c)(6) is limited to disclosures for individual-level care coordination and case management that constitute treatment or health care operations, rather than population-level activities, and such disclosures remain subject to the minimum necessary standard, where applicable. The limitation to individual-level activities ensures that the disclosures made under this permission are comparable to disclosures for treatment, which individuals expect to occur without

[630] 45 CFR 160.103 (definition of ''Business associate'').

[631] 86 FR 6475–76 (Jan. 21, 2021).

[632] The Privacy Rule requires that the NPP contain a description, including at least one example, of the types of uses and disclosures the covered entity is permitted to make for treatment and health care operations (as well as for payment), among other information, and the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required. *See* 45 CFR 164.520(b)(1)(ii)(A) and (D).

their authorization or consent. The right to request restrictions on disclosures for TPO purposes also remains available for individuals to request limitations on such disclosures.[633]

Comment: A few commenters expressed concern that the proposed provision could permit disclosures of PHI to law enforcement or child welfare agencies. Several commenters identified examples of potential harms that they believed could result from this proposal, including discrimination, increased health disparities and inequities, and loss of privacy.

Response: This provision does not permit disclosures of PHI to law enforcement or child welfare agencies for law enforcement or investigatory purposes. The Privacy Rule's existing provisions governing disclosures for law enforcement, public health, or other public policy purposes remain unchanged by this final rule and continue to apply independently of 45 CFR 164.506(c)(6).

The Privacy Rule does not permit a regulated entity to disclose PHI for law enforcement purposes without an individual's authorization unless the disclosure is made pursuant to process and as otherwise required by law,[634] or another express permission applies.[635] Additionally, disclosures to child welfare or protective services agencies are permitted only under the applicable provisions of the Privacy Rule, including disclosures for public health activities and for reports of child abuse, domestic violence, and neglect.[636] Section 164.506(c)(6) does not expand or alter these existing permissions.

Comment: Some commenters requested clarification of how this proposal would interact with the proposed modification to the minimum necessary standard or recommended modifications that would require the application of the minimum necessary standard to the proposal.

Response: As discussed in this final rule, the Department is not finalizing the proposed exception to the minimum necessary standard for health care operations uses and disclosures related to individual-level care coordination and case management.[637] This final rule does not alter the minimum necessary requirements.

The applicability of the minimum necessary standard for disclosures of PHI to a third party for individual-level care coordination and case management is governed by 45 CFR 164.502(b). Disclosures to or requests by a health care provider for the treatment activities of either the requesting health care provider or another health care provider are not subject to the minimum necessary standard. Disclosures of PHI for treatment to third parties that are not health care providers and for health care operations remain subject to the minimum necessary standard. Thus, if the minimum necessary standard applies, a covered entity must take reasonable steps to limit the disclosure of PHI to the minimum necessary to accomplish the intended purpose.[638]

F. Encouraging Disclosures of PHI When Needed To Help Individuals Experiencing Substance Use Disorder (Including Opioid Use Disorder), Serious Mental Illness, and in Emergency Circumstances

1. Current Rule

Sections 164.502(g) and 164.510–164.514 of the Privacy Rule permit covered entities to disclose PHI in certain circumstances when an individual is unable to agree or object to the disclosure of their PHI or where a disclosure may be needed to prevent or lessen a threat to health or safety. In such circumstances, the Privacy Rule provides for the exercise of professional judgment when determining whether such disclosure should be made.

Disclosures to Personal Representatives

Under 45 CFR 164.502(g), a personal representative generally is a person with authority under applicable law (*e.g.,* state law) to act on behalf of an individual in making decisions related to health care.[639] In many circumstances, the parent or guardian of an unemancipated minor child is treated as the child's personal representative under applicable law. In circumstances where state or other applicable law does not treat a parent as an unemancipated minor child's personal representative, 45 CFR 164.502(g)(3)(ii)(C) permits, but does not require, covered entities to provide PHI under the right of access to a parent, guardian or other person acting *in loco parentis,* if the action is consistent with state or other applicable law and the decision to disclose the child's PHI is based on the professional judgment of a licensed health care professional.

Uses and Disclosures Requiring an Opportunity for the Individual To Agree or Object

Section 164.510 of the Privacy Rule generally requires that covered entities must provide an individual with the opportunity to agree or object before using or disclosing the individual's PHI for inclusion in a facility directory or disclosing PHI to family members, caregivers, or others involved in care or payment for care. However, individuals are not always able to agree or object to such uses or disclosures, particularly in emergency situations. Accordingly, 45 CFR 164.510(a)(3) permits a covered health care provider to disclose in its facility directory certain PHI, including name, location within the facility, general condition, and religious affiliation to clergy and persons who ask for the individual by name, when the individual cannot agree or object because of incapacity or an emergency treatment circumstance, if providing this information meets both of the following conditions:

- The disclosure is consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider.
- The disclosure is in the individual's best interests, as determined by the covered health care provider, in the exercise of professional judgment.

For similar reasons, 45 CFR 164.510(b)(2)(iii) permits a covered entity to disclose relevant PHI about an individual who is present and has decision-making capacity, if the covered entity can reasonably infer, based on the exercise of professional judgment, that the individual does not object to the disclosure. Further, 45 CFR 164.510(b)(3) permits a covered entity to disclose relevant PHI about an individual who is not present or cannot agree or object because of incapacity or an emergency circumstance to family members and other caregivers involved in the individual's care or payment for care, if the covered entity, based on professional judgment, determines that the disclosure is in the best interests of the individual.

Disclosures To Avert a Threat to Health or Safety

Section 164.512(j) of the Privacy Rule permits covered entities, consistent with applicable law and standards of ethical conduct, to use or disclose PHI when

---

[633] *See* 45 CFR 164.522(a).

[634] *See* 45 CFR 164.512(f)(1).

[635] *See* ''When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #505 (Dec. 28, 2022), *https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.*

[636] *See* 45 CFR 164.512(b)(1)(ii) and (c).

[637] *See* proposed 45 CFR 164.502(b)(2)(i).

[638] *See* 45 CFR 164.502(b) and 164.514(d); *see also* ''Minimum Necessary Requirement,'' Office for Civil Rights, U.S. Department of Health and Human Services (Apr. 4, 2003), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html.*

[639] 45 CFR 164.502(g)(3)(i) and (g)(5) contain the exceptions to this general rule.

necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.[640] To ''lessen'' a threat could mean, for example, to reduce the severity of the threatened harm, or the likelihood of the anticipated harm occurring. The permission is intended to accommodate, and be consistent with, a ''duty to warn'' others of a threat as established in case law (and in some states, statutory requirements).[641] Certain conditions apply, including that the recipient of the PHI must be reasonably able to prevent or lessen the threat, or the use or disclosure must be necessary for law enforcement to identify or apprehend the subject individual.[642] In the case of a disclosure to law enforcement, additional conditions include that the individual made a statement admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim, or that circumstances demonstrate that the subject individual escaped from a correctional institution or lawful custody, as defined in the Privacy Rule.[643]

Identity Verification

Section 164.514(h)(2)(iv) of the Privacy Rule generally requires covered entities to verify the identity and authority of a person requesting PHI.[644] In certain situations, the circumstances surrounding the disclosure itself may accomplish the verification without having to collect additional documents or rely on a preestablished procedure.[645] Accordingly, 45 CFR 164.514(h)(2)(iv) provides that a covered entity's obligation to verify a requestor's identity is met if the covered entity relies on an exercise of professional judgment pursuant to 45 CFR 164.510, or acts on a good faith belief in making a disclosure pursuant to 45 CFR 164.512(j) to prevent or lessen certain serious and imminent threats.

2. Proposed Rule

As we explained in the 2021 Privacy Rule NPRM,[646] support from family members, friends, and caregivers is essential for many individuals who are experiencing SUD[647] or SMI.[648] However, family members and caregivers need sufficient information to provide this support.

To address these concerns, the Department has issued extensive guidance on the circumstances in which the Privacy Rule permits disclosures of PHI to an individual's friends, family, and others.[649] For example, guidance issued in 2017 addresses the permission for covered health care providers to disclose PHI to an individual's friends, family, and others involved in the individual's care or payment for that care when the individual has experienced an overdose and is unable to agree or object to uses and disclosures of PHI.[650] The guidance clarifies that a health care provider may use professional judgment to talk to the parents of an individual who has been incapacitated by an opioid overdose about the overdose and related medical information, but generally cannot share PHI unrelated to the overdose without the individual's agreement.[651] The guidance further clarifies when a covered health care provider may rely on the permission at 45 CFR 164.512(j) in an overdose situation. Additionally, in response to the Cures Act,[652] OCR compiled a full suite of guidance and materials on its website related to mental and behavioral health for health care professionals and consumers.[653] As we explained in the 2021 Privacy Rule NPRM, although the guidance focuses primarily on overdose situations, the provisions apply equally to the disclosure of PHI during other health emergencies or dangerous situations.

Despite this extensive guidance, the Department continued to receive reports that covered entities were reluctant to disclose PHI to persons involved in the care of individuals experiencing SUD or SMI, even when the Privacy Rule permits such disclosures. Accordingly, in the 2021 Privacy Rule NPRM, we proposed to replace ''exercise of professional judgment'' with ''good faith belief'' as the standard pursuant to which covered entities would be permitted to make certain uses and disclosures in the best interests of individuals in 45 CFR 164.502(g)(3)(ii)(C), 164.510(a)(3), 164.510(b)(2)(iii), 164.510(b)(3), and 164.514(h)(2)(iv). In these five provisions, the proposed new standard in 45 CFR 164.502(k) would include a presumption of a covered entity's good faith that could be overcome with evidence of bad faith. Under this proposal, disclosures for any improper purpose, such as crime, fraud, or personal enrichment, would be considered ''bad faith'' disclosures. Additionally, in 45 CFR 164.512(j), we proposed to replace ''serious and imminent'' threat with ''serious and reasonably foreseeable,'' define reasonably foreseeable based on an ordinary person's understanding, and add a provision for heightened

[640] 45 CFR 164.512(j)(1)(i)(A).

[641] *See* 65 FR 82462, 82538 (Dec. 28, 2000); *see also* state law requirements compiled at *https://www.ncsl.org/health/mental-health-professionals-duty-to-warn.* To the extent that state or other law requires a disclosure (*e.g.,* as part of a statutory duty to warn), the Privacy Rule would permit the disclosure under its permission for uses and disclosures of PHI required by law. *See* 45 CFR 164.512(a). However, not all states have enacted such requirements, and those that do apply a variety of different standards. In contrast, HIPAA's disclosure permission applies a uniform permissive standard to covered entities nationwide.

[642] *See* 45 CFR 164.512(j)(1)(ii).

[643] *Id.; see also* 45 CFR 164.501 (definition of ''Correctional institution'').

[644] *See* 65 FR 82462, 82546–47 (Dec. 28, 2000). When considered with 45 CFR 164.530(i) and (j), the Privacy Rule generally requires covered entities to establish and use written policies and procedures reasonably designed to verify the identity and authority of the person requesting PHI.

[645] *Id.*

[646] *See* 86 FR 6446, 6477 (Jan. 21, 2021).

[647] SUDs occur when the recurrent use of alcohol and/or drugs causes clinically significant impairment, including health problems, disability, and failure to meet major responsibilities at work, school, or home. *See* ''Co-Occurring Disorders and Other Health Conditions,'' Substance Abuse and Mental Health Services Administration, U.S. Department of Health and Human Services (Dec. 22, 2025), *https://www.samhsa.gov/find-help/disorders.*

[648] SMI is defined by someone over 18 having (within the past year) a diagnosable mental, behavioral, or emotional disorder that causes serious functional impairment that substantially interferes with or limits one or more major life activities. For minors, the term ''Serious Emotional Disturbance'' refers to a diagnosable mental, behavioral, or emotional disorder in the past year, which resulted in functional impairment that substantially interferes with or limits the child's role or functioning in family, school, or community activities. *Id.*

[649] *See* ''Information Related to Mental and Behavioral Health, including Opioid Overdose,'' Office for Civil Rights, U.S. Department of Health and Human Services (Feb. 13, 2026), *https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html.*

[650] ''When does HIPAA allow a doctor to notify an individual's family, friends, or caregivers that a patient has overdosed?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #3001 (Jan. 4, 2018), *https://www.hhs.gov/hipaa/for-professionals/faq/3001/when-does-hipaa-allow-doctor-notify-individuals-family-friends-caregivers-patient-has-overdosed/index.html.*

[651] ''How HIPAA Allows Doctors to Respond to the Opioid Crisis,'' Office for Civil Rights, U.S. Department of Health and Human Services (2017), *https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents/hipaa-opioid-crisis.pdf.*

[652] Section 11001 of the Cures Act includes a ''sense of Congress'' that clarification was needed regarding the Privacy Rule's existing permitted uses and disclosures of PHI by health care professionals to communicate with caregivers of adults with SMI to facilitate treatment, while section 11003(b) directed the Secretary, acting through the Director of OCR, to issue guidance clarifying the circumstances in which a covered entity may disclose PHI, including those that are based on the exercise of professional judgment regarding the best interests of a patient when the patient is incapacitated or in an emergency situation, and the circumstances in which a covered entity may disclose PHI to a patient's family and other caregivers. *See* Public Law 114–255, 130 Stat. 1270 (Dec. 13, 2016) (codified at 42 U.S.C. 1320d–2 note).

[653] *See* ''Information Related to Mental and Behavioral Health, including Opioid Overdose,'' *supra* note 649.

deference to decisions about such disclosures by workforce members with specialized training, expertise, or experience.

3. Overview of Comments

The commenters expressed support for and opposition to these proposals in even numbers. Family members and caregivers of individuals experiencing SUD or mental illness generally expressed support for the proposals about good faith and preventing harm and threatened harm because they believed that the proposed modifications would encourage health care providers to provide PHI to the family members and caregivers without fear of violating HIPAA, particularly during emergencies, crises, and circumstances in which the individual is incapacitated. In contrast, many commenters expressed opposition to the proposal because they believed that it would decrease an individual's privacy and autonomy. Many of these commenters asserted that the proposed modifications would lead to discrimination, shame, stigma, interference with efforts to seek care, and care avoidance.

4. Final Rule

The Department is not finalizing the proposed changes to the standards for good faith and professional judgment in 45 CFR 164.502 and 164.510–514. Upon review and analysis of public comments, the Department is not persuaded that the proposed changes would provide the clarity sought. We also are concerned that finalizing the proposals could increase complexity and burden for covered entities while chilling access to care. The Department believes that additional technical assistance and public education about the Privacy Rule's provisions that permit covered entities to disclose PHI to an individual's family and caregivers would better address any misunderstandings about the scope of the existing permissions.

5. Responses to Public Comments

Comment: Many commenters expressed support for the proposal to replace the ''professional judgment'' standard with a ''good faith'' standard because they believed that it would reduce barriers that prevent family members and caregivers from assisting loved ones experiencing SUD or SMI. They described challenges under the current rule, including a lack of notification to family members and caregivers when the individual is discharged, difficulty locating loved ones, and their inability to obtain the information that they need to support individuals who cannot care for themselves. Commenters asserted that the proposed changes would improve access to care, enable earlier intervention, and facilitate more effective coordination between families and clinicians.

Response: The Department recognizes the difficulties families and caregivers face when caring for individuals with SUD and SMI. However, after reviewing the comments, the Department has determined that replacing ''professional judgment'' with a ''good faith'' standard likely would introduce ambiguity without improving outcomes. The equal proportion of comments expressing support for and opposition to the proposals reinforces the need for a measured approach to balancing the privacy interests of individuals with the need for disclosure in urgent situations. The Department is persuaded that the existing provisions provide the appropriate balance. Rather than finalizing the proposed changes, the Department intends to emphasize outreach and technical assistance to covered entities to improve their understanding of existing permissions to disclose PHI to family, friends, and caregivers.

Comment: Some commenters asserted that the proposal to adopt a good faith standard would help health care providers, family members, and caregivers respond effectively during emergencies. According to these commenters, this proposal would reduce providers' concerns about violating the Privacy Rule, alleviate confusion about what the Privacy Rule permits, and facilitate appropriate disclosures of PHI. A few commenters stated that the proposal would reduce the refusal of covered entities to disclose PHI and improve continuity of care.

Response: The Department acknowledges commenters' interest in reducing uncertainty involving disclosures allowed under 45 CFR 164.502(g), 164.510, and 164.512(j). However, the Department has determined that altering the disclosure standard likely will not resolve concerns about the hesitancy of covered entities to disclose PHI and, in fact, could create additional challenges. Instead, we will continue to focus on providing outreach and technical assistance to address these concerns.

Comment: A few commenters recommended various further modifications, such as applying good faith based on the belief that disclosure will improve the individual's care or benefit the individual. Others suggested that the Department add exceptions that would permit a covered entity to override an individual's prior expressed preference in certain circumstances.

A few commenters requested that the Department clarify what would constitute good faith under the proposed standard and how the proposal would interact with information blocking regulations, protect sensitive PHI, and apply to non-clinical workforce members, such as peer counselors. A few commenters suggested that the Department provide safe harbors for disclosures made in good faith, and a few requested that the Department provide guidance on how to address situations in which an individual's previously expressed disclosure preferences may have changed.

Response: As discussed above, the Department is not finalizing the proposals to replace the professional judgment standard with a good faith standard. The Department's decision not to finalize the proposed changes to the professional judgment is based, in part, on the lack of clear consensus on whether the modifications would offer meaningful improvements to individuals' health care and access to care.

Comment: Several commenters expressed support for the Department's proposal to revise 45 CFR 164.512(j) by replacing ''serious and imminent'' with ''serious and reasonably foreseeable.'' These commenters asserted that this proposal would allow for earlier intervention and help prevent escalations in harm. A few commenters requested that the Department give greater deference to harm assessments made by health care professionals with specialized clinical or behavioral health training.

Response: Rather than providing the certitude sought by commenters, the Department has determined that revising the threat standard in 45 CFR 164.512(j) could increase uncertainty about when disclosures are appropriate. Accordingly, the Department is not finalizing this proposed revision. Instead, we refer stakeholders to guidance issued by OCR on applying the serious and imminent threat standard for individuals with mental health conditions and SUD.[654]

Comment: A few commenters who expressed support for the proposals requested that the Department clarify

[654] ''HIPAA Privacy Rule and Sharing Information Related to Mental Health'' Office for Civil Rights, U.S. Department of Health and Human Services (Feb. 13, 2026), *https://www.hhs.gov/sites/default/files/hipaa-privacy-rule-and-sharing-info-related-to-mental-health.pdf.*

the interaction of the proposed changes with state laws or consider preempting stricter state requirements to ensure consistency.

Response: The preemption provisions of HIPAA are statutory; thus, they are not subject to modification by the Department. HIPAA excepts from its general preemption authority contrary provisions of state law that impose requirements, standards, or implementation specifications that are more stringent than those of the Privacy Rule.[655] In addition, if a provision of state or other Federal law provides greater privacy protection (*e.g.,* a state or Federal law that requires an individual's consent or authorization before a covered entity is permitted to disclose PHI) than a provision of the Privacy Rule, and it is possible for regulated entities to comply with both the state or other Federal law and the Privacy Rule, there is no conflict between the laws and no preemption of state law.

Comment: Several commenters urged the Department to better align the HIPAA Rules and Part 2 to reduce barriers to coordinated care for individuals with SUD.

Response: The Privacy Rule does not conflict with Part 2 in circumstances where it is possible for regulated entities to comply with both Part 2 and the Privacy Rule. Thus, where the HIPAA Rules and Part 2 both apply, the Privacy Rule permissions for disclosure without authorization to family members, caregivers, and others do not negate Part 2's general requirement to obtain a patient's written consent for the disclosure of Part 2 records.[656] Where an exception to Part 2's general requirement applies, a Privacy Rule permission also may apply, subject to the conditions of the applicable Part 2 exception. For example, Part 2 permits disclosure without patient consent for a bona fide medical emergency, subject to the condition that the disclosure be documented afterwards, while the Privacy Rule permits—but does not require—a broader range of disclosures without an individual's authorization for treatment purposes, including emergency medical treatment. Accordingly, a covered entity that is also subject to Part 2 can be in compliance with both regulations when it makes the more limited disclosure permitted by Part 2 for a bona fide medical emergency and meets the applicable requirements and conditions of both the Part 2 exception and Privacy Rule permission.

To address concerns about the alignment between Part 2 and the HIPAA Rules, the Department published two final rules in early 2024. The Confidentiality of Substance Use Disorder (SUD) Patient Records Final Rule, published on February 16, 2024,[657] and the 2024 Privacy Rule, published April 26, 2024,[658] implemented section 3221 of the CARES Act and modified the requirements of the NPP to align it with the Part 2 Patient Notice. This final rule makes additional modifications to the NPP, discussed in detail below, to further align it with the Part 2 Patient Notice.

Comment: A few commenters asserted that the proposal to replace the professional judgment standard would not discourage individuals from seeking care and that a good faith approach could improve care coordination. A few commenters urged the Department to expand the definition of incapacity to include individuals who cannot exercise sound judgment because they have been diagnosed with dementia, psychosis, or another SMI.

Response: The Department is concerned that modifying the professional judgment standard for disclosing PHI to an individual's family, friends, and caregivers or altering the definition of incapacity could introduce more ambiguity and result in unintended consequences. Although an individual who has been diagnosed with dementia, psychosis, or other SMI may lack decision-making capacity in some circumstances, a diagnosis of SMI, by itself, does not determine whether an individual can make independent decisions.[659] Neither 45 CFR 164.510 nor 45 CFR 164.512 requires a legal determination of incapacity; instead, an individual's inability to make decisions about uses and disclosures of their PHI may be transient or situational. For example, an individual with SMI may temporarily lack decision-making capacity when their symptoms are untreated, but their decision-making capabilities may resume upon treatment.[660]

Comment: Some commenters expressed opposition to the proposal to replace the professional judgment standard with a good faith standard because they believed that it would weaken privacy protections for individuals' PHI, increase stigma associated with SUD and SMI, and deter individuals from seeking care. These commenters asserted that broad disclosure permissions could particularly harm individuals in certain situations (*e.g.,* individuals seeking sensitive health care services such as mental health care and SUD treatment).

A few commenters asserted that the proposal to replace the professional judgment standard was unnecessary because the Privacy Rule already permits appropriate disclosures to family members or caregivers. According to these commenters, it is misinformation, not regulatory limits, that leads to inappropriate refusals to disclose PHI.

Several commenters expressed opposition to the Department's proposal to replace professional judgment with good faith because they believed that clinical expertise should guide decisions about the appropriateness of disclosures of PHI to family, friends, and caregivers. These commenters also asserted that a good faith standard would be subjective and difficult to enforce. Several commenters expressed concern that the proposal would allow non-clinical workforce members to make disclosure decisions without sufficient knowledge of an individual's circumstances. Other commenters observed that covered entities sometimes lack information about family dynamics.

Some commenters expressed opposition to the proposal to include a presumption of good faith and stated that individuals would struggle to prove bad faith without a requirement that covered entities document the rationale for their decision.

A few commenters expressed their opposition to the implementation of a good faith standard for identity verification because they believed that family members would not need to provide proof of their identity under such a standard.

Response: As discussed above, the Privacy Rule already permits many of the disclosures sought by family members and caregivers. OCR has longstanding guidance on these topics, including those that specifically address circumstances involving individuals that have been diagnosed with mental and behavioral health conditions, such

[655] *See* 45 CFR 160.203(b).

[656] Part 2 generally prohibits the disclosure of a patient's Part 2 records absent the patient's written consent, or a court order and subpoena, except in certain limited circumstances, such as in a bona fide medical emergency; for scientific research; for management audits, financial audits, and program evaluation; and to public health authorities. *See* 42 CFR 2.13 and 2.51–2.54.

[657] 89 FR 12472 (Feb. 16, 2024).

[658] 89 FR 32976 (Apr. 26, 2024). The vacatur of most of the 2024 Privacy Rule left intact the provisions of the rule related to Part 2. *See Purl,* 787 F. Supp. 3d 284.

[659] *See* Dilip V. Jeste, et al., ''Supported Decision Making in Serious Mental Illness,'' Psychiatry, p. 3 (Aug. 15, 2018), *https://pmc.ncbi.nlm.nih.gov/articles/PMC6093283/pdf/nihms-1502003.pdf.*

[660] *Id.*

as SMI and SUD.[661] The Department agrees that maintaining trust and confidentiality is essential for individuals to seek health care and that decisions to disclose PHI about individuals in certain circumstances may require the exercise of clinical expertise. The Department is persuaded by concerns about the potential chilling effect of the proposals to replace the professional judgment standard at 45 CFR 164.502(g) and 45 CFR 164.510–512 with a good faith standard on the willingness of individuals to seek or obtain health care, as well as concerns that the proposals might cause additional confusion or limit an individual's exercise of their autonomy. Accordingly, we are not finalizing the proposed changes to the professional judgment standard in 45 CFR 164.502(g) and 45 CFR 164.510–512. Moreover, commenters have convinced us that the current provisions in the Privacy Rule are sufficient to permit appropriate disclosures to family members or caregivers.

Comment: Many commenters expressed their belief that covered entities should honor the expressed privacy preferences of individuals except in true emergencies.

Response: The Privacy Rule requires that a covered entity honor an individual's expressed privacy preferences in certain circumstances.[662] While not required in many circumstances, the Department generally encourages covered entities to take an individual's expressed privacy preferences into consideration before making permitted disclosures.

G. Modifying Notice of Privacy Practices Requirements To Reduce Regulatory Burden and Increase Transparency

1. Current Rule

The Privacy Rule generally requires that certain covered entities provide individuals with an NPP to ensure that they understand how the covered entity may use and disclose their PHI, their rights, and the covered entity's legal duties with respect to PHI.[663] There are limited exceptions to this general requirement. For example, a correctional institution[664] that is a covered entity is not required to provide individuals who are inmates[665] with a copy of its NPP.[666]

Section 164.520(b) of the Privacy Rule describes the contents of the NPP, both required and optional, including descriptions of the types of permitted uses and disclosures of individuals' PHI. For example, the NPP must describe how the covered entity is permitted to use and disclose PHI for TPO,[667] as well as each of the other purposes for which the covered entity is permitted or required to use or disclose PHI without the individual's written authorization.[668] Additionally, the NPP must include a statement that the covered entity is required by law to maintain the privacy of PHI and abide by the terms of the current notice.[669] It also must include a statement of the individual's rights with respect to PHI, including the right to inspect or obtain a copy of their PHI, or both, and a brief description of how the individual may exercise these rights.[670] If the covered entity intends to use or disclose PHI to engage in certain activities, such as fundraising, the NPP must contain statements informing the individual of such activities.[671]

Section 164.520(c) of the Privacy Rule sets forth the circumstances in which a covered entity must provide the NPP to an individual. Under 45 CFR 164.520(c)(2)(ii), a covered health care provider that has a direct treatment relationship with an individual generally must make a good faith effort to obtain a written acknowledgment of receipt of the provider's NPP. If the provider is unable to do so, it must document its good faith efforts and the reason for not obtaining the acknowledgment and maintain such documentation for six years.[672] Those same requirements apply to an NPP sent electronically.[673]

2. Proposed Rule

The Department has proposed changes to the NPP requirements several times in recent years, including in the 2021 Privacy Rule NPRM and the 2022 Part 2 NPRM.[674] Some of those proposals were finalized in the 2024 Privacy Rule, while others remain outstanding. This final rule addresses those outstanding proposals, as summarized below.

Of significance, we proposed to eliminate 45 CFR 164.520(c)(2)(ii), which requires a covered health care provider that has a direct treatment relationship with an individual to obtain a written acknowledgment of receipt of the NPP. Removing this provision also would eliminate the requirement that if the covered health care provider is unable to obtain the written acknowledgment, it must document its good faith effort and the reason for not obtaining the acknowledgment.[675] Similarly, the Department proposed to remove, from 45 CFR 164.520(c)(2)(iii),[676] the same requirements for an NPP sent electronically. We also proposed to remove the requirement at 45 CFR 164.520(e) to retain copies of such documentation for 6 years, pursuant to 45 CFR 164.530(j)(2).

To ensure that individuals are informed about a covered entity's privacy practices, we proposed to replace the written acknowledgment with a right for the individual to discuss the NPP with a person designated by the covered entity. Additionally, we proposed at 45 CFR 164.520(b)(1)(vii) to require the covered entity to include the designated contact person's email address and a statement specifying that the designated person is available to answer questions about the NPP.

The Department also proposed to modify the prominent and specific language in the NPP header to help increase individuals' understanding of a covered entity's privacy practices and their rights with respect to their PHI. We proposed to modify the required header to specify that the notice provides information to individuals about: (1) how to access their health information; (2) how to file a HIPAA complaint; and (3) their rights to their medical information, including an individual's right to receive a copy of the notice and to discuss its contents with a designated person. Additionally, in preamble, we explained that we were considering adding a requirement that the header specify whether the designated contact

[661] ''Information Related to Mental and Behavioral Health, Including Opioid Overdose,'' *supra* note 649; *see also* ''Does the HIPAA Privacy Rule permit a doctor to discuss a patient's health status, treatment, or payment arrangements with the patient's family and friends?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #488 (Nov. 3, 2003), *https://www.hhs.gov/hipaa/for-professionals/faq/488/does-hipaa-permit-a-doctor-to-discuss-a-patients-health-status-with-the-patients-family-and-friends/index.html.*

[662] *See* 45 CFR 164.510 and 164.522(a).

[663] *See* 45 CFR 164.520. Section 164.520 applies only to certain covered entities, as opposed to all covered entities or both covered entities and their business associates. *See also* 45 CFR 164.500(b) with respect to the applicability of 45 CFR 164.520 to health care clearinghouses.

[664] *See* 45 CFR 164.501 (definition of ''Correctional institution'').

[665] *See* 45 CFR 164.501 (definition of ''Inmate'').

[666] 45 CFR 164.520(a)(4).

[667] 45 CFR 164.520(b)(1)(ii)(A).

[668] 45 CFR 164.520(b)(1)(ii)(B).

[669] 45 CFR 164.520(b)(1)(v)(A) and (B).

[670] 45 CFR 164.520(b)(1)(iv).

[671] 45 CFR 164.520(b)(1)(iii).

[672] *See* 45 CFR 164.520(e) and 45 CFR 164.530(j)(2).

[673] 45 CFR 164.520(c)(3)(iii).

[674] Many of these changes were proposed in both the 2021 Privacy Rule NPRM and the 2022 Part 2 NPRM.

[675] *See* 45 CFR 164.520(c)(2)(ii).

[676] This modification was not discussed in the preamble of the 2021 Privacy Rule NPRM but was included in the amendatory text.

person is available onsite. The Department also proposed to require that the header include a phone number and email address the individual can use to reach the designated person. And in the 2022 Part 2 NPRM, the Department proposed to make a non-substantive modification to change the word ''Medical'' to ''Health'' throughout the header to refer to the type of information covered by the NPP.[677]

Consistent with the proposed language in the header, the Department proposed to modify the required element of an NPP that addresses the right of access. The Department proposed to require that an NPP describe how an individual can exercise the right to obtain a copy of their records at limited cost or, in some cases, free of charge, and the right of access to direct.

Additionally, the Department proposed at 45 CFR 164.520(b)(2)(iii) to permit covered entities to include in the NPP information to address circumstances in which individuals seek to direct their PHI to a designated person, when the request does not meet the conditions of the right of access to direct under 45 CFR 164.524(d).

Finally, in the 2022 Part 2 NPRM, the Department proposed to remove the provision that excepts individuals who are inmates of correctional institutions that are covered entities from the requirement that covered entities must provide individuals with an NPP.[678] The Department explained that we no longer believed there to be a safety or security risk associated with providing inmates an NPP.

3. Overview of Comments

Most commenters asserted that the requirement to obtain a written acknowledgment increases the administrative burden on covered entities and is misunderstood by individuals. Commenters were evenly divided on their views of the proposed content modifications to the NPP. Several commenters stated that the proposed NPP changes would increase administrative burdens. A few commenters expressed opposition to the proposal to provide individuals with the right to discuss the NPP with a designated contact person because they believed that it would be more burdensome than obtaining the written acknowledgment. According to these commenters, the proposal was unnecessary because individuals always have had the ability to ask questions about the NPP. Several commenters expressed support for creating a right for an individual to discuss the NPP with a designated person because they believed that it would increase individuals' understanding of their privacy rights. Some commenters asserted that the proposed header modifications would draw attention to the items of greatest relevance to the individual.

A few commenters expressed support for the Department's proposal that would eliminate the provision that excepts individuals who are inmates of correctional institutions that are covered entities from the requirement that covered entities must provide individuals with an NPP because they believed that such individuals would benefit from transparency about how their health information is used and disclosed. One commenter asserted that providing the NPP would increase the burden on workforce members with minimal benefit to the individual who is an inmate.

4. Final Rule

The Department is finalizing our proposals to modify the NPP provisions, including certain proposals included in the 2022 Part 2 NPRM, with minor modifications as described below. Specifically, we are removing the requirement at 45 CFR 164.520(c)(2)(ii) for a covered health care provider with a direct treatment relationship to an individual to obtain a written acknowledgment of receipt of the NPP. Removing this provision also eliminates the requirement that if a covered entity is unable to obtain the written acknowledgment, it must document its good faith efforts and the reason for not obtaining the acknowledgment. Relatedly, we are removing the parallel requirement at 45 CFR 164.520(c)(3)(iii) for an NPP sent electronically. We also are removing the requirement at 45 CFR 164.520(e) to retain copies of such documentation for 6 years. Removing these NPP requirements eliminates a significant documentation and storage burden for health care providers and increases the resources available for providing high-quality health care. These modifications also will remove the burden on covered entities to document a good faith effort to obtain the written acknowledgment in situations where the individual is unconscious or otherwise incapacitated or cannot sign the acknowledgment because of communication barriers. Moreover, eliminating these requirements will remove confusion for individuals about the purpose of the written acknowledgment or whether it is required for treatment, in addition to removing confusion for workforce members who may erroneously believe that individuals must sign the acknowledgment to obtain care. Eliminating these requirements does not affect the obligation of a covered entity to document compliance with the notice requirements by retaining copies of the versions of the notice issued by the covered entity consistent with 45 CFR 164.530(j).[679]

As discussed above, covered entities must include in the NPP information about individuals' rights under the Privacy Rule and how individuals may exercise those rights with respect to the covered entity.[680] Thus, to ensure that individuals understand and can make decisions based on the information in the NPP, the Department is finalizing the proposal to replace the written acknowledgment requirement with a new provision at 45 CFR 164.520(b)(1)(iv)(G), which requires the NPP to state the individual's right to discuss the NPP with a person designated by the covered entity. A covered entity can satisfy the right to discuss the NPP in a variety of ways. For example, the covered entity could have one or more workforce members with knowledge of the NPP available onsite during business hours to answer questions or could offer to schedule meetings or calls with individuals within a reasonable time period of receiving their requests to discuss (whether a request is made in person, by telephone, or by email). As another example, a covered entity could implement technology, such as super intelligence (SI),[681] in a manner that is compliant with the Privacy and Security Rules, to receive and triage questions from individuals on its NPP, provided that individuals have the option to discuss the NPP with a workforce member knowledgeable about the covered entity's privacy practices to address their questions. Additionally, we are finalizing language to permit covered entities to name either an office or a specific contact person to align the NPP with the Part 2 Patient Notice.[682]

We believe that having a designated contact person or office with whom an individual can discuss their privacy rights will be more effective for

[677] 87 FR 74216, 74237 (Dec. 2, 2022).

[678] At the time the proposal was made, the provision was at 45 CFR 164.520(a)(3). While the 2024 Part 2 Final Rule did not address this proposal, it adopted other modifications, which led to the redesignation of this provision as 45 CFR 164.520(a)(4). *See also* 87 FR 74216, 74237 (Dec. 2, 2022).

[679] *See* 67 FR 53182, 53261 (Aug. 14, 2002).

[680] 45 CFR 164.520(b)(1)(iv).

[681] *See* 91 FR 63129 (Oct. 2, 2026).

[682] *See* 42 CFR 2.22. The Patient Notice applies to Part 2 programs under 42 CFR part 2.

enhancing an individual's understanding of their privacy rights than signing an acknowledgment that they received the NPP. Accordingly, we encourage covered entities to identify as the designated person or office responsible for providing further information and answering questions a person or office that is knowledgeable about the covered entity's privacy practices and HIPAA complaint process, rather than a general customer service contact.

Relatedly, the Department is finalizing its proposal to modify 45 CFR 164.520(b)(1)(vii), which requires a covered entity to provide contact information for their designated contact person or office, including the person or office's email address. We also are finalizing the proposal to require that the NPP specify that the designated contact person or office responsible for providing further information is available to answer questions about the covered entity's privacy practices and receive complaints as required by 45 CFR 164.530(a)(1)(ii).

We adopt our proposal, with a minor modification, to revise 45 CFR 164.520(b)(1)(iv)(C) to describe how an individual can exercise the right of access to obtain a copy of their records at limited cost or, in some cases, free of charge, and the right of access to direct.[683] The Department believes that this modification provides individuals with additional information about how to access their PHI to manage their own health care and payment for care, further empowering them. Consistent with modifications made elsewhere to this final rule, we are replacing ''third party'' with ''person designated by the individual.'' This language aligns with the language of the HITECH Act and emphasizes that the individual themselves (or their personal representative) is seeking the disclosure, not a third party.[684]

To ensure consistency with how NPP content is presented to individuals, the Privacy Rule requires that covered entities use a specific header for their NPP. Accordingly, to improve clarity in the NPP for individuals, the Department is finalizing the proposal to modify 45 CFR 164.520(b)(1)(i) to require that the header state that the NPP provides information about: (1) how to access their health information; (2) how to file a HIPAA complaint; and (3) their rights to their health information, including an individual's right to receive a copy of the notice, and to discuss its contents with a designated person or office. Consistent with the modification to permit covered entities to list a specific office as the designated contact rather than a person, the Department also is finalizing the proposal to modify the header to give covered entities the option to include the contact information of an office rather than a person. We are not finalizing our proposal, described in the preamble, to require that the contact be onsite because we believe it is sufficient for individuals to have the contact person or office's telephone number and email address. However, the Department encourages covered entities to have the designated contact person or someone from the designated office available onsite or otherwise easily reachable during operating hours to promptly answer individuals' questions about the NPP and receive HIPAA complaints.

The Department is also finalizing the proposal to modify the header of the NPP to change the word ''Medical'' to ''Health,'' to align with the modification to the Part 2 Patient Notice. As discussed in the 2022 Part 2 NPRM, this change does not modify substantive requirements. Instead, it will more accurately reflect and clarify that the information covered by the notice is not limited to the information in an individual's medical record.

The Department believes that providing this information at the beginning of the NPP will improve individuals' awareness of their Privacy Rule rights, what they can do if they suspect a violation of the Privacy Rule, and how to contact a designated person or office to ask questions.

The Department also is modifying 45 CFR 164.520(b)(2)(iii) to add a new optional element for a covered entity to include information addressing an individual's alternatives when they seek to direct their PHI to a designated person, but their request is outside the scope of the right of access to direct.[685] This optional element will help increase awareness that individuals retain the right to obtain the PHI directly from the covered entity and give it to a person of their choosing. Alternately, it will inform individuals that they can request that the covered entity send a copy of PHI directly to a designated person using a valid authorization. While this provision is optional, the Department encourages covered entities to include in the NPP information about how an individual can send PHI to a person the individual designates in such circumstances. For example, if an individual requests that a paper copy of PHI in an electronic health record be sent to another person, the covered entity could address in this optional NPP provision how the individual may obtain that information, such as through a request made pursuant to the right of access and send it to the other person themselves, or how to request that the covered entity send the information to the other person pursuant to a valid authorization. We are finalizing this provision as proposed, with one minor modification, replacing ''third party'' with ''person designated by the individual'' to ensure consistency with modifications discussed elsewhere in this final rule.

The Department also is finalizing the proposal that we made in the 2022 Part 2 NPRM to remove the exception at 45 CFR 164.520(a)(4), ''exception for inmates.'' Thus, covered entities that serve correctional institutions, and correctional institutions that are covered entities, will be required to provide individuals who are inmates with a copy of the NPP. Consistent with a goal of section 3221 of the CARES Act, this modification aligns the NPP with the Part 2 Patient Notice, which does not include an exception regarding the provision of the notice to individuals who are inmates. Removing this exception ensures that individuals who are inmates receive an NPP that is consistent with what is provided to other individuals while also retaining the limitation on the ability of individuals who are inmates to exercise the right of access to ensure the safety and security of correctional facility personnel and others.[686] Furthermore, providing individuals who are inmates with an NPP affords inmates greater transparency on how the correctional institution, or a covered entity that serves a correctional institution, may use and disclose their PHI, such entities' legal duties with respect to PHI, and the individuals' rights with respect to their PHI, without changing other rights or duties unrelated to the NPP.

5. Responses to Public Comments

Comment: Most commenters expressed support for the proposal to eliminate the requirement to obtain a signed acknowledgment of the NPP, stating that the requirement is an administrative burden and causes confusion for individuals without providing any meaningful benefit. A few commenters recommended that the Department provide covered entities

[683] *See* 45 CFR 164.524.

[684] *See* sec. 13405(e) of the HITECH Act, 123 Stat. 268 (Feb. 17, 2009) (codified at 42 U.S.C. 17935(e)).

[685] *See* 45 CFR 164.524(d).

[686] *See* 45 CFR 164.524(a)(2)(ii). The Department continues to believe that this limitation is necessary to address potential security concerns that are unique to inmates.

with the ability to obtain an individual's acknowledgment through alternative mechanisms, such as verbal and electronic confirmation. A few commenters expressed opposition to the proposal because they believed that the acknowledgment requirement ensures that individuals receive the NPP and are aware of the covered entity's privacy practices.

Response: Eliminating the requirement to obtain a written acknowledgment of receipt of the NPP will reduce the covered entity's administrative burden, improve workflow congestion, and allow more time for individuals to discuss the NPP with the designated person or office. The Department is not replacing the requirement to obtain a written acknowledgment with an alternative mechanism, such as obtaining verbal or written confirmation of receipt, because such requirement would add unnecessary complexity. Importantly, removing the requirement to obtain a written acknowledgment does not remove the requirement for covered entities to provide individuals, including inmates, with an NPP to ensure that they are aware of the entity's privacy practices and know how to contact a designated person or office to answer any questions about the NPP or submit a HIPAA complaint. This modification also does not affect an individual's ability to access an NPP that is posted on a covered entity's website, consistent with the Privacy Rule's requirements for the website posting of NPPs.[687] Removal of this requirement does not prevent a covered entity from continuing to document that it has provided individuals with an NPP if it wishes to do so.

Comment: Several commenters expressed support for the Department's proposal to create a right for an individual to discuss the NPP with a designated contact person. A few commenters recommended that the Department permit the designated person to be a group or a department, rather than requiring that it be a particular person, because it would allow the covered entity to identify the specific person who is best able to respond to each inquiry. One commenter recommended that the Department require that the designated contact person meet certain minimum qualifications.

Some commenters expressed opposition to the proposal because they believed that it would be burdensome and unnecessary. According to these commenters, this proposal would replace the documentation burden with an increase in workforce time and burden on workflow.

Response: The Department is adopting a modified version of the proposal that requires covered entities to designate a person or office as the contact for discussing the NPP with individuals and accepting HIPAA complaints. While the definition of ''person'' in the HIPAA Rules is broad enough to refer to an office, we are persuaded by public comments that this modification is necessary to clarify that covered entities may designate an office or a workforce member as the contact.[688] This modification is consistent with other instances in the Privacy Rule that refer to ''person or office.'' [689]

According to commenters, individuals generally do not ask questions about the NPP. Based on these comments, we do not expect that covered entities will receive many questions about their privacy practices. Thus, the Department believes that having a designated person or office available to answer questions about the NPP will create less administrative burden than obtaining a written acknowledgment of receipt of the NPP or documenting good faith efforts and the reason for not obtaining the acknowledgment. Furthermore, the final rule provides flexibility by permitting covered entities to choose to designate either a person or office as the contact. The Department has long stated that duties may be delegated and shared, so long as there is one point of accountability for the covered entity's privacy practices to ensure that individuals are able to speak to a knowledgeable person.[690] Thus, although the Department recommends that the designated person or office be versed in the entity's privacy practices and HIPAA complaint process, we are not requiring that the designated contact person or office must meet certain minimum qualifications to answer questions about the NPP or receive HIPAA complaints. Providing a designated contact person or office recognizes the importance of assuring patients that their PHI is being protected and shared appropriately. Additionally, it engenders trust and encourages open dialogue between individuals and covered entities.

Comment: Some commenters expressed support for the proposal to modify the header because it would draw attention to the items of greatest relevance to individuals, thereby improving individuals' understanding of, and ability to exercise, the rights afforded to them by the Privacy Rule. Some commenters expressed opposition to the proposal to modify the header because of an increased administrative burden associated with modifying the NPP.

Response: The Department is adopting the proposal to revise the header because it will make it easier for individuals to quickly see and improve their understanding of the entity's privacy practices in the NPP. We acknowledge that updating the NPP will create a one-time burden for covered entities; however, we believe that eliminating the recurring requirement to obtain and document the written acknowledgment, or the covered entity's good faith effort and reason for not obtaining the acknowledgment, will more than offset this burden.

Comment: A few commenters recommended that the Department update the model NPP to: (1) address how an individual's information may be used and disclosed within the health care system and by business associates; and (2) include examples related to health care operations and psychotherapy notes.

Response: The Department intends to update the model NPPs and model Part 2 Patient Notice, which addresses SUD patient records, to reflect the changes herein prior to the compliance date for this final rule.[691]

Comment: One commenter expressed support for the Department's proposal to make it optional for covered entities to include in the NPP information about how an individual who seeks to direct a copy of their PHI to a designated person can instead obtain a copy of PHI themselves or request that the covered entity send a copy of the PHI to a designated person using a valid authorization if the request does not meet the conditions of 45 CFR 164.524(d) because of the variability of options and fees.

Response: Allowing covered entities to include in the NPP a thorough explanation of individuals' options of obtaining access to and sharing their

[687] *See* 45 CFR 164.520(c)(3)(i).

[688] *See* 45 CFR 164.501 (definition of ''Person'').

[689] *See, e.g.,* 45 CFR 164.520(b)(1)(vii), 45 CFR 164.524(d)(2)(iii) (redesignated by this final rule to 45 CFR 164.524(e)(2)(iii)), 45 CFR 164.526(d)(1)(iv), and 45 CFR 164.530(a)(1)(ii)).

[690] 65 FR 82462, 82744 (Dec. 28, 2000) (discussing that covered entities are organized differently and have different information systems, which is why the Department did not delegate who within a covered entity must be the privacy official).

[691] ''Model Notices of Privacy Practices,'' Office for Civil Rights, U.S. Department of Health and Human Services (Feb. 13, 2026), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html.*

PHI with others informs and empowers individuals to make such decisions in a thoughtful and educated manner. Covered entities that choose to include this information are not required to include in the NPP information about their fees for disclosing such PHI. Elsewhere in this final rule, we discuss the decision to finalize the proposal to require covered entities to make available a fee schedule that applies to requests made pursuant to the right of access and valid authorizations.

Comment: One commenter expressed opposition to the proposal to remove the exception to the requirement to provide individuals with a copy of the NPP for individuals who are inmates of correctional facilities that are covered entities because they believed issuing the NPP to such individuals would mean that they would have the same health information privacy rights as individuals who are not inmates. The commenter also expressed concern about potential safety and security risks associated with sharing information about scheduled appointments or surgeries with an individual who is an inmate or family or friends of an individual who is an inmate.

Response: We are finalizing this provision as proposed in the 2022 Part 2 NPRM. Individuals who are inmates are afforded the same health information privacy rights under the Privacy Rule as other individuals, with limited exceptions. For example, a correctional institution that is a covered entity may limit the disclosure of PHI in response to an inmate's right of access request if such disclosure would jeopardize the health, safety, or security of the individual or other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.[692] And while an inmate's personal representative (which could be a family member or friend) may be able to obtain a copy of PHI on the inmate's behalf in some cases where a covered entity may deny access to the individual, this has been true since the 2000 Privacy Rule.[693] Additionally, while the NPP is provided to each individual, it does not include information about the individual; rather, it addresses the covered entity's privacy practices and individuals' rights and how to exercise them.

H. Permitting Disclosures for Telecommunications Relay Services for People Who Are Deaf, Hard of Hearing, or Deaf-Blind, or Who Have a Speech Disability

1. Current Rule

As we explained in the 2021 Privacy Rule NPRM, TRS providers facilitate telephone calls between individuals who are deaf, hard of hearing, or deaf-blind, or who have a speech disability, and others.[694] Federally regulated common carriers (*e.g.,* operators of all landline and mobile telephone services) must provide TRS to individuals in the general public who are deaf, hard of hearing, or deaf-blind, or who have a speech disability.[695] TRS providers facilitate such communications by using a communications assistant who transliterates conversations (or in some cases, interprets using American Sign Language (ASL)).[696] The communications assistant relays information, which may include PHI, between a person who uses text or video and another person, who may be communicating by voice or who also may be using TRS.[697] All TRS providers must comply with standards for operators established by the Federal Communications Commission pursuant to Title IV of the Americans with Disabilities Act of 1990 (ADA), as amended,[698] including protecting the confidentiality of all relayed communications.[699]

The Privacy Rule currently does not explicitly permit the use and disclosure of PHI for purposes expressly related to TRS, nor does it explicitly address whether a TRS communications assistant is a business associate. However, the Department previously explained in guidance that a covered entity is permitted to disclose an individual's PHI to a TRS communications assistant when communicating with the individual without the need for a business associate agreement with the TRS provider.[700] As explained in the guidance, the Privacy Rule permits disclosures to TRS communications assistants under 45 CFR 164.510(b) because individuals have an opportunity to agree or object to disclosures of PHI to a TRS communications assistant at the beginning of a call, and the individuals are effectively identifying the communications assistant as involved in their care if the individuals do not object. Additionally, the guidance also explains that the TRS provider is not acting for or on behalf of the covered entity when it provides such relay services. Thus, the TRS provider is not a business associate.

Also as explained in the 2021 Privacy Rule NPRM, the Department has become aware that advances in technology now allow people who are deaf, hard of hearing, or deaf-blind, or who have a speech disability to communicate with the help of a TRS communications assistant in a seamless manner, with immediate connection and instantaneous transliteration of text or interpretation of ASL to voice and vice versa, such that the other party to the call may not know that a person is using a TRS communications assistant. Additionally, TRS is used not only to connect individuals with workforce members of regulated entities, but also to assist in communications between workforce members of regulated entities. For these reasons, the assumption that individuals always would have the opportunity to agree or object to a use or disclosure of PHI to a TRS communications assistant no longer holds when it is a workforce member of the regulated entity, rather than an individual, who needs the TRS services to assist with communications.

2. Proposed Rule

The Department proposed to add a new subsection (v) to paragraph (4) of the definition of business associate at 45 CFR 160.103 that would exclude TRS providers from the definition of business associate. This proposal would ensure that regulated entities would not need to analyze whether they need business associate agreements with TRS providers, nor would they need to enter into and implement such agreements.

[692] *See* 45 CFR 164.524(a)(2)(ii).

[693] 45 CFR 164.502(g)(1); *see* 45 CFR 164.502(g)(2)–(5) (exceptions to this general rule); *see also* 65 FR 82462, 82732 (Dec. 28, 2000).

[694] *See* ''Consumer Guide, Telecommunications Relay Service,'' *supra* note 362.

[695] *See* 47 U.S.C. 225(b).

[696] *See* 47 CFR 64.601(a)(12).

[697] *See generally* ''Consumer Guide, Telecommunications Relay Service,'' *supra* note 362. TRS types include Text-to-Voice, Voice Carry Over, Speech-to-Speech Relay, Shared Non-English Language Relay, Captioned Telephone Service, internet Protocol Captioned Telephone Service, internet Protocol Relay Service, and Video Relay Service. *Id.*

[698] Public Law 101–336, 104 Stat. 327 (July 26, 1990) as amended (codified at 47 U.S.C. 225); 47 CFR 64.604(c)(5)(iii)(K).

[699] Except in very limited circumstances specified in FCC regulations, TRS communications assistants are not permitted to keep notes of the contents of a call after a call, unless the caller requests that the communications assistant retain such information to facilitate the completion of subsequent calls. In no case may the communications assistant retain such information after the completion of the subsequent call(s). *See* 47 CFR 64.604(a)(2).

[700] ''When a covered entity, such as a doctor, uses a certified Telecommunications Relay Service to contact patients with hearing or speech impairments, is the Relay Service a business associate of the doctor?,'' *supra* note 364.

The Department also proposed to add a new paragraph (m) to 45 CFR 164.512 that would expressly permit covered entities to disclose PHI to TRS communications assistants, as defined at 47 CFR 64.601(a)(12).[701] This proposed permission would cover all disclosures to TRS communications assistants related to any covered functions performed by, for, or on behalf of covered entities.

Together, the proposed modifications to 45 CFR 160.103 and 164.512 would help to ensure that workforce members and individuals who are deaf, hard of hearing, deaf-blind, or who have a speech disability are able to communicate easily using TRS for care coordination and other purposes.

3. Overview of Comments

The Department received relatively few comments on this proposal. Commenters generally expressed support for the proposal because they asserted that it would facilitate care coordination for individuals who are deaf, hard of hearing, deaf-blind, or who have a speech disability, as well as enable regulated entities and their workforce members, who may be deaf, hard of hearing, deaf-blind, or have a speech disability, to communicate with individuals and each other using TRS.

4. Final Rule

Consistent with the Department's proposal, this final rule modifies the definition of business associate at 45 CFR 160.103 by adding a new subsection (v) to paragraph (4) to expressly exclude TRS providers from the definition of business associate. Additionally, it permits regulated entities to disclose PHI to TRS communications assistants to conduct covered functions by adding a new paragraph (m) to 45 CFR 164.512. Section 164.512(m)(1) permits covered entities to disclose PHI to TRS communications assistants to conduct covered functions, while 45 CFR 164.512(m)(2) expressly permits business associates to disclose PHI to TRS communications assistants to conduct covered functions for, or on behalf of, a covered entity. The language that we are adopting is modified from the proposed language for 45 CFR 164.512(m) to clarify in regulatory text that business associates can make such disclosures regardless of whether their business associate agreements address the ability of the business associates to disclose PHI to TRS communications assistants for the purposes described above. This modification is consistent with the intended scope of the Department's proposal, as described in preamble to the 2021 Privacy Rule,[702] and helps further our goals of reducing administrative burden on regulated entities and facilitating communications for persons who rely on TRS communications assistants.

As of 2024, hearing loss was the third most common chronic physical condition in the United States,[703] affecting more than 37.9 million Americans [704] and projected to rise to over 70 million by 2060.[705] Further, hearing loss that is disabling is experienced by 5 percent of adults aged 45 to 54, 10 percent of those aged 55–64, 22 percent of those aged 65 to 74, and 55 percent of adults over the age of 75.[706] Moreover, in this same time period, over 17 million adults experienced difficulties using their voice in the 12 months preceding this time period while over 9 million adults experienced the problem for a period of 1 week or longer.[707] With respect to vision loss, according to estimates from the 2024 National Health Interview Survey, 49.5 million American Adults age 18 and older reported experiencing some degree of vision loss. Of these, 3.8 million adults have a lot of trouble seeing, even when wearing glasses, and 420,000 cannot see at all.[708] Thus, the need for TRS communications assistants to aid such individuals in communicating with regulated entities, and workforce members of regulated entities in communicating with each other and outside parties, is likely to increase in the near future.

Accordingly, the Department believes that this modification to the Privacy Rule promotes access to health care for individuals who are deaf, hard of hearing, deaf-blind, or who have a speech disability and will facilitate the compliance of regulated entities with applicable Federal and state disability laws. Additionally, we believe that clarifying that regulated entities are permitted to disclose PHI to TRS communications assistants to conduct covered functions eliminates confusion and enables persons who are deaf, hard of hearing, deaf-blind, or who have a speech disability to be employed in the health care industry without imposing on regulated entities the need for a business associate agreement, while presenting no real risk to the privacy and confidentiality of PHI.

5. Responses to Public Comments

Comment: Commenters almost universally expressed support for the proposal to exclude TRS providers from the definition of a ''business associate'' and clarify that regulated entities are not required to enter into business associate agreements with TRS providers in order to disclose PHI to them. According to commenters, this proposal would eliminate the administrative burden associated with implementing a business associate agreement, enabling regulated entities to more easily make necessary disclosures to TRS communications assistants for patient care. Many commenters asserted that it would reduce burden for patients who are deaf, hard of hearing, deaf-blind, or who have a speech disability. These commenters expressed uncertainty about whether regulated entities must enter into business associate agreements with TRS providers, which has caused some regulated entities to be reluctant to communicate via TRS or to require business associate agreements from TRS providers. According to commenters, this uncertainty has resulted in delays to the timely provision of health care for affected individuals. Commenters asserted that this proposal would alleviate concerns about potential violations of the ADA [709] and the burdens imposed on affected individuals in circumstances where

[701] The proposed regulatory text in the 2021 Privacy Rule NPRM incorrectly stated that the definition of ''communications assistant'' was at 47 CFR 64.601(a)(10).

[702] 86 FR 6446, 6487 (Jan. 21, 2021).

[703] *See* ''About Occupational Hearing Loss,'' National Institute for Occupational Safety and Health, U.S. Centers for Disease Control and Prevention (May 15, 2024), *https://www.cdc.gov/niosh/noise/about/index.html.*

[704] David B. Rein, et al., ''The prevalence of bilateral hearing loss in the United States in 2019: a small area estimation modelling approach for obtaining national, state, and county level estimates by demographic subgroup,'' The Lancet Regional Health—Americas, p. 5 (Feb. 2024), *https://www.thelancet.com/action/showPdf?pii=S2667-193X%2823%2900244-2.*

[705] *See* Adele M. Goman, et al., ''Addressing Estimated Hearing Loss in Adults in 2060,'' JAMA Otolaryngology Head & Neck Surgery (July 2017), *https://jamanetwork.com/journals/jamaotolaryngology/fullarticle/2606784.*

[706] ''Quick Statistics about Hearing, Balance, & Dizziness,'' National Institute on Deafness and other Communication Disorders, U.S. Department of Health and Human Services (Sept. 20, 2024), *https://www.nidcd.nih.gov/health/statistics/quick-statistics-hearing.*

[707] *See id.;* ''Quick Statistics About Voice, Speech, and Language,'' National Institute on Deafness and other Communication Disorders, U.S. Department of Health and Human Services (July 8, 2025), *https://www.nidcd.nih.gov/health/statistics/quick-statistics-voice-speech-language.*

[708] ''Facts and Figures on Adults with Vision Loss from the National Health Interview Survey (NHIS),'' American Foundation for the Blind (Mar. 2026), *https://www.afb.org/research-and-initiatives/statistics/adults-vision-loss-nhis.*

[709] Public Law 101–336, 104 Stat. 327 (July 26, 1990) (codified as amended at 42 U.S.C. 12101 *et seq.*). The ADA prohibits discrimination based on disability.

covered entities did not implement accessible telephone systems.

One commenter opined that the proposal would not result in any adverse consequences, such as posing significant risks to individuals' privacy or undue burdens on regulated entities.

Response: The Department agrees that this modification reduces barriers to both health care for individuals who are deaf, hard of hearing, deaf-blind, or who have a speech disability, and employment for such persons. The Department also agrees that eliminating the need to implement a business associate agreement with TRS providers will reduce the administrative burden on regulated entities, namely the amount of time and other resources associated with determining whether a business associate agreement is necessary and implementing such business associate agreements. Additionally, we are unaware of any potential unintended, adverse consequences that would be created by this proposal.

Accordingly, we are finalizing these modifications.

Comment: One commenter recommended that the Department modify the proposal to permit covered entities to disclose PHI to TRS communications assistants to the same extent as during a traditional voice call. The commenter expressed concern that regulated entities otherwise might conclude that the minimum necessary standard applies to the disclosure of PHI when using a TRS communications assistant.

Response: The Department declines to modify the proposal as requested because the recommended language could cause uncertainty about the scope of the permission. This final rule permits a regulated entity to disclose PHI when necessary to conduct a function covered by the HIPAA Administrative Simplification provisions but does not permit it to disclose PHI beyond such functions. Further, the Department believes that the finalized text vests discretion with the disclosing regulated entity to ensure that the amount of PHI disclosed is consistent with the purpose for which it is disclosed. The minimum necessary standard at 45 CFR 164.502(b) will continue to be applicable consistent with its requirements.

I. Expanding the Permission To Use and Disclose the PHI of Armed Forces Personnel To Cover All Uniformed Services Personnel

1. Current Rule

Section 164.512(k) of the Privacy Rule contains the standard for uses and disclosures of PHI for specialized government functions, including U.S. military and veteran activities. Paragraph (k)(1)(i) of this section specifically permits covered entities to use and disclose the PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. Application of the permission requires the military authority to publish notice in the **Federal Register** of the appropriate military command authorities and the purposes for which the PHI may be used or disclosed.[710] Section 164.512(k)(1)(ii) permits a component of the Departments of Defense or Homeland Security that is a covered entity to disclose to the VA the PHI of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a VA determination of eligibility or benefits entitlement. These permissions enable covered entities to use and disclose the PHI of Armed Services personnel, under certain conditions, to avoid the burden and obstacles of obtaining individuals' authorizations when the balance of privacy interests and societal values weighs toward permitting the use or disclosure of PHI without authorization for specialized purposes.[711] When taken together, they ensure that the PHI of members of the Armed Forces is made available for operations that tie directly to military and VA operations.

2. Proposed Rule

As we explained in the 2021 Privacy Rule NPRM, according to the Directors of the USPHS and NOAA Commissioned Corps, the existing provision limits the ability of the USPHS and NOAA Commissioned Corps to facilitate care coordination and case management for Commissioned Corps personnel.[712] Such care coordination and case management are important for ensuring that personnel meet medical readiness standards and are able to fulfill the Commissioned Corps' respective missions. Accordingly, the Department proposed to expand the applicability of 45 CFR 164.512(k)(1) from the Armed Forces to all Uniformed Services, which—in addition to the Armed Forces—includes HHS's USPHS Commissioned Corps and the Department of Commerce's NOAA Commissioned Corps. This would permit covered entities to use and disclose PHI for mission requirements and veteran eligibility of members of these Services without individual authorization. The Department proposed to modify 45 CFR 164.512(k)(1)(i) to permit covered entities to use and disclose the PHI of individuals who are members of the USPHS or NOAA Commissioned Corps for activities deemed necessary by appropriate Service authorities to assure the proper execution of the missions of the respective Commissioned Corps. The Department also proposed to modify 45 CFR 164.512(k)(1)(ii) to permit a component of either the Department of Commerce or HHS that is a covered entity to disclose PHI to the VA concerning members of their respective Commissioned Corps in the same manner that is currently allowed for the Departments of Defense and Homeland Security with respect to the Armed Forces under their respective jurisdictions.

3. Overview of Comments

The Department received relatively few comments on this proposal, but the comments that we received generally expressed support for it.

4. Final Rule

The final rule adopts the proposal to expand the permission for covered entities to use and disclose PHI of members of the Armed Services to include members of all Uniformed Services, with minor modifications to account for the organizational structure of the Department of Defense.[713] Additionally, because Uniformed Services includes the USPHS and NOAA Commissioned Corps, the final rule adopts the modification to permit a covered component of either the Department of Commerce or Health and Human Services to disclose PHI to the VA at 45 CFR 164.512(k)(1)(ii).

The Uniformed Services are composed of the Armed Forces (Army, Navy, Air Force, Marine Corps, Space Force, Coast Guard) plus the USPHS and NOAA Commissioned Corps. While members of the USPHS and NOAA

[710] *See* 45 CFR 164.512(k)(1)(i).

[711] *See* 65 FR 82462, 82704–05, 82817 (Dec. 28, 2000).

[712] *See* 86 FR 6446, 6487 (Jan. 21, 2021).

[713] The Department of Defense may also be referred to as the Department of War. *See* 90 FR 43893 (Sept. 10, 2025).

Commissioned Corps are not members of the Armed Forces, they maintain similar obligations to those of the Armed Services. For example, for the USPHS, 42 U.S.C. 204(a) establishes both a Regular Corps and Ready Reserve Corps to be available for deployment in certain specified circumstances. Paragraph (1) of 42 U.S.C. 402(a) requires the Secretary to establish requirements to ensure the readiness of both Corps' components for response to urgent or emergency public health care needs that cannot otherwise be met at the Federal, state, and local levels; and any member who fails to maintain fitness is subject to disciplinary actions. Under 42 U.S.C. 217, the President may, by Executive Order, in time of war, or of emergency involving the national defense, declare the USPHS Commissioned Corps to be a military service. Similarly, section 3007 of title 33 of the U.S. Code requires the Secretary of the Department of Commerce to ensure a ''high physical state of readiness'' by establishing physical fitness standards for NOAA personnel that are substantially equivalent to those prescribed for Coast Guard personnel. Section 3030 of 33 U.S.C. provides that officers of NOAA shall be subject to the same laws as Navy personnel for purposes of temporary appointment or advancement in time of war or national emergency. Section 3061 of 33 U.S.C. provides that the President may, whenever in the judgment of the President a sufficient national emergency exists, transfer NOAA commissioned officers, ships, and stations to the military departments if the President deems it in the best interest of the country.

Members of the USPHS and NOAA Commissioned Corps are obligated to maintain physical fitness to ensure duty readiness in a similar manner to members of the Armed Forces. Members of these Commissioned Corps also enjoy certain benefits linked to their service.[714] As explained by the directors of the USPHS and NOAA Commissioned Corps in their joint comments, the Commissioned Corps are part of the eight Uniformed Services and may be assigned or detailed to the Armed Services. As such, according to the directors, members of the USPHS and NOAA Commissioned Corps ''must meet medical readiness standards consistent with the various military missions.'' [715] Thus, it is appropriate to permit the use and disclosure of PHI, without authorization, of members of the USPHS Commissioned Corps and the NOAA Commissioned Corps for the same purposes, and in a similar manner as the Privacy Rule currently permits with respect to the PHI of members of the Armed Forces.

Additionally, based on public comments, the Department believes that expanding the Armed Forces permission is likely to facilitate efficient care coordination and case management for members of the USPHS and NOAA Commissioned Corps, and thus help the respective Commissioned Corps ensure the health and safety of their officers. As explained by the Directors of the USPHS and NOAA Commissioned Corps, the health and safety of officers is crucial for ensuring that such officers can fulfill the mission of the Corps and protect the health and safety of the nation's population. Accordingly, we are finalizing the proposal with minor modifications to account for the organizational structure of the Department of Defense. The final regulatory text in paragraphs (k)(1), (k)(1)(i), (k)(1)(i)(A), and (k)(1)(ii) hews closely to the original regulatory text but substitutes the term ''Uniformed Services'' for the terms ''military'' and ''Armed Forces'' in certain instances and in others, substitutes ''command'' for ''military'' or ''military command.'' These modifications clarify that ''Uniformed Services'' refers to the personnel whose PHI may be used or disclosed under this permission, not to the departments, agencies, or components that oversee those personnel. The appropriate command authorities for purposes of 45 CFR 164.524(k)(1)(i) are those identified in the **Federal Register** notice required by that provision. Thus, this modification enshrines an explicit permission for covered entities to use and disclose the PHI of members of all Uniformed Services for the purposes specified in this provision. The final regulatory text is also consistent with the regulatory text suggested by USPHS and NOAA in their joint comments on the 2018 RFI, as explained in the 2021 Privacy Rule NPRM. The final rule does not modify the scope of the permission, nor does it change the requirement at 45 CFR 164.512(k)(1)(i) that the appropriate authority publish a notice in the **Federal Register** identifying the appropriate command authorities and the purposes for which PHI may be used or disclosed.

5. Responses to Public Comments

Comment: One commenter who expressed support for the proposal suggested that the Department define ''Uniformed Services.''

Response: At this time, the Department declines to define the term ''Uniformed Services.'' Instead, we look to 37 U.S.C. 101, which provides that the Uniformed Services consists of the six branches of the military plus the USPHS and NOAA Commissioned Corps. For purposes of 45 CFR 164.512(k)(1), Uniformed Services refers to the members whose PHI may be used or disclosed under this permission and does not refer to the departments, agencies, or components that oversee those members.

Comment: One commenter who expressed support for this proposal asserted that it would reduce barriers to care and enable the exchange of PHI for care coordination and case management for individuals whose PHI is subject to the permission, particularly when they seek care from military and non-military health care providers. Another commenter who expressed support for the proposal stated that it would reduce impediments to universal data exchange.

Response: The Department agrees that permitting covered entities to use and disclose the PHI of individuals who are Uniformed Services personnel for activities deemed necessary by the appropriate command authorities to assure the proper execution of the Uniformed Services mission will support the exchange of PHI for care coordination and case management. Accordingly, we are finalizing this proposal.

Comment: One commenter requested clarification on whether the proposed expansion of the permission to all Uniformed Services would include Armed Services recruitment activities. Another commenter expressed concern about the use or disclosure of genetic information for decision making related to an individual's ability to execute military missions.

Response: Consistent with the prior language at 45 CFR 164.512(k), this final rule continues to defer to appropriate command authorities to determine which uses and disclosures of PHI are deemed necessary to assure the proper execution of the mission. This final rule only expands the permission for use and disclosures of the PHI of members of the Armed Services to also include members of the USPHS and NOAA

[714] *See* 42 U.S.C. 213 and 33 U.S.C. 3071 (extending certain privileges granted to members of the Armed Forces to members of the USPHS and NOAA Commissioned Corps).

[715] Letter from Rear Admiral Joan Hunter, PHS Corps Director, Commissioned Corps Headquarters and Rear Admiral Michael J. Silah, NOAA Director, NOAA Corps to the Office for Civil Rights, U.S. Department of Health and Human Services (Feb. 11, 2019) (citing 42 U.S.C. 204a(a)(1), 33 U.S.C. 3073), *https://www.regulations.gov/comment/HHS-OCR-2018-0028-0965.*

Commissioned Corps, referred to collectively as ''Uniformed Services.''

J. Providing a Transition Period for Business Associate Agreements

1. Current Rule

The transition provisions for business associate contracts and other written arrangements (collectively, ''business associate agreements'') are found in 45 CFR 164.532(e). The Department's most recent revisions to this provision, made in 2013, allowed regulated entities to continue operating under existing business associate agreements for up to 1 year beyond the compliance date of the 2013 modifications to the HIPAA Rules.[716]

2. Proposed Rule

The Department did not specifically propose to modify the transition provisions at 45 CFR 164.532(e) as part of the 2021 Privacy Rule NPRM. However, as discussed above, we did solicit comments on the sufficiency of an 180-day compliance period.

3. Overview of Comments

While the Department did not specifically propose to provide regulated entities with additional time to modify business associate agreements, several commenters urged the Department to provide additional time for them to do so, citing the administrative burden and costs of implementing the revised business associate agreement provisions.

4. Final Rule

The Department recognizes that regulated entities may have existing business associate agreements that are not set to terminate or expire until after the compliance date, and we understand that a 6-month compliance period may not provide enough time to reopen and renegotiate all business associate agreements. Accordingly, we are modifying 45 CFR 164.532(e) to allow regulated entities to continue to operate under certain existing business associate agreements for up to 1 year beyond the effective date (*i.e.,* 6 months beyond the compliance date) for the revisions to the Privacy Rule made by this final rule.

The Department's authority to provide additional time for regulated entities to comply with certain provisions of the Privacy Rule is set forth in 45 CFR 160.104(c), which permits the Secretary to establish the compliance date for any modified standard or implementation specification, considering the extent of the modification and the time needed to comply with the modification. We provided a similar transition period for revising business agreements in the 2002 Privacy Rule[717] and 2013 Omnibus Rule[718] for similar reasons.

Specifically, the final rule modifies the transition provisions at 45 CFR 164.532(e) to allow regulated entities to continue to operate under certain existing business associate agreements for up to 1 year beyond the effective date of this final rule. The additional transition period is available to a regulated entity if, prior to the publication date of this final rule, the regulated entity has an existing contract or other written arrangement with a business associate or subcontractor that complies with the HIPAA Rules, and such contract or arrangement is not renewed or modified between the effective date and the compliance date of this final rule. These transition provisions allow regulated entities that have valid business associate agreements with business associates and subcontractors to continue to disclose PHI to the business associate or subcontractor, or to allow the business associate or subcontractor to continue to create, receive, maintain, or transmit PHI on behalf of the regulated entity, for up to 1 year beyond the effective date of this final rule, regardless of whether the business associate agreement meets the applicable requirements of this final rule. The Department will deem such business associate agreements compliant with the modifications to the Privacy Rule until the earlier of: (1) the regulated entity either renews or modifies the business associate agreement following the compliance date of this final rule; or (2) the date that is 1 year after the effective date.

Business associate agreements that renew automatically without any change in terms or other action by the parties (also known as ''evergreen contracts'') are eligible for the extension, and they will continue to be deemed compliant with the final rule, as described above, when they automatically roll over. These transition provisions apply only to written contracts or other written arrangements, and not to verbal contracts or other arrangements.

These transition provisions apply only to the requirement to amend business associate agreements; they do not affect any other compliance obligations under the HIPAA Rules. For example, beginning on the compliance date of this rule, a business associate that responds to requests for individual access on behalf of a covered entity must respond to such requests as soon as practicable, but not later than 15 calendar days after receiving a request, even if the business associate agreement has not yet been amended to reflect the modifications to the Privacy Rule.

5. Responses to Public Comments

Comment: A few commenters requested that the Department provide additional time for regulated entities to revise business associate agreements affected by the revised Privacy Rule.

Response: We agree with commenters that regulated entities may require additional time to update and renegotiate their business associate agreements. The Department is aware that many regulated entities have existing business associate agreements that do not terminate or expire until after the compliance date, and that a 240-day compliance period may be insufficient for regulated entities with many business associate agreements to come into compliance, while also implementing the other modifications finalized in this rule. To reduce this administrative burden, we are revising 45 CFR 164.532(e) to provide regulated entities with a 1-year transition period during which certain existing business associate agreements may remain in effect beyond the compliance date of this final rule.

K. Other Technical and Conforming Changes

In addition to the substantive modifications described above, this final rule implements several technical or conforming changes that are non-substantive in nature.

To improve readability and clarity, this final rule replaces semicolons with periods at the end of paragraphs in: (1) the definition of ''health care operations''; (2) 45 CFR 164.502(a)(2); (3) 45 CFR 164.524(a)(1); (4) 45 CFR 164.524(a)(3); and (5) 45 CFR 164.524(d)(3). Additionally, clarifying phrases were added before the colon: (1) in paragraph (6) of the definition of health care operations, the phrase ''any of the following''; (2) 45 CFR 164.502(a)(2) adds the phrase ''in each of the following circumstances''; and (3) Section 164.524(a)(1) adds the phrase ''either of the following.'' Section 164.524(a)(2) adds ''any of'' before ''the following circumstances'' and changes the period to a colon after ''circumstances.'' Section 164.524(a)(3) adds ''any of'' before ''the following circumstances.'' Section 164.524(d)(3) adds ''either of'' before ''the following circumstances.'' Additionally, 45 CFR 164.524(c)(2)(iv) adds a comma before ''or may.'' These technical changes do

[716] *See* 78 FR 5566, 5602–03 (Jan. 25, 2013).

[717] 67 FR 53182, 53247–51 (Aug. 14, 2002).

[718] 78 FR 5566, 5602–03 (Jan. 25, 2013).

not modify the substance of the relevant provisions.

Section 164.512(d)(3) contains a minor spelling error. This final rule replaces ''Nothwithstanding'' with ''Notwithstanding.''

Section 164.512(k)(1)(ii) currently uses the acronym ''DVA'' for the U.S. Department of Veterans Affairs. This final rule replaces the acronym ''DVA'' with ''VA,'' consistent with the U.S. Department of Veterans Affairs' use of VA.[719]

Additionally, we are finalizing a technical correction for the citation to the National Security Act of 1947 in 45 CFR 164.512(k)(2). Periodically, the Office of the Law Revision Counsel, which maintains and publishes the United States Code (U.S.C.) (a codification of the general and permanent laws of the United States organized into titles based on subject matter) may recodify statutes in the U.S.C. In 2013, the codified version of the National Security Act in chapter 15 of title 50 was recodified in the U.S.C.[720] In accordance with the current citation, this final rule modifies 45 CFR 164.512(k)(2) to change the citation for the National Security Act from 50 U.S.C. 401, *et seq.* to 50 U.S.C. 3001, *et seq.*

For consistency and clarity, in the NPP provisions we are modifying ''sponsor of the plan'' to ''plan sponsor'' at 45 CFR 164.520(b)(1)(iii)(B).[721]

Finally, we use the terms ''the'' and ''an'' before the term ''individual'' throughout 45 CFR 164.524. Generally, we use the term ''an'' at the beginning of a provision, while ''the'' refers back to the original individual referenced in the provision. This final rule makes such changes for clarity to change the term ''the'' to ''an'' before the term ''individual'' in 45 CFR 164.524(c)(1), 164.524(c)(2)(i), 164.524(c)(2)(iv)(A), 164.524(c)(3), 164.524(c)(4), and 164.524(e). In 45 CFR 164.524(c)(1) we changed the term ''them'' to ''an individual.''

V. Regulatory Impact Analysis

The Department has examined the impact of the final rule as required by Executive Order (E.O.) 12866 on Regulatory Planning and Review,[722] E.O. 13563 on Improving Regulation and Regulatory Review,[723] E.O. 13132 on Federalism,[724] E.O. 13175 on Consultation and Coordination with Indian Tribal Governments,[725] E.O. 14192 on Unleashing Prosperity Through Deregulation,[726] the Congressional Review Act (CRA),[727] the Unfunded Mandates Reform Act of 1995 (UMRA),[728] the Regulatory Flexibility Act (RFA),[729] E.O. 13272 on Proper Consideration of Small Entities in Agency Rulemaking,[730] the Assessment of Federal Regulation and Policies on Families,[731] and the Paperwork Reduction Act of 1995 (PRA).[732]

A. E.O. 12866 and E.O. 13563 and Related Executive Orders on Regulatory Review

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits.

This final rule is deregulatory. The Department has estimated that the effects of the requirements for covered entities[733] will result in new costs of $783.98 million within 12 months of implementing the final rule, in 2025 dollars. The Department estimates that these first-year costs will be offset by recurring cost savings of $798.13 million, followed by net savings of $702.75 million annually in years two through five, resulting in overall undiscounted net cost savings of $2,825.15 million over 5 years. The Department estimates that this final rule will generate $0.54 billion in net annualized savings at a 7 percent discount rate over a perpetual time horizon, in 2025 dollars.

The Department estimates that the private sector will bear approximately 60 percent of the costs, with state and Federal health plans bearing the remaining 40 percent of the costs. All of the cost savings experienced from the first year through subsequent years will benefit covered entities. Because of the economic effects, this rule is an economically significant regulatory action within the meaning of section 3(f)(1) of E.O. 12866. Accordingly, the Office of Management and Budget (OMB) has reviewed this rule. Because the rule has an annual effect on the economy of $100,000,000 or more, it is also a major rule, as defined by the CRA.[734] The Department presents a detailed analysis below.

1. Summary of Costs and Benefits

The Department estimates that the regulatory changes described in the preamble will result in quantified costs of approximately $1 billion and numerous and substantial deregulatory benefits in the form of quantified cost savings of approximately $4 billion. Additionally, the Department believes the modifications in this final rule will result in numerous unquantified benefits, including all of the following:

- Improved health outcomes because of better care coordination and case management.
- Greater understanding by individuals of their rights and the privacy practices of covered entities.
- Enhanced access to care.
- Quicker, more convenient access to protected health information (PHI) by individuals.
- Fewer disputes about access fees because of increased transparency about such fees.
- Expanded adoption and utilization of certified health information technology (health IT).
- Improved employment conditions and opportunities for workforce members of covered entities and business associates[735] who are deaf, hard of hearing, or deaf-blind, or who have a speech disability.
- Streamlined compliance with non-discrimination laws that require accessibility for individuals with disabilities.

The Department has identified four general categories of quantified costs arising from these regulatory changes, which generally relate to activities by covered entities, particularly health care providers and health plans:

- Administrative activities (non-recurring and recurring).
- Revising or creating policies and procedures, the Notice of Privacy Practices (NPP), and an access fee schedule.

[719] ''July 21, 1930: Creation of the Veterans Administration,'' U.S. Department of Veterans Affairs (Nov. 12, 2021), *https://department.va.gov/history/featured-stories/va-created/.*

[720] ''Editorial Reclassification Title 50, United States Code,'' Office of the Law Revision Counsel, U.S. House of Representatives (last accessed Mar. 2, 2026), *https://uscode.house.gov/editorial reclassification/t50/index.html.*

[721] *See* Public Law 93–406, 88 stat. 835 (Sept. 2, 1974) (codified at 29 U.S.C. 1002) (definition of ''plan sponsor'' in Employee Retirement Income Security Act of 1974).

[722] 58 FR 51735 (Oct. 4, 1993).

[723] 76 FR 3821 (Jan. 21, 2011).

[724] 64 FR 43255 (Aug. 10, 1999).

[725] 65 FR 67249 (Nov. 9, 2000).

[726] 90 FR 9065 (Feb. 6, 2025).

[727] Sec. 251 of Public Law 104–121, 110 Stat. 868 (Mar. 29, 1996) (codified at 5 U.S.C. 801–808).

[728] Public Law 104–4, 109 Stat. 48 (Mar. 22, 1995) (codified at 2 U.S.C. 1531–1538).

[729] Public Law 96–354, 94 Stat. 1164 (Sep. 19, 1980) (codified at 5 U.S.C. 601–612).

[730] 67 FR 53461 (Aug. 16, 2002).

[731] Sec. 654 of Public Law 105–277, 112 Stat. 2681–528 (Oct. 21, 1998) (codified at 5 U.S.C. 601 note).

[732] Public Law 104–13, 109 Stat. 163 (May 22, 1995).

[733] 45 CFR 160.103 (definition of ''Covered entity'').

[734] *See* 5 U.S.C. 804(2).

[735] *See* 45 CFR 160.103 (definition of ''Business associate'').

- Modifying training programs for workforce members.
- Non-recurring and recurring costs to provide individuals with a copy of the NPP, including individuals who are inmates.[736]

TABLE 1—ESTIMATED 5-YEAR COSTS AND COST-SAVINGS, UNDISCOUNTED, IN MILLIONS

	Amount
Costs	
Revise Training	$148.02
Revise Policies and Procedures, NPP, and Fee Schedule	$483.38
Administrative Activities	$502.41
Distribute NPP	$31.67
Total Costs	**$1,165.48**
Cost Savings	
Eliminate NPP Acknowledgment	$3,990.63
Total Cost Savings	**$3,990.63**
Net Total (negative = savings)	**-$2,825.15**

Table 2 reports quantified costs and benefits over 5 years.

TABLE 2—ACCOUNTING TABLE OF ESTIMATED BENEFITS AND COSTS OF ALL CHANGES, IN MILLIONS (2025 DOLLARS)

Costs	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Total**
Undiscounted	$783.98	$95.37	$95.37	$95.37	$95.37	**$1,165.48**
3% Discount	$761.15	$89.90	$87.28	$84.74	$82.27	**$1,105.34**
7% Discount	$732.69	$83.30	$77.85	$72.76	$68.00	**$1,034.61**
Cost Savings	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Total**
Undiscounted	$798.13	$798.13	$798.13	$798.13	$798.13	**$3,990.63**
3% Discount	$774.88	$752.31	$730.40	$709.12	$688.47	**$3,655.18**
7% Discount	$745.91	$697.11	$651.51	$608.89	$569.05	**$3,272.47**
Net (undiscounted)						**Savings $2,825.15**

Table 3 reports the present value and annualized estimates of costs, cost savings, and net cost savings of this final rule covering a 5-year time horizon. Using a 7 percent discount rate, the Department estimates that this final rule will result in annualized costs of $252.33 million, annualized cost savings of $798.13 million, and annualized net cost savings of $545.79 million. Using a 3 percent discount rate, the Department estimates this final rule will result in annualized costs of $241.36 million, annualized cost savings of $798.13 million, and annualized net cost savings of $556.77 million.

BILLING CODE 4153–01–P

[736] 45 CFR 164.501 (definition of ''Inmate'').

TABLE 3—ACCOUNTING TABLE (2025 $ MILLIONS) FOR 5-YEAR PERIOD 2026-2030

Category	Primary estimate	Discount rate (%)
Costs, present value	$1,165.48	Undiscounted
Costs, present value	1,034.61	7
Costs, present value	1,105.34	3
Annualized Costs	233.10	Undiscounted
Annualized Costs	252.33	7
Annualized Costs	241.36	3
Cost Savings, present value	3,990.63	Undiscounted
Cost Savings, present value	3,272.47	7
Cost Savings, present value	3,655.18	3
Annualized Cost Savings	798.13	Undiscounted
Annualized Cost Savings	798.13	7
Annualized Cost Savings	798.13	3
Net Cost Savings, present value	2,825.15	Undiscounted
Net Cost Savings, present value	2,237.86	7
Net Cost Savings, present value	2,549.85	3
Annualized Net Cost Savings	565.03	Undiscounted
Annualized Net Cost Savings	545.79	7
Annualized Net Cost Savings	556.77	3
Transfers to Individuals, present value	7.35	Undiscounted
Transfers to Individuals, present value	6.03	7
Transfers to Individuals, present value	6.74	3
Annualized Transfers to Individuals	1.47	Undiscounted
Annualized Transfers to Individuals	1.47	7
Annualized Transfers to Individuals	1.47	3

The regulatory changes likely will result in important benefits that the Department is unable to fully quantify at this time. The resulting benefits are summarized in Table 4.

TABLE 4—NON-QUANTIFIED COSTS/BENEFITS FOR COVERED ENTITIES AND INDIVIDUALS

Regulatory Changes	Costs	Benefits
Modifying definition of health care operations and clarifying disclosures permitted to social services agencies for certain purposes	Potential increase in requests for disclosures for certain care coordination and case management purposes	Improved health outcomes because of better care coordination and case management
Modifying requirements for identity verification		Improved access for individuals to their PHI
Adding permission to disclose PHI to Telecommunications Relay Services (TRS) and excluding TRS providers from the definition of business associate		Improved employment conditions and opportunities for workforce members who are deaf, hard of hearing, or deaf-blind, or who have a speech disability; compliance with non-discrimination laws
Adding right for individuals to discuss covered entity's privacy practices, eliminating requirement to acknowledge receipt of NPP, modifying NPP content requirements, and requiring provision of NPP to incarcerated individuals		Greater understanding of individuals' rights and covered entities' privacy practices; enhanced trust in the health care system
Strengthening right of access (free access using an internet-based method, decreased wait times for access, and information about access fees)		Improved access to PHI for individuals—receiving PHI more quickly; fewer disputes about access fees; increased certainty about allowable fees; expanded ability to use health IT
Restricting the right of access to direct a covered entity to transmit PHI in an electronic health record to a person designated by the individual ("right of access to direct")	Increased burden on individuals to submit two forms—an access request and an authorization—when seeking to send a complete designated record set (electronic and non-electronic) to a person they designate	Improved clarity and certainty for covered entities about the scope of the right of access to direct

BILLING CODE 4153–01–C

In addition to quantified costs and cost savings, the Department estimates that there is likely a monetary transfer attributable to this final rule. The Department estimates that the adjustments to costs that can be charged to individuals for copies of PHI in an electronic health record on electronic media will result in an estimated annual monetary transfer from covered entities to individuals of $1.47 million.

2. Baseline Conditions

The cost-benefit analysis in this final rule adopts in part the cost-benefit analysis in the 2021 Proposed Modifications to the [Health Insurance Portability and Accountability Act of 1996 (HIPAA)] Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement notice of proposed rulemaking (NPRM) (''2021

Privacy Rule NPRM'').[737] The Department has modified and updated its cost-benefit analysis for the following reasons:

- To account for the smaller subset of 2021 proposed changes that we are finalizing.
- To incorporate certain proposals to modify the Privacy Rule included in the 2022 NPRM to modify 42 CFR part 2 (''2022 Part 2 NPRM'').[738]
- To incorporate updated wage and industry data.

The Regulatory Impact Analysis (RIA) explains and describes changes from the analysis in the 2021 Privacy Rule NPRM below.

a. Analytic Assumptions

The Department relies on Bureau of Labor Statistics (BLS) 2025 wage data.[739] See Table 5. All calculations that use mean hourly wages include benefits and overhead by multiplying the mean hourly pay for an occupation by two.

TABLE 5—OCCUPATIONAL PAY RATES

Occupational code and title[a]	Benefit loaded hourly labor wage[b]
23-1011 Lawyers	$178.70
13-1151 Training and Development Specialists	72.64
29-2072 Medical Records Specialists	54.60
29-1141 Registered Nurses	97.52
15-1254 Web Developers	94.98
43-9061 Office Clerks, General	44.64
11-9111 Medical and Health Services Managers	135.54
29-0000 Healthcare Practitioners and Technical Occupations	104.52

[a] To update wage data from the 2021 Privacy Rule NPRM to 2025 data, the Department implements the following changes because of revisions to the BLS occupational categories: 1) Replaces "29-2098 Medical Dosimetrists, Medical Records Specialists, and Health Technologists and Technicians, All Other" with "29-2072 Medical Records Specialists;" 2) Replaces "15-1134 Web Developer and Digital Interface Designer" with "15-1254 Web Developers;" and 3) Replaces "43-4171 Receptionists and Information Clerks" with "43-9061 Office Clerks, General."

[b] To incorporate employee benefits, these figures represent a doubling of the BLS mean hourly wage.

b. Covered Entities

This final rule applies to covered entities.[740] The Department uses the most recent Census data (year 2022) and industry data about pharmacy establishments, and the same methodology adopted in the 2021 Privacy Rule NPRM, to calculate that there are 847,506 covered entities' business establishments. See Table 6.[741]

[737] 86 FR 6446 (Jan. 21, 2021).

[738] 87 FR 74216 (Dec. 2, 2022).

[739] ''Occupational Employment and Wage Statistics (OEWS) Tables,'' Bureau of Labor Statistics, U.S. Department of Labor (May 2025), *https://www.bls.gov/oes/tables.htm.*

[740] The term ''covered entity'' includes health plans, health care clearinghouses, and most health care providers. Only certain provisions of the Privacy Rule apply to clearinghouses in their role as covered entities. Certain other provisions apply to clearinghouses in their role as business associates of other covered entities. *See* 45 CFR 164.500(b) and (c). Because the provisions addressed in this rule generally do not apply directly to clearinghouses, the Department does not anticipate that they will experience an increase in costs from the changes made by this final rule.

[741] *See* ''2022 Statistics of U.S. Businesses (SUSB) Annual Data Tables by Establishment Industry,'' United States Census Bureau (Apr. 2025), *https://www.census.gov/data/tables/2022/econ/susb/2022-susb-annual.html.*

TABLE 6—COVERED ENTITIES

NAICS[a] code	Type of entity	Firms	Establishments
524114	Direct Health and Medical Insurance Carriers	1,071	6,220
524292	Third Party Administrators	431	1,347
622	Hospitals	3,136	7,713
44611	Pharmacies and Drug Stores	18,857	56,910
6211-6213	Office of Drs. & Other Professionals	431,216	542,844
6215	Medical and Diagnostic Laboratories	9,025	19,810
6214	Outpatient Care Centers	28,324	59,802
6219	Other Ambulatory Health Care Services	11,317	16,715
623	Nursing and Residential Care Facilities	43,215	95,137
6216	Home Health Care Services	28,198	39,117
532283	Home Health Equipment Rental	485	1,891
Total		**575,275**	**847,506**

[a] North American Industry Classification System (NAICS) codes are six-digit industry identifiers used by Federal agencies to classify businesses for economic data analysis.

According to 2022 Census data, there are 1,071 Direct Health and Medical Insurance Carrier firms among the 6,116 Insurance Carrier firms (NAICS Code 5241); health and medical insurance firms make up 17.5 percent of insurance firms. Also, according to Census data, there are a total of 2,467 Third Party Administration of Insurance and Pension Funds firms (NAICS code 524292) with 7,693 establishments.[742] The Department assumes that 17.5 percent of these firms and establishments serve health and medical insurance because, although the Census does not specify what percentage of Third Party Administration firms and establishments are related to health care, it is reasonable to apply the same proportion as for insurance firms and establishments. Thus, in Table 6, the Department computes that this rule affects 431 of these firms (17.5 percent of 2,467) and their 1,347 associated establishments (17.5 percent of 7,693).

There were 56,910 community pharmacies (Census reports 18,857 pharmacy and drug store firms) operating in the U.S. in 2022.[743]

While certain changes will affect some health care providers and health plans differently than they affect others, all affected covered entities will need to adopt or modify some policies and procedures and re-train some employees. Affected entities include Federal, state, local, tribal, and private sector providers of health care. Because this final rule primarily affects covered entities, the Department does not calculate separately the effects of estimated costs and cost savings on business associates. To the extent that covered entities engage business associates to perform activities affected by this final rule, the Department logically anticipates that any additional costs are borne by the covered entities through their contractual agreements with business associates.

c. Individuals Affected

The Department believes that a large proportion of the approximately 343 million individuals in the United States[744] will be affected by this final rule because most individuals, even individuals who do not have health insurance or do not visit a health care provider this year, have some contact with at least one covered entity in a given year. The primary effect of the final rule on individuals will result from the modifications to the right of access, which will affect the speed of access, the fees that may be charged for access, and notice of those fees. Individuals also will be affected by an increase in disclosures for care coordination and case management to third parties, such as social services agencies, community-based support organizations, and home and community-based service providers. Eliminating the requirement for a covered health care provider to make a good faith effort to obtain a signed acknowledgment of receipt of the NPP, and replacing it with the right of an individual to discuss a covered entity's NPP, will affect nearly all individuals who receive services from a health care provider.

Individuals who are inmates and receive health care from covered health care providers will be affected by their inclusion in the right of an individual to receive an NPP at their first visit with a new health care provider. The Department provides details of the calculated estimate of the costs of this modification in section V.A.3.a.iv. below.

An express regulatory permission for workforce members to disclose PHI to a TRS communications assistant will have the greatest effect on the estimated 170,000 individuals employed in the health care sector who are deaf, hard of hearing, or deaf-blind,[745] as well as sector employees who have a speech disability.

3. Estimated Costs, Cost Savings, and Transfers Arising From Finalized Changes

Below, the Department provides the basis for the estimated quantified costs

[742] Each business organization consists of one firm that has one or more establishments (*i.e.,* places of business).

[743] ''2022 NCPA Digest, sponsored by Cardinal Health,'' The National Community Pharmacists Association, p. 9, Table 5 (2022), *https://ncpa.org/sites/default/files/2022-09/2022-Digest.pdf.*

[744] ''U.S. and World Population Clock,'' United States Census Bureau (last accessed Aug. 17, 2026), *https://www.census.gov/popclock/.*

[745] *See* ''Building Pathways to Health Care Careers for the Deaf and Hard-of-Hearing Community, Final Report,'' Task Force on Health Care Careers for the Deaf and Hard-of-Hearing Community, p. 14, 79, Table 4 (Mar. 2012), *https://www.rit.edu/ntid/sites/rit.edu.ntid/files/deafhub/taskforcereport2012.pdf; see also* Christopher J. Moreland, et al., ''Deafness Among Physicians and Trainees: A National Survey,'' Academic Medicine (Feb. 2013), *https://academic.oup.com/academicmedicine/article-abstract/88/2/224/8351869?redirectedFrom=fulltext.*

and savings resulting from the modifications to the Privacy Rule. These estimated quantified costs and savings are based on assumptions formed from the experience of the Office for Civil Rights with enforcement of the Privacy Rule, anecdotal reports from stakeholders, and public comments on the 2021 Privacy Rule NPRM and the 2022 Part 2 NPRM.

For the total annual number of access requests received by covered entities, this analysis adopts certain estimates from a survey commissioned by a trade association that responded to the request for comments on the 2021 Privacy Rule NPRM's assumptions [746]— estimates that are much greater than those in the proposed rule. See Table 7. This survey relied on responses from a sample of nearly 60 percent of association members who received 25 percent of total annual requests for copies of PHI, according to the survey's authors.

TABLE 7—ESTIMATED NUMBER OF ANNUAL REQUESTS FOR COPIES OF PHI, BY RECIPIENT[a]

Recipient of PHI copies	Number of PHI requests
Individuals	4,802,000[b]
Health Care Providers and/or Health Plans	24,108,000[c]
Designated Persons other than Providers and/or Plans	15,386,000[d]
Total	**44,296,000**

a. The figures in the table are based on an estimated total of 98 million annual requests for copies of PHI and adopt percentages presented in the association-sponsored study, which excluded 54.8 percent of requests (or 53.70 million) as unrelated to the right of access or the right of access to direct.
b. 4.9 percent of 98 million.
c. 24.6 percent of 98 million.
d. 15.7 percent of 98 million. This figure is used as a proxy for requests pursuant to the right of access to direct.

In addition to an estimate of total annual requests for copies of PHI, the survey included detailed quantitative estimates for the type of recipient, type of sender (a covered entity or a release of information company on behalf of a covered entity), PHI format (*i.e.,* paper, electronic PHI (ePHI) in an EHR,[747] and ePHI not in an EHR), and average fee per request. These estimates are largely consistent with estimates provided by other commenters.[748]

The survey provided data on the proportion of requests to send PHI to third parties other than health plans and health care providers in three formats: paper (8.7 percent); in an EHR (84.4 percent); and non-EHR electronic (6.8 percent). The Department applied these percentages to the 15.39 million requests to direct PHI to a person designated by the individual other than providers and/or health plans (in Table 7 above) to determine that 84.4 percent of requests (nearly 13 million) are for ePHI in an electronic health record and 6.8 percent of the 15.39 million requests are for ePHI that is not in an electronic health record (1 million). We do not have data to estimate the proportion of requests made pursuant to the right of access to direct that are for ePHI in an electronic health record and involve sending the copies via a non-internet-based method.

a. Quantified Costs to Covered Entities

The Department quantifies four categories of estimated costs arising from this final rule:

- Administrative activities [749] (non-recurring and recurring).
- Revising or creating policies and procedures, the NPP, and an access fee schedule.
- Revising training programs for workforce members.
- Distributing the NPP.

The Department estimates costs and cost savings for most activities attributable to this final rule using the equation below: [750]

Labor costs = fully loaded hourly wage (in 2025 dollars) × time (in hours) to perform regulatory requirement × number of instances the regulatory requirement is performed each year

i. Administrative Activities

Table 8 quantifies the additional estimated administrative non-recurring costs that covered entities will incur in the first year of implementing changes in this final rule.[751] This table does not include the costs for implementing proposals to require covered entities to print (and sometimes send) individualized fee estimates and itemized lists of copying charges,[752] which were reported as capital costs in the 2021 Privacy Rule NPRM, because those proposals are not being finalized.

[746] The commenter's members are release of health information companies.

[747] For purposes of this final rule, we use the term ''EHR'' to refer to the commonly understood meaning of the term; *i.e.,* a system that stores electronic health information across different health care settings. We use the term ''electronic health record'' when referring to the term defined in the HITECH Act and this final rule. *See* 42 U.S.C. 17921(5) (definition of ''Electronic health record''); 45 CFR 164.501 (definition of ''Electronic health record'').

[748] These commenters provided quantitative data estimates on a more limited set of issues than the association-sponsored survey. The survey also specifies how its estimates correspond to the estimates in the 2021 Privacy Rule NPRM. (Other commenters typically did not.)

[749] As used in this RIA, this term primarily applies to activities related to changes in the right of access.

[750] The Department estimates limited non-labor costs (paper, toner, and envelope and stamps as needed) to: (i) make fee schedules available at the point of service and upon request; (ii) distribute NPPs to individuals who are inmates; and (iii) provide NPPs to health plan subscribers. These costs represent an insignificant proportion of total costs of the final rule: about 1.7 percent in the first year; and 0.02 percent in subsequent years.

[751] The Department increased the estimated time to post each document online from 10 minutes to 15 minutes to align with the estimate in the 2024 Privacy Rule for posting documents online.

[752] *See* 86 FR 6446, 6517, (Jan. 21, 2021), Table 12b; proposed 45 CFR 164.525.

TABLE 8—NON-RECURRING ADMINISTRATIVE ACTIVITIES COSTS (2025 MILLION DOLLARS)

One-time cost	Burden count	Multiplier	Total administrative costs (millions)
Post access fee schedule online	15 min. x Web Developer ($94.98) = $23.75.	Total covered entities (847,506)	$20.12
Post revised NPP online	15 min. x Web Developer ($94.98) = $23.75.	Total covered entities (847,506)	$20.12
Total One-Time Administrative Burden			**$40.25**[a]

[a] Discrepancies in the total result from rounding.

Table 9 quantifies the recurring labor and capital [753] costs that the Department anticipates covered entities will incur for administrative activities that are included in the final rule.[754] The multipliers for the first three rows in Table 9 contain data from or associated with the estimated number of access requests for PHI in Table 7. These multipliers are substantially higher than the corresponding multipliers in the 2021 Privacy Rule NPRM [755] and incorporate information from commenters and Department assumptions. We adopt the approach taken in the 2021 Privacy Rule NPRM of increasing estimated costs for providing access within a shorter period of time by 1 minute of labor per request; however, in this final rule we are applying this approach equally to requests made pursuant to the right of access to direct. While one commenter reported that responding to requests made pursuant to the right of access to direct takes approximately 10 times the labor hours that the Department estimates (3–5 minutes), another commenter stated that in most cases, patients and other health care providers receive requested PHI in a matter of minutes. Some release of information firms stated that they generally respond to requests for copies of PHI in fewer than 15 days, which is consistent with the requirement in the final rule to provide access ''as soon as practicable'' and ''no later than 15 days.'' Given the variability in commenters' responses, the Department believes the approach used to estimate the burden hours for providing copies of PHI pursuant to the right of access (*i.e.,* adding an incremental labor burden) is reasonable. However, we also recognize that there are burdens associated with the right of access to direct that we did not previously acknowledge and are allocating 3 minutes per request as a previously unacknowledged burden on covered entities for the right of access to direct. See section V.G of this analysis.

[753] *See* 90 FR 15792, 15893 (Apr. 15, 2025) for the basis of our capital costs estimates.

[754] The proposed cost items that are excluded from the final rule are: ''Providing good faith fee estimates upon request''; ''Providing itemized list of access and authorization fees upon request''; and ''Submitting access requests to providers & plans for individuals.'' *See* 86 FR 6446, 6516, (Jan. 21, 2021), Table 12a.

[755] 86 FR 6446, 6516 (Jan. 21, 2021), Table 12a.

TABLE 9—RECURRING ADMINISTRATIVE ACTIVITIES COSTS (2025 MILLION DOLLARS)

Recurring Costs	Burden Hours & Pay or Capital Cost	Multiplier	Total Annual Cost (Millions)
Access for individuals in less time—Search and retrieval	1 min. x Medical Records Specialists time ($54.60) = $0.91	4,802,000 access requests	$4.37
Sending copies of ePHI to persons other than covered entities pursuant to the right of access to direct in less time—Non-internet-based method	1 min. x Medical Records Specialists time ($54.60) = $0.91	91.3% of 15,386,000 access requests = 14,046,078[a]	$12.78
Sending copies of ePHI to health plans and providers pursuant to the right of access to direct in less time—Non-internet-based method	1 min. x Medical Records Specialists time ($54.60) = $0.91	25% of 24,108,000 access requests = 6,027,000	$5.48
Discussing privacy practices with individuals upon request	7 min. x Registered Nurses time ($97.52) = $11.38	1% of 613,000,000 1st time encounters = 6,130,000	$69.74
Making fee schedule available at the point of service and upon request	2-page document printed on 1 sheet of paper = $0.021	3 copies for each of 847,506 covered entities = 2,542,518	$0.05
Total Annual Recurring Administrative Costs			**$92.43**

[a] Discrepancies in the total result from rounding.

The total estimated first year costs (including costs that will be recurring) for administrative activities are approximately $132.68 million (Table 8 total and Table 9 total).

ii. Costs for Revising Policies and Procedures

Table 10 quantifies non-recurring costs for covered entities to revise their policies and procedures to comply with the modifications made by this final rule. The Department also includes revising the NPP in this category because the labor costs for all these activities are attributable to the same occupation, a lawyer.

TABLE 10—COSTS FOR REVISING POLICIES AND PROCEDURES (2025 MILLION DOLLARS)

Revising policies & procedures	Time (mins.)	Covered entities affected	Burden hours
Disclosures for Care Coordination & Disclosures to Social Services Agencies & Community-Based Organizations	50	847,506	706,255
Right of Access	70	847,506	988,757
NPP (Revision)	60	847,506	847,506
Disclosures for Uniformed Services & TRS	10	847,506	141,251
Identity Verification	30	5% of 847,506 = 42,375	21,188
Total Burden Hours			**2,704,957**
Total Costs	1 hour of Lawyer's time ($178.70) * 2,704,957		**$483.38 million**

As compared to the 2021 Privacy Rule NPRM,[756] the estimated time to revise policies and procedures related to care coordination is reduced from 75 to 50 minutes because the Department is not finalizing modifications to the minimum necessary standard. Additionally, the estimated time to revise policies and procedures related to the right of access is reduced from 180 to 70 minutes because only a portion of the proposed modifications are being finalized. Specifically, covered entities will not be required to create or revise policies and procedures for the following proposals that are not being adopted:

- A right to inspect copies of PHI in person during a health care visit.
- A right to request that a health care provider forward an access request to another provider or health plan.
- A requirement to provide an individualized estimate of fees for copies of PHI.
- A requirement to provide an itemized list of costs for requested copies of PHI.

Finally, because the Department is not finalizing proposals addressing disclosures of PHI to family and friends of individuals and disclosures of PHI to prevent harm, we no longer include the corresponding non-recurring labor costs to revise related disclosure policies and procedures. This results in a reduction in labor of 60 minutes per covered entity (limited to health care providers) compared to the proposed rule.

In all other aspects (remaining time estimates, 5 percent estimate regarding covered entities expected to simplify verification and revise policies and procedures), Table 10 reflects the estimates in the 2021 Privacy Rule NPRM for revising HIPAA policies and procedures.[757]

iii. Training Costs

Table 11 quantifies non-recurring costs for revising HIPAA training programs.

[756] 86 FR 6446, 6517 (Jan. 21, 2021), Table 13.

[757] *See, e.g.,* 86 FR 6446, 6517 (Jan. 21, 2021), Table 13.

TABLE 11—COSTS FOR REVISING HIPAA TRAINING PROGRAMS (2025 MILLION DOLLARS)

Training content to be revised	Time (mins.)	Covered entities affected	Burden hours
Disclosures for Care Coordination, Disclosures to Social Services Agencies & Community-Based Organizations	40	847,506	565,004
Right of Access	80	847,506	1,130,008
Disclosures for Uniformed Services & TRS	15	847,506	211,877
Right to Discuss NPP	5	847,506	70,626
Identity Verification	10	5% of 847,506 = 42,375	7,063
Total Time to Update Training Content			1,984,577
Total Costs	1 hour of Training Specialists time = $72.64 * 1,984,577		**$144.16 million**

The Department is reducing the estimated time for a training specialist to update a covered entity's HIPAA training program, as compared to the 2021 Privacy Rule NPRM, because we are finalizing only some of the corresponding proposals. Accordingly, we have removed 20 minutes of labor for revising the training on the minimum necessary standard and removed 70 minutes of labor for revising the training to reflect multiple proposals to modify the right of access. Training will not be required to address proposed modifications that are not being adopted, namely, the proposals to:

- Expand the right to inspect copies of PHI in person to include viewing and recording PHI in conjunction with a health care visit.
- Add a right to request that a health care provider forward an access request to another provider.
- Require that a covered entity provide an individualized estimate of fees for copies of PHI.
- Require a covered entity to provide an itemized list of costs for copies of PHI.

Finally, because the Department is not finalizing proposals addressing disclosures of PHI to family and friends of individuals or to prevent harm, the Department no longer includes the corresponding labor costs to revise related training.

For all other components of the cost analysis for training (*i.e.,* remaining time estimates, 5 percent estimate of covered entities expected to change ''verification of identity'' procedures), Table 11 reflects the estimates in the 2021 Privacy Rule NPRM.

The Department also estimates non-recurring costs that will be incurred in the first year for training medical records specialists to implement changes to the right of access procedures as follows. On average, for each of the 847,506 covered entities, a medical records specialist will spend 5 additional minutes in training on this set of changes. These 70,626 hours for training workforce members correspond to $3.86 million non-recurring costs in 2025 dollars, based on the hourly wage in Table 5.

In total, additional non-recurring training costs attributable to changes in the final rule are $148.02 million in 2025 dollars.

iv. Distributing the NPP

Providing the NPP to Individuals Who Are Inmates

This final rule removes paragraph (a)(4) from 45 CFR 164.520, which excepts inmates in correctional institutions from the right to receive a copy of the NPP and excepts correctional institutions that are covered entities from the obligation of providing it. The Department requested comments about this proposal and did not receive any that addressed quantified costs for implementing it, although one commenter asserted that the proposal would add to workflow without any benefit. The Department is finalizing a new right for individuals who are inmates to receive a copy of an NPP and including an estimate of the costs for covered health care providers to provide such copies in person. We understand that contractors that provide health care in prisons and jails generally serve two roles: (1) managing a provider network and (2) handling claims for payments. To the extent that the contractor is a single covered entity, only one NPP is required. Where the contractor's business arrangements rely on separate covered entities to perform different functions, a joint NPP likely would be sufficient.[758] Thus, the cost estimates include only one NPP per individual who receives health care while an inmate in a correctional institution.

The Department anticipates that individuals who are newly admitted to prisons and jails will receive a two-page double-sided printed copy of the NPP during their first health care encounter, as will individuals who are already incarcerated when the rule becomes effective, likely upon their next visit to a covered health care provider. The Department estimates that distributing each NPP costs $0.972: $0.042 in paper and toner[759] and $0.930 in labor costs.[760] This totals approximately $4 million in year one for distributing an NPP to individuals who are inmates[761] and $3 million annually for this modification in years two through five.

The Bureau of Justice Statistics (BJS) reported that in 2023, there were 472,000 new admissions to prisons and

[758] *See* 45 CFR 164.520(d) (allowing joint notice for organized health care arrangements).

[759] *See* 90 FR 15792, 15893 (Apr. 15, 2025).

[760] One minute and 15 seconds of an office clerk's time at $44.624/hour in 2025 dollars.

[761] The non-recurring portion of the estimated cost in the first year is $1,185,193.

7,627,000 new admissions to jails.[762] The BJS reported that there were 1,230,000 individuals in prison as of the last day of the previous year, and 663,100 inmates in jails as of the last day of the previous year.[763]

At the high end, the Department assumes that during the first year, each individual who is a new inmate has a health care visit with a covered health care provider, as do individuals who were inmates on the last day of the previous year. While theoretically possible, there are several reasons why this scenario is unlikely to happen and the number of distributed NPPs will be lower in practice, as explained further below.

In the first year, the Department estimates that at the high end, costs for these new activities will be $9,712,321,[764] while annual costs in years two through five will be $7,872,228.[765] These estimates include labor and costs of paper and printing the NPPs. This likely is an overestimate for at least three reasons. First, some of the health care provided to individuals who are inmates is paid for directly by correctional facilities employing staff in prison or jail health clinics, rather than through electronic transactions using standards adopted under HIPAA.[766] Thus, only a portion of health care is provided by health care providers who are subject to HIPAA. Second, jail admission statistics include repeat offenders. The same individual who is admitted to the same jail multiple times in a year would receive only one NPP when the correctional institution health care provider's records show the individual is not a new patient. Third, unlike prisons that house persons who are serving sentences of longer than 1 year, individuals who are admitted to jails often are there for short periods of time and have less opportunity to receive health care, or may not need health care during that time period.[767]

The Department's low-end estimate accounts for these circumstances as follows. First, a recent study reports that 90 percent of jails contracted with private companies to provide health care.[768] The Department calculates its low-end estimates by assuming that only 85 percent of jails contract with private companies (slightly fewer than 90 percent), which implies that only 85 percent of new and current jail inmates will receive an NPP.

There is limited public information about the use by Federal prisons of covered health care providers; however, we do know that Federal prisons both employ workforce members and engage private companies to provide health care.[769] For its low-end estimates, the Department assumes that 85 percent of prisoners [770] in state prisons receive health care from covered health care providers, while 0 percent of Federal prisoners do. BJS reports that state prisons account for approximately 91 percent of new admissions to prison and 88 percent of individuals who are imprisoned at the end of the reporting year.[771] We estimate that 77 percent of individuals who are new inmates have rights under the Privacy Rule because they receive health care from a covered health care provider (weighted average of 85 percent and 0 percent); 74 percent is the percentage (average of Federal and state) of individuals in prison at the end of the year who have such rights.

Second, according to a recent study, ''[i]n 2023, there were 7.6 million jail admissions, but 1 in 4 of these admissions was someone returning to jail for at least the second time that year.'' For its low-end estimates, the Department assumes that unique jail inmates are 75 percent of the 85 percent of new jail inmates who have rights under HIPAA.

Third, the BJS reports that the average number of days an individual spent in jail was 31.8 in 2023, a number that is likely skewed upward by relatively few (about 30 percent) convicted individuals serving their sentence in jail, while the majority (70 percent) of individuals in jail are there for much shorter times.[772]

The BJS does not report detailed information about the distribution of the length of jail stay statistics. A recent study using data from a sample of jails reports that the median length of stay was 4 days.[773] The Department assumes that only individuals who spend more than 1 month in jail will receive a medical examination (and an NPP). The figures presented above imply that the fraction of jailed individuals whose stay is shorter than 1 month is greater than 50 percent and likely closer to 100 percent than 75 percent (the midpoint between the two). For its low-end estimate, the Department adopts an estimate that 80 percent of jailed individuals' stay is shorter than 1 month, and thus further reduces the counts of jailed individuals by that proportion (after reducing it to account for individuals who are admitted to jail multiple times and health care providers that are not covered entities).

Thus, at the low end, the Department estimates that individuals who are inmates will receive 2,330,628 NPPs at a $2,265,370 cost during the first year. The non-recurring portion of the estimated cost in the first year is $966,892, which reflects that, as compared to the high-end estimate, only 74 percent of individuals in prison and 12.75 percent of individuals in jail (85 percent × 75 percent × 20 percent) contribute to costs.

The recurring portions of the low-end estimates, which equal the estimates for the second year onward, are 1,335,883 NPPs and $1,298,478 in costs. These figures reflect that, as compared to the high-end estimate, only 77 percent of individuals in prison and 12.75 percent of individuals in jail (85 percent × 75 percent × 20 percent) contribute to costs.

For its primary estimate, the Department uses data from the

[762] *See* ''Prisoners in 2023—Statistical Tables,'' Office of Justice Programs, Bureau of Justice Statistics, U.S. Department of Justice, NCJ 310197 (Sept. 2025), *https://bjs.ojp.gov/document/p23st.pdf;* ''Jail Inmates in 2023—Statistical Tables,'' U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, U.S. Department of Justice, NCJ 309965 (Apr. 2025), *https://bjs.ojp.gov/document/ji23st.pdf.* Figures rounded to thousands of admissions. Jail statistics for the 12-month period ending on June 30, 2023.

[763] *Id.*

[764] $0.972 × 9,992,100, which is the sum of 8,099,000 new admissions and 1,893,100 year-end individuals who are inmates. The non-recurring portion of this amount is $1,840,093 ($0.972 × 1,893,100). Discrepancies in totals result from rounding.

[765] $0.972 × 8,099,000. Discrepancies in totals result from rounding.

[766] *See* Sec. 262(a) of Public Law 104–191, 110 Stat. 2021, adding sec. 1173(a) (codified at 42 U.S.C. 1320d–2(a)(1); *see also* 45 CFR 162.1101 *et seq.* and 162.1601 *et seq.*

[767] BJS also reports that people admitted to local jails spent an average of 32 days in custody before release.

[768] Jessica Carda-Auten, et al., ''Jail Health Care in the Southeastern United States from Entry to Release,'' The Milbank Quarterly, Vol. 100, No. 3, pp. 722–760 (May 3, 2022), *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9576246/.*

[769] *See* ''Medical Care,'' Federal Bureau of Prisons, *https://www.bop.gov/inmates/custody_and_care/medical_care.jsp* (last accessed Mar. 9, 2026) (stating that the Federal Bureau of Prisons operates seven medical referral centers providing advanced care); *see also* ''Health Services Division,'' Federal Bureau of Prisons, *https://www.bop.gov/about/agency/org_hsd.jsp* (last accessed Mar. 9, 2026) (stating that the Federal Bureau of Prisons has over 3,000 health care positions).

[770] Here ''prisoners'' refers to individuals who are incarcerated in state and Federal prisons, as distinct from those who are held in jails.

[771] *See* ''Prisoners in 2023—Statistical Tables,'' Office of Justice Programs, Bureau of Justice Statistics, U.S. Department of Justice, NCJ 310197 (Sept. 2025), *https://bjs.ojp.gov/document/p23st.pdf.*

[772] *See* Zhen Zeng, ''Jail Inmates 2023—Statistical Tables,'' Office of Justice Programs, Bureau of Justice Statistics, U.S. Department of Justice, NCJ 309965 (Apr. 2025), *https://bjs.ojp.gov/document/ji23st.pdf.*

[773] Leah Wang, ''Jailing the homeless: New data shed light on unhoused people in local jails,'' Prison Policy Initiative Briefing (Feb. 11, 2025), *https://www.prisonpolicy.org/blog/2025/02/11/jail_unhoused_bookings/.*

Connecticut Department of Correction on individuals in jail to determine whether costs are likely closer to the low-end estimate.[774] The analysis shows that about 15 percent of new admissions to jail in any given year are for repeat offenders, which is closer to the 25 percent used in the low estimate than the 0 percent in the high estimate. The analysis shows that, when considering only the longest stay in jail for repeat offenders, about 50 percent of unique newly admitted individuals stay for 1 month or longer, which is closer to the 20 percent used in the low estimate than the 100 percent in the high estimate.

Thus, the Department's primary estimate is a weighted average of the low-end (75 percent) and high-end (25 percent) estimates. Based on the Department's primary estimate, individuals who are inmates will receive 4,245,996 NPPs at a $4,127,108 cost during the first year,[775] and 3,026,662 NPPs at a $2,941,915 cost in years two through five.

Providing the NPP to Health Plan Subscribers

The Department does not anticipate any new costs for covered health care providers associated with distribution of the revised NPP other than posting it on their websites (if they have one) because they have an ongoing obligation to provide the NPP to first-time patients that is already accounted for in cost estimates for the HIPAA Rules. Health plans that post their NPP online will incur minimal costs by posting the updated NPP and then including it in the next annual mailing to subscribers. Health plans that do not provide an annual mailing will incur the additional costs (capital and labor expenses) for mailing the revised NPP off-cycle.

Health plans that do not provide an annual mailing will potentially incur an additional $12,990,000 in capital expenses[776] for an off-cycle mailing of the revised NPP. The Department estimates that health plans will mail the NPP to an estimated 10 percent of the 150 million health plan subscribers who receive a mailed, paper copy of the NPP, as well as the labor expense for an office clerk at the rate shown in Table 5 to complete the mailing at a mailing rate of 240 NPPs per hour (15 seconds or 0.25 minutes per NPP), for $2,790,000 [= 62,500 hours × $44.64].

Total Costs of Distributing the NPP

The total costs of distributing the NPP to individuals who are inmates and to health plan subscribers are $19,907,108 in the first year and $2,941,915 in years two through five. These expenses include labor and capital costs.

v. Eliminating the NPP Acknowledgment

The final rule eliminates the requirement for covered health care providers who have a direct treatment relationship with an individual to make a good faith effort to obtain an acknowledgment from the individual that they received a copy of the NPP (or document the provider's efforts to obtain such acknowledgment) and adopts the estimated cost savings for approximately 613 million first time visits with health care providers annually.[777] As proposed in the 2021 Privacy Rule NPRM, the Department estimates a burden reduction because of the regulatory modifications in the amount of 1 minute and 45 seconds of labor at the hourly wage rate of an office clerk. One minute and 15 seconds of labor is retained for the act of providing a copy of the NPP. The final rule also replaces the wage rate of a general health occupations worker (used to calculate estimated costs for this requirement in the 2024 Privacy Rule) with that of a clerical worker.[778]

vi. Total Quantified Cost Savings

Table 12 summarizes the quantification of cost savings for covered entities and reports their value in 2025 dollars. This table eliminates the projected cost savings from creating an exception to the minimum necessary standard in 45 CFR 164.502(b).[779]

TABLE 12—RECURRING BENEFITS (LABOR COST SAVINGS, 2025 MILLION DOLLARS)

Cost item	Burden count	Multiplier	Savings (millions)
Eliminating NPP Acknowledgment	1 minute and 45 seconds (0.0292 hours) of Office Clerk, General time x $44.64 = $1.302	613,000,000 first-time encounters	$798.13
Total Annual Cost Savings			**$798.13**
Total Cumulative Cost Savings (5 years, undiscounted)			**$3,990.60**

[774] *See* ''Accused Pre-Trial Inmates in Correctional Facilities,'' State of Connecticut, Department of Corrections (2017–2025 data) (last accessed Mar. 9, 2026), *https://data.ct.gov/Public-Safety/Accused-Pre-Trial-Inmates-in-Correctional-Faciliti/b674-jy6w/about_data*.

[775] The non-recurring portion of the estimated cost in the first year is $1,185,193.

[776] *See* 90 FR 15792, 15893 (Apr. 15, 2025) for the basis of our capital cost estimates. We assume a 2-page, double-sided NPP to cost $.042 in paper and toner, an envelope to cost $0.044, and for the metered postage to cost $0.78 (as of Aug. 17, 2026). Accordingly, each NPP costs approximately $0.866, which is a high estimate given the availability of bulk postage rates for large volume mailings.

[777] 78 FR 5566, 5675 (Jan. 25, 2013).

[778] We are not adopting the proposal in the 2021 Privacy Rule NPRM to replace a general health occupations worker with a receptionist. *See* 86 FR 6446, 6514 (Jan. 21, 2021).

[779] *See* 86 FR 6446, 6515, (Jan. 21, 2021), Table 10.

b. Comparison of Quantified Costs and Benefits

The tables below present the Department's summary of estimated first year (Table 13) and ongoing (Table 14) quantified costs and cost savings.

TABLE 13— FIRST-YEAR ESTIMATED COSTS/COST SAVINGS (2025 MILLION DOLLARS)

Cost item	Costs	Savings
Revise Training	$148.02	
Revise Policies & Procedures	$483.38	
Administrative Costs	$132.68	
Distribute NPP	$19.91	
Eliminate NPP Acknowledgment		($798.13)
TOTAL	**$783.98**	**($798.13)**
NET SAVINGS/COST		**($14.15)**

TABLE 14—RECURRING ESTIMATED ANNUAL COSTS/COSTS SAVINGS (2025 MILLION DOLLARS)

Cost item	Costs	Set-off amount (savings)
Access & Administrative Costs	$92.43	
Distribute NPP	$2.94	
Eliminating NPP Acknowledgment		($798.13)
TOTAL	**$95.37**	**($798.13)**
NET SAVINGS/COST		**($702.75)**

c. Estimated Transfers From Modifications to Access Fees

As described below, the Department has revised estimates of monetary transfers resulting from changes to access fees by relying in part on quantitative data from a trade association that provided comments on the assumptions in the 2021 Privacy Rule NPRM.

Comment: One commenter submitted the results of a voluntary survey of members that it sponsored. The survey addressed the financial effects of the proposed rule, particularly modifications to the right of access to direct and allowable fees for the right of access to direct. According to the commenter, the results were based on data from responding members, who the commenter estimated were responsible for processing approximately 25 percent of the total number of requests for PHI annually. By extrapolating from the responses, the commenter then estimated the total number of requests for copies of PHI to be approximately 100 million annually. Other public comments on the 2021 Privacy Rule NPRM included estimates in the same order of magnitude—some as high as 200 million.

The total number of annual requests for copies of PHI represented in the survey included both requests made pursuant to the right of access and requests for disclosures based on authorizations, copies provided in all formats (electronic or not), and copies provided directly by health care providers and those provided by release of information companies on behalf of health care providers. According to the survey, the proposed changes would apply to only approximately 45 percent of requests (those made pursuant to the right of access). The percentages in the survey were consistent with estimates submitted in other public comments.[780]

The survey categorized the number of requests annually by type of person receiving the requested PHI (*i.e.,* individuals, health care providers or health plans, persons other than health care providers and health plans). It assumed that requests from health care providers or health plans were for treatment, care coordination, or payment and excluded those requests from the right of access category. The survey also categorized requests for copies of PHI by format (*i.e.,* ePHI in an electronic health record, ePHI not in an electronic health record, paper copies of PHI). According to the survey, almost 90 percent of all requests were for electronic copies of PHI in an electronic health record, and that percentage was increasing over time, while the other two formats were becoming increasingly rare. The percentages in the survey were consistent with percentage estimates provided by other commenters.[781]

Response: Based on public comments, the Department extrapolates the size of

[780] The survey reported that individuals, health care providers or health plans, and persons other than health care providers and health plans accounted for 11, 54, and 35 percent of requests, respectively. Another release of information company reported that disclosures to facilitate patient care accounted for 50 percent of the requests directed to one of its health care provider clients. An individual commenter asserted that 60–70 percent of requests received by his employer (a release of information company) were from health care providers requesting the transfer of PHI to facilitate care for individuals; another commenter reported that 50 percent of requests annually were to facilitate patient care.

[781] *Id.* Additionally, a commenter reported that fewer than 1 percent of requests were for paper records.

the total number of requests for copies of PHI from the figures provided in the survey described above and estimates a range between 78 and 171 million requests annually.[782] In addition to being consistent with other commenters' estimates, the Department believes that the survey correctly recognized that requests made pursuant to the right of access represent only about 45 percent of total requests for copies of PHI made annually, and thus the modifications made to fee limitations by this final rule cannot and do not apply to the majority of total requests for PHI.

Reducing the Expenses That Can Be Included in Calculated Access Fees for Providing Individuals With Copies of PHI in an Electronic Health Record on Electronic Media

The final rule prohibits a covered entity from charging an individual for the costs of electronic media and postage when providing access by mailing copies of PHI in an electronic health record on electronic media. The Department estimates that the costs of electronic media may range from $1 for a CD to $4 for a USB drive and the postage may range from $1 to $3, resulting in a range of estimated increased costs to covered entities of $2 to $7 per request of this type, or an average estimated increase of $4.50.

Based on the survey described above, the Department estimates that about 6.8 percent of the 4,802,000 copies of PHI that individuals receive annually will be subject to the fee limitations for sending copies on electronic media (or 326,863).[783] Thus, the Department estimates a total reduction in access fees paid by individuals of $1,470,883 because of this change. At the same time, these are payments that previously were revenue for covered entities (or their business associates), and thus may be considered a monetary transfer from covered entities to individuals, as reflected in Table 15.

Summary Results of the Department's Estimated Transfers Due to Fee Adjustments

The Department summarizes in Table 15 the estimated annual recurring monetary transfers that parties will experience because of changes in regulation.

TABLE 15—ESTIMATED ANNUAL TRANSFERS (2025 MILLION DOLLARS)

Monetary Change	Amount of monetary transfer (transferors)	Amount of monetary gain (transferees)
Decreased fees for providing electronic copies of PHI in an electronic health record on electronic media to individuals	$1.47 (covered entities, primarily providers)	$1.47 (individuals)

The Department estimates that individuals will benefit from an annual monetary transfer of $1.47 million from covered entities or their business associates as result of reductions in allowable fees for providing copies of PHI to individuals.

d. Costs Borne by the Department

The Department expects to incur costs related to disseminating information about the regulatory changes to covered entities, including health care providers and health plans. However, we expect that many of these costs will be included in the costs for the ongoing dissemination of guidance and other explanatory materials that the Department provides on the HIPAA Rules. The Department also expects to incur costs to enforce the final rule; however, these costs will be absorbed into the baseline budget for the ongoing enforcement of the Privacy Rule. The covered entities that are operated by the Department will be affected by the regulatory changes in a similar manner to other covered entities, and the Department has factored those costs into the estimates above.

e. Qualitative Analysis of Non-Quantified Benefits

The Department confirms the 2021 Privacy Rule NPRM's analysis of non-quantified benefits for the proposals that are being adopted in this final rule.

f. Uncertainty Analysis for Estimated Costs and Cost Savings

Below, the Department quantifies ranges for costs and cost savings for key compliance burdens. We perform an uncertainty analysis for each of the main drivers of costs and cost savings, reporting low, mid, and high values for each category, and for the final rule as a whole, to capture the range of potential outcomes.

In summary, the Department estimates that total costs of implementation over a 5-year period range from a low of approximately $0.63 billion to a high of approximately $4.93 billion and that the cost savings over that same 5-year period range from approximately $1.14 billion to approximately $6.65 billion.

[782] The annual number of access requests, as extrapolated from information provided by several commenters, varied from 171 million requests per year to 139 million, 136 million, and 78 million. The number of right of access requests annually as reported in the survey was approximately 20 times higher than the number estimated by the Department in the 2021 Privacy Rule NPRM (86 FR 6446, 6506 (Jan. 21, 2021), Table 6). The Department recognizes that larger studies provide stronger and more reliable results; a 25 percent sample relative to total number of requests for PHI (such as provided in the survey) is large by statistical standards.

[783] The survey reported that about 6.8 percent of access requests under the right of access to direct were for electronic records contained in systems that predate EHR systems. The Department believes it is reasonable to apply this same percentage to estimate that 6.8 percent of the 4,802,000 copies of PHI individuals receive annually will be subject to the proposed fee limitations for sending copies on electronic media (or 326,863). (The survey also reported that 8.7 percent of access requests under the right of access to direct were for paper records, and 84.4 percent were for electronic records in an EHR. Because of rounding, the three percentages sum to 99.9 percent (6.8+8.7+84.4=99.9 percent). The Department applied a mathematical correction to these percentages for accuracy.)

TABLE 16—RANGE OF TOTAL COSTS OVER 5 YEARS, 2025 DOLLARS[a]

Cost item	Low	Mid	High
Training	$130,056,576	$148,015,793	$166,746,240
Policies & Procedures	$376,939,119	$483,375,753	$904,434,863
Access & Administrative Tasks	$102,964,668	$502,411,896	$3,798,535,593
Distribute NPP	$23,239,281	$31,674,769	$56,981,233
TOTAL COSTS	**$633,199,644**	**$1,165,478,212**	**$4,926,697,929**

[a] Discrepancies in totals result from rounding.

TABLE 17—RANGE OF TOTAL COSTS SAVINGS OVER 5 YEARS, 2025 DOLLARS

Cost savings item	Low	Mid	High
Eliminating NPP Acknowledgment	$1,140,180,000	$3,990,630,000	$6,651,050,000
TOTAL COST SAVINGS	**$1,140,180,000**	**$3,990,630,000**	**$6,651,050,000**

The Department calculates these ranges adopting a methodology that is as close as possible as the uncertainty analysis in the 2021 Privacy Rule NPRM, as detailed below.

i. Cost Estimates

Updated Training Content

The 2021 Privacy Rule NPRM's uncertainty analysis for revising training content focused solely on the 150 minutes that each covered entity would spend on changes related to the right of access,[784] including allowable fees,[785] and established an uncertainty range between 120 minutes (2 hours) at the low end (80 percent of 150 minutes) and 180 minutes (3 hours) on the high end (120 percent of 150 minutes).

This final rule adopts the same approach by setting a range above and below the 80 minute estimate in Table 11, second row, between 64 minutes at the low end (80 percent of 80 minutes) and 96 minutes at the high end (120 percent of 80 minutes). This results in a low estimate of 904,006 total annual burden hours for all covered entities at a non-recurring cost of $65,667,025 and a high estimate of 1,356,010 burden hours at a non-recurring cost of $98,500,537 for updating the right of access portions of the training program. Overall, the total non-recurring cost for updating training content is $144,159,641, with a range between $127,742,884 and $160,576,397 in a low-end and high-end scenario, respectively.

Time Spent in Training

In this final rule, the Department revises downward the estimated additional time a medical records specialist will spend in training from 7 minutes to 5 minutes because proposed changes to the allowable fees for the right of access to direct are not addressed in this final rule.[786] The Department adopts the range that it applied in the 2021 Privacy Rule NPRM (minus 2 minutes or plus 3 minutes), and applies it to the revised 5-minute base estimate, resulting in a low of 3 minutes to a high of 8 minutes. Accordingly, the non-recurring burden hours for additional training of medical records specialists is 70,626 and ranges between 42,375 and 113,001 burden hours ($3.86 million base cost ranges between $2.31 and $6.17 million) for a low-end or high-end scenario, respectively.

Training, Overall

Overall (updating training content plus time spent in training), the estimated training burden ranges from a low of $130,056,576 (and 1,800,950 burden hours) to a high of $166,746,240 (and 2,323,579 burden hours), with a base estimate (the mid-range) of $148,015,793 (and 2,055,203 burden hours).

Updated Policies and Procedures

The 2021 Privacy Rule NPRM used a range for cost burden from $542,791,420 to $1,302,384,017 (78.0 percent and 187.1 percent relative to a base estimate of $696,059,017). For consistency, this analysis applies 78.0 percent and 187.1 percent to the base estimate of $483,375,753 in 2025 dollars, which yields a range between $376,939,119 and $904,434,863.

Access and Administrative Tasks—Recurring Costs Unless Specified

Post an Access Fee Schedule and a Revised NPP Online

As compared to the 2021 Privacy Rule NPRM, the Department increased the time to post each document online from 10 to 15 minutes for consistency with the estimate for posting documents online that was adopted in the 2024 Privacy Rule.

The Department adjusts the range used in the 2021 Privacy Rule NPRM for this non-recurring burden to a low of 8 minutes and a high of 20 minutes for each of the documents posted online. Thus, the total annual burden hours in Table 8 are 423,753 at a cost of $40,248,060 million, with a range from 226,002 to 565,004, and costs range from $21,465,632 at the low end to $53,664,080 at the high end.

Unreimbursed Costs of Providing Access (Search And Retrieval in Less Time)

To account for the additional costs to perform search and retrieval of PHI in less time, the Department applies a range of 0.5 minutes below the base estimate of 1 minute (at the low end) and 2.5 minutes above the base estimate of 1 minute (at the high end).[787] The Department applies these values to the number of copies of PHI sent to individuals in Table 9. Thus, the total estimated burden hours are 80,033 with a range from a low of 40,017 hours to a high of 200,083 hours. Annual

[784] In other words, the Department's estimate in Table 14 of the time required to make other revisions to training content did not vary across a low, middle, and high end. 86 FR 6446, 6517 (Jan. 21, 2021), Table 14.

[785] *Id.* at Table 14, second row.

[786] *See* 86 FR 6446, 6518 (Jan. 21, 2021), Table 14b.

[787] This is the same range applied in the 2021 Privacy Rule NPRM.

estimated cost in 2025 dollars is $4,369,820 with a range from a low of $2,184,910 to a high of $10,924,485 (see the first row of Table 9 for base estimate methodology).

Transmit Electronic Copies of PHI in an Electronic Health Record to Designated Persons Through Non-Internet-Based Method

The Department uses this range above and below the base estimate of 1 minute for the costs attributable to transmitting electronic copies of PHI in an electronic health record to persons designated by individuals: 0.5 minutes at the low end and 2.5 minutes at the high end. We apply these values to our estimate of copies of ePHI not in an EHR sent to designated persons via non-internet-based methods. Accordingly, the total estimated burden hours are 234,101 with a range from a low of 117,051 hours to a high of 585,253. The annual estimated cost in 2025 dollars is $12,781,931 with a range from a low of $6,390,966 to a high of $31,954,828 (see the second row of Table 9 for details of base estimate methodology).

Transmit ePHI to Health Plans and Providers Through Non-Internet-Based Method

The Department uses this range above and below the base estimate of 1 minute for these costs: 0.5 minutes at the low end and 2.5 minutes at the high end. We apply these values to our estimate of copies of ePHI not in an EHR sent to designated persons via non-internet-based methods. Accordingly, the total estimated burden hours are 100,450 with a range from a low of 50,225 hours to a high of 251,125. The annual estimated cost in 2025 dollars is $5,484,570 with a range from a low of $2,742,285 to a high of $13,711,425 (see the third row of Table 9 for details of base estimate methodology).

Discussing Privacy Practices

For these costs, the Department applies a range above and below the base estimate of 7 minutes for each of 6,130,000 health care encounters (1 percent of 613,000,000 total new health care encounters per year) for a total of 715,617 burden hours and an estimated cost of $69,743,053. The range is computed as follows: at the low end, a registered nurse spends 5 minutes for each of 613,000 health care encounters (0.1 percent of 613,000,000 total new health care encounters per year); at the high end, a health care manager spends 10 minutes for each of 30,650,000 health care encounters (5 percent of total new health care encounters per year).[788]

Thus, total estimated burden hours range from 51,083 at the low end to 5,108,333 at the high end. Estimated costs range from $4,981,647 at the low end to $692,383,500 at the high end (see the fourth row of Table 9 for details of base estimate methodology). Over time, it is likely that more covered health care providers will choose to employ technologies such as super intelligence as an option for individuals to obtain answers to their questions about the NPP. As a result of increased efficiencies from a technology-assisted approach, the burden hours and associated costs of the right to discuss may decrease; however, we are unable to predict the magnitude or velocity of this decrease.

NPP to Individuals Who Are Inmates

The Department's base estimate ($15,894,769 over 5 years), and low-end and high-end estimates ($7,459,281 and $41,201,233, respectively) have been discussed in detail above.

ii. Cost Savings Estimates

Removing NPP Acknowledgment Requirement

The Department adopts a range of cost savings from a low of 30 seconds to a high of 2 minutes and 55 seconds for each NPP that is provided to a new patient with whom the health care provider has a direct treatment relationship (respectively 166.7 percent and 28.6 percent relative to the mid-range value of 105 seconds in Table 12).[789]

On an annual basis for all covered entities, cost savings from removing the requirement to obtain a written acknowledgment of receipt of the NPP range from a total savings of 5,108,331 burden hours and $228,036,000 in cost savings at the low end to 29,798,611 burden hours and $1,330,210,000 in cost savings at the high end (respectively 28.6 percent and 166.7 percent relative to mid-range annual values of 17,879,167 burden hours and $798,126,000 in estimated cost savings).

4. Consideration of Regulatory Alternatives

The Department carefully considered several alternatives to issuing this final rule, including the option of not pursuing any regulatory changes, but rejected that approach for several reasons. First, the regulatory changes that we are finalizing will further the Administration's goal of reducing regulatory burden on individuals and the regulated community and promoting care coordination. Second, many commenters on the 2021 Privacy Rule NPRM believed that the Privacy Rule could be improved and offered comments that expressed support for some of the ideas suggested in the NPRM that are now finalized. Revising the Privacy Rule will clarify covered entities' obligations and flexibilities, improve individuals' access to their PHI, and improve care coordination and case management overall.

Table 18 reports estimated costs, benefits (*i.e.,* cost savings), and monetary transfers of finalizing the 2021 Privacy Rule NPRM as published and compares them to the corresponding values in this final rule. The costs, benefits, and transfers in the right-hand column (NPRM column) are an update of the estimates presented in the NPRM that match the assumptions in this final rule.

[788] *Id.*

[789] *Id.*

TABLE 18—COMPARISON OF FINAL RULE AND NPRM ESTIMATED 5-YEAR COSTS, COST-SAVINGS, AND TRANSFERS, UNDISCOUNTED, IN MILLIONS

	Final Rule	NPRM
Costs		
Revise Training	$148.02	$281.04
Revise Policies and Procedures, NPP, and Fee Schedule	$483.38	$974.23
Administrative Activities	$502.41	$569.33
Distribute NPP	$31.67	
Provide Individualized Fee Estimates and Itemized List of Copy Charges		$0.87
Total Costs	**$1,165.48**	**$1,825.47**
Cost Savings		
Eliminate NPP Acknowledgment	$3,990.63	$3,990.63
Clarifying Minimum Necessary		$2,297.42
Total Cost Savings	**$3,990.63**	**$6,288.05**
Net Total (negative = savings)	**-$2,825.15**	**-$4,462.58**
Transfers To Individuals	**$7.35**	**$7.35**

In addition to the proposals in the 2021 Privacy Rule NPRM that the Department declines to finalize at this time, the Department considered several other regulatory alternatives.

Scope of Health-Related Information of an Individual

The Department considered adopting a definition of the term ''electronic health record'' in which the scope of the ''health-related information of an individual'' description within the definition would cover the same scope of information as PHI as defined in the Privacy Rule at 45 CFR 160.103. Such an approach would have, by definition, excluded the subset of individually identifiable health information that is expressly excluded from the definition of PHI.[790]

However, the Department is adopting a definition of electronic health record for the specific purpose of clarifying how the Privacy Rule aligns with the statutory right of access to direct as set forth in section 13405(e) of the Health Information Technology for Economic and Clinical Health (HITECH) Act.[791] Section 164.524 limits the right of access to PHI about the individual in a designated record set. Because the HITECH Act added the right of an individual to direct a covered entity to transmit an electronic copy of their PHI in an electronic health record to a person designated by the individual as a component of the right of access at 45 CFR 164.524, the right of access to direct also is necessarily limited to PHI about the individual in a designated record set. Therefore, the Department believes that it is unnecessary to limit the information included in an electronic health record. Additionally, the Department believes that it is more appropriate to address the limitations of the right of access to direct within the applicable standard.

Further Reduce Timeliness Requirements for Responding to Requests Made Pursuant to 45 CFR 164.524

In the 2021 Privacy Rule NPRM, the Department requested comment on the ability of covered entities to respond to a request for access in under 15 days, and in this final rule considered requiring a shorter response time for requests to obtain electronic copies of PHI or a subset of PHI, including where such requests are made pursuant to the right of access to direct. In this alternative scenario, as in the final rule, covered entities would be required to respond to access requests ''as soon as practicable'' and ''no later than'' a certain number of days. The Department believes that it is possible for covered entities using health IT to provide access to at least electronic copies of ePHI in fewer than 15 days. In fact, as discussed with respect to recurring costs for providing access within a shorter time and Table 9 in section A.3.a.i of the RIA, the Department believes that some portion of covered entities already are providing individuals with access in fewer than 15 days. Adopting such an approach would have been consistent with opinions expressed by some commenters. However, the Department believes that we do not have sufficient information to determine whether this is true for all PHI or only a subset of such. Thus, we believe that this issue would be more appropriately addressed through additional notice and comment rulemaking. Accordingly, we intend to issue an NPRM in the future to address and obtain public comment on this issue.

Table 19 reports cost estimates to shorten access response time from 30 days to 3 days for all requests for electronic copies of PHI maintained electronically pursuant to 45 CFR 164.524. These estimates rely on the

[790] *See* 45 CFR 160.103 (definition of ''Protected health information'').

[791] 42 U.S.C. 17935(e).

methodology in Table 9, which projects that reducing the required response time by at least 15 days (from no more than 30 days to as soon as practicable but no more than 15 days) will cost $22.64 million (sum of costs in first three rows) annually. These costs are extrapolated proportionally: the Department estimates that reducing the required response time by an additional 12 days would add 80 percent of a minute (12/15 = 80 percent) or 48 seconds to the 1 minute in Table 9.

TABLE 19—ESTIMATED RECURRING ADMINISTRATIVE COSTS (2025 MILLION DOLLARS), RESPONSES WITHIN 3 DAYS

Recurring Costs	Burden Hours & Pay	Multiplier	Total Annual Administrative Cost (Millions)
Access for Individuals — Search and retrieval in less time.	1 min. and 48 sec. x Medical Records Specialists time ($54.60) = $1.64	91.3% of 4,802,000 access requests = 4,383,808[a]	$7.18
Sending copies of ePHI to third parties other than covered entities in less time—Non-internet-based method.	1 min. and 48 sec. x Medical Records Specialists time ($54.60) = $1.64	91.3% of 15,386,000 access requests = 14,046,[078b]	$23.01
Sending copies of ePHI to health plans and providers under the right of access in less time—Non-internet-based method.	1 min. and 48 sec. x Medical Records Specialists time ($54.60) = $1.64	25.0% of 24,108,000 access requests = 6,027,000	$9.87
Total Annual Recurring Administrative Costs			**$40.06**

[a] Discrepancies in total result from rounding.

Prohibition on Conditioning Provision of PHI Through a Personal Health Application (''personal health app'') on a Written Agreement

The Department considered adding a provision that would expressly prohibit covered entities from conditioning an individual's ability to access electronic copies of their PHI using a personal health app upon a separate writing, such as a user agreement or signature. The Department did not finalize such a provision because we believe that such prohibition is unnecessary. By modifying 45 CFR 164.524(c)(2)(ii), we clarify that when the individual requests an electronic copy of their PHI through a secure, standards-based Application Programming Interface (API) via a personal health app and the requested PHI is readily producible in such form and format, a covered provider must provide the requested access. This modification, coupled with the new prohibition against the imposition of unreasonable measures that impede an individual's access when a less burdensome measure is available and practicable for the entity, serves the same purpose as the considered prohibition.

The Department acknowledges the comments that express concerns about the security of personal health apps and the liability that could attach to a covered entity for failing to comply with HIPAA security provisions. Commenters also expressed concerns about the limitations of the Department's authority with respect to personal health apps and other persons that are not covered entities or business associates of covered entities.

The Department believes that individuals have a right of access to their own PHI subject only to the exceptions in the Privacy Rule.[792] While the Security Rule obligates covered entities, including health care providers, to ensure the confidentiality, integrity, and availability of any ePHI they transmit, covered entities also have an obligation to comply with the right of access without unduly or unnecessarily encumbering the right. Under the right of access, an individual may request a covered entity to transmit their ePHI to a personal health app in an unsecure manner or through an unsecure channel because the Security Rule addresses the level of risk to the security of the PHI on the covered entity's electronic information systems in responding to requests for access.[793] It does not

[792] *See* 45 CFR 164.524(a)(1).

[793] *See* ''Do individuals have the right under HIPAA to have copies of their PHI transferred or transmitted to them in the manner they request, even if the requested mode of transfer or transmission is unsecure?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #2060 (June 24, 2016), *https://www.hhs.gov/hipaa/for-professionals/faq/2060/do-*

Continued

address the level of privacy or security risks to the PHI once it has left the covered entity's electronic information systems.[794] For example, as discussed elsewhere in this final rule and consistent with the information blocking regulations, an individual may request that their unencrypted ePHI be transmitted to an app in an unsecure manner or through an unsecure channel. In such circumstances, the covered entity may consider informing the individual of the potential risks involved when the individual makes the request.[795]

Limiting Readily Producible Electronic Form And Format to That Required By Federal Law

The Department considered finalizing a provision deeming PHI readily producible to an individual who requests access to PHI in a particular electronic form and format based on Federal law only, and not state law. If adopted, to the extent that a state law requires the provision of ePHI in a particular form or format, such a requirement under state law would not automatically result in the ePHI being considered readily producible under the Privacy Rule right of access provisions. The Department determined that such an approach would cause confusion for covered entities and individuals, particularly for covered entities that operate in multiple states. Accordingly, we are not adopting this approach. The facts and circumstances of a covered entity's actions would be considered in any investigation into an individual's complaint alleging a violation of the right of access requirements. This includes circumstances where a state law requires a covered entity to provide PHI in a particular form and format requested by an individual, electronic or otherwise, and the covered entity declines to provide PHI to individuals in that form and format.

Issue Interim Guidance To Clarify That a Business Associate Agreement Is Not Required To Disclose PHI to TRS Providers

The Department considered issuing interim guidance to clarify that a business associate agreement is not required to disclose PHI to TRS providers. The Department has a longstanding FAQ that states that pursuant to 45 CFR 164.510(b), PHI can be shared during a telephone communication using a TRS provider because the individual will have an opportunity to agree or object to disclosures of PHI to the communication assistant.[796] For example, when the individual initiates the call through the TRS, it is reasonable for a covered health care provider to infer from these circumstances that the individual has identified the communication assistant as involved in the individual's care, and that the individual does not object to the disclosure.[797] The Department declined to issue such interim guidance because we believed that soliciting public comment on this issue via informal rulemaking would be helpful, even if not legally necessary.[798]

B. E.O. 14192

Section 4(a) of E.O. 14192 [799] stipulates that for regulations that increase incremental costs, the Department must identify offsetting regulations and provide the agency's best approximation of the total costs or savings associated with each new or repealed regulation. Section 3(c) requires any new costs associated with new regulations to be offset by the elimination of existing costs associated with at least 10 prior regulations, to the extent permitted by law.

Table 2 above shows that this is a deregulatory rule: cost savings exceed corresponding costs in each year (including the first, despite most costs being incurred only in the first year) and over 5 years at any discount rate. The Department calculates that this final rule generates $0.54 billion in net annualized savings at a 7 percent discount rate over a perpetual time horizon, in 2025 dollars.

TABLE 20—EO 14192 SUMMARY TABLE (2025 MILLION DOLLARS OVER AN INFINITE TIME HORIZON)[a]

Item	Primary Estimate (7%)
Present Value of Costs	$1,637,535,460
Present Value of Cost Savings	9,307,265,133
Present Value of Net Costs	-7,669,729,673
Annualized Costs	114,627,482
Annualized Cost Savings	651,508,559
Annualized Net Costs	-536,881,077

a. Showing values as of January 1, 2024, as is required when the first year of costs and cost savings is the year starting January 1, 2027. *See* "Accounting Methods under Executive Order 14192," Office of Information and Regulatory Affairs, Office of Management and Budget (last accessed Aug. 21, 2026), https://www.reginfo.gov/public/pdf/eo14192/Accounting_Methods_under_EO_14192.pdf.

individuals-have-the-right-under-hipaa-to-have/index.html.

[794] *See* 45 CFR 164.524(a)(1), (c)(2)(ii), and (c)(3)(ii).

[795] *See* 85 FR 25642, 25814 (May 1, 2020) (discussing how a covered entity that also meets the definition of an "actor" at 45 CFR 171.102 may provide individuals with such information).

[796] "When a covered entity, such as a doctor, uses a certified Telecommunications Relay Service to contact patients with hearing or speech impairments, is the Relay Service a business associate of the doctor?," *supra* note 364.

[797] *Id.; see also* 45 CFR 164.510(b)(2)(iii).

[798] 5 U.S.C. 553(c) (stating that interested persons must be given an opportunity to "participate in the rulemaking through submission of written data, views, or arguments").

[799] 90 FR 9065 (Feb. 6, 2025).

C. Regulatory Flexibility Act

The Department has examined the economic implications of this final rule as required by the RFA.[800] The Department generally considers a final rule to have significant economic impact on a substantial number of small covered entities if it generates a change in revenues of 3 percent or more for at least 5 percent of small covered entities.[801]

We published an initial assessment of the potential economic implications of the 2021 Privacy Rule NPRM in Section C., RFA, and a factual basis for certifying that the proposed rule would not result in a significant negative impact on a substantial number of small entities. We received no public comments on the small entity analysis or proposed certification under the RFA. We received several comments about the reduced burden resulting from the removal of the requirement for direct treatment providers to make a good faith effort to obtain an acknowledgment of receipt of the NPP and the addition of the permission for disclosures to certain third parties for individual-level care coordination and case management activities that constitute treatment or health care operations. We also received several comments that the number of simultaneous changes needed to update policies and procedures during the coronavirus disease 2019 public health emergency would be overly burdensome for small entities, particularly sole provider practices, such that more time and additional guidance from the Department would be needed to comply. In response to these comments and input from other Federal agencies, we have reconsidered certain aspects of the RFA analysis, including the scope of effects that may be relevant to certification. In this revised analysis, we include a comparison of the average costs by firms with employees (across all firm sizes) and the average yearly revenue of the smallest firms in each industry category that is potentially affected by this final rule. Generally, this approach likely would overestimate any economic effect on small entities because we also expect that the costs would be roughly proportional to entity size. For example, the cost to revise policies and procedures and revise training (representing more than 80 percent of costs in the first year, see Table 13) increases significantly as revenue increases because we assume that only larger businesses will incur expenses for lawyers' time for the revisions and training experts' time to revise training materials. We do not anticipate that small businesses with less than $100,000 in annual revenue will pay for tailor-made revisions to policies and training programs. Instead, we expect that they will adapt resource materials or tools offered by professional and trade associations and free government resources, such as the model NPP, in a manner suitable to their business. Even with these assumptions, we do not identify a significant economic impact on a substantial number of small entities in the smallest revenue categories. These findings also are generalizable to small entities in larger revenue categories (*e.g.,* firms with annual revenues between $100,000 and $500,000), which will have a lower cost-to-revenue ratio than the cost-to-revenue for the smallest entities. The ratio will be lower because the average costs are the same for smaller entities within the category as they are for the larger entities, but the actual revenue increases for the larger entities. This final regulatory flexibility analysis explains the factual basis for certifying the final rule under the RFA.

In addition to the statistical analysis that follows, the Department believes that the smallest of the small entities will be affected most directly by the final rule's reduced time period for responding to access requests because such entities generally do not have dedicated workforce members (or a business associate) to respond to requests for PHI. However, based on their size, we believe that such entities will receive few requests for access even if the cost per request is larger, and thus, will experience a negligible effect (lower than the effect estimated in this section) because the effect of the change is proportional to entity size. For purposes of the RFA, small entities include small businesses, nonprofit organizations, and small governmental jurisdictions. The Act defines ''small entities'' as (1) a proprietary firm meeting the size standards of the Small Business Administration (SBA), (2) a nonprofit organization that is not dominant in its field, and (3) a small government jurisdiction of less than 50,000 population. Because 90 percent or more of all health care firms meet the definition of small entities,[802] the Department generally treats all health care providers as small entities for purposes of performing a regulatory flexibility analysis. The SBA size standard for health care providers ranges between $9 million and $47 million in annual receipts, depending upon the type of entity.[803]

With respect to health insurers (NAICS code 524114), the SBA size standard is a maximum of $47 million in annual receipts, and for third party administrators (NAICS code 524292) it is $45.5 million.[804] While some insurers are classified as nonprofit, they may be dominant in their market. For example, many Blue Cross/Blue Shield insurers are organized as nonprofit entities; yet, they dominate the health insurance market in the states where they are licensed.

Table 21 provides an estimated count of affected small entities that have employees—which represent about 97 percent of all covered entities that are employer firms and affected by the final rule, but generate only 15.7 percent of total revenues).

[800] 5 U.S.C. 601–612.

[801] *See* 81 FR 31463 (May 18, 2016); *see also* 87 FR 47906 (Aug. 4, 2022).

[802] Specifically, of the 575,275 firms that are covered entities, an estimated 556,246 are small entities. ''2022 Statistics of U.S. Businesses (SUSB) Annual Data Tables by Establishment Industry,'' *supra* note 741, shows that 96.6 percent of the Health Care and Social Assistance (NAICS Sector 62) firms in Table 6 are small by SBA size standards, and the establishments owned by these small firms account for 73.8 percent of the Sector 62 establishments listed in Table 6. In addition, some large firms/establishments may be nonprofit organizations, thereby increasing the percentage of entities who are either small or nonprofit.

[803] *See* ''Small Business Size Standards by NAICS Industry,'' U.S. Small Business Administration (Mar. 17, 2023), 13 CFR 121.201 The $9 million SBA size standard applies to dentists and chiropractors, among others; the $47 million SBA size standard applies to hospitals.

[804] *Id.*

TABLE 21—ESTIMATED COUNTS OF SMALL COVERED ENTITIES

NAICS code	Type of entity	Firms	SBA small size threshold ($ million)	Small firms as % of all firms[a]	Small firms[b]	Small firm share of industry revenues
524114	Direct Health and Medical Insurance Carriers	1,071	$47.0	74.4%	797	0.1%
524292	Third Party Administrators	431	$45.5	89.3%	385	2.3%
622	Hospitals	3,136	$47.0	41.2%	1,292	1.5%
44611	Pharmacies and Drug Stores	18,857	$37.5	97.8%	18,442	21.2%
6211-6213	Office of Drs. & Other Professionals	431,216	$9.0 - $16.0	98.2%	423,454	42.3%
6215	Medical and Diagnostic Laboratories	9,025	$19.0 - $41.5	91.6%	8,267	22.1%
6214	Outpatient Care Centers	28,324	$19.0 - $47.0	90.4%	25,605	21.1%
6219	Other Ambulatory Health Care Services	11,317	$20.5 - $40.0	95.3%	10,785	22.9%
623	Nursing and Residential Care Facilities	43,215	$16.0 - $34.0	92.2%	39,844	42.4%
6216	Home Health Care Services	28,198	$19.0	95.5%	26,929	31.6%
532283	Home Health Equipment Rental	485	$41.0	91.9%	446	18.6%
Total		**575,275**		**96.6%**	**556,246**	**15.7%**

[a] Estimated using Census SUSB data by revenue size classes. *See* "2022 Statistics of U.S. Businesses (SUSB) Annual Data Tables by Establishment Industry," *supra* note 741.
[b] *Id.*

Table 22 demonstrates that more than 5 percent of small covered entities that are employer firms in each relevant NAICS category have annual revenues below $100,000 [805] with the exception of Pharmacies and Drug Stores (NAICS 446111).[806] Thus, the analysis relies on data for this set of firms to evaluate whether the final rule has an estimated effect of more than 3 percent on covered entity firms with employees.

BILLING CODE 4153–01–P

[805] This is the small revenue size class in Census' public SUSB dataset.

[806] The next revenue size class groups firms with at least $100,000 in annual revenues but below $500,000. For NAICS 446111, this revenue size class accounts for 9.4 percent of the total 18.4 thousand small covered entities (the average annual revenue in this class is $292,526).

TABLE 22—ESTIMATED COUNTS OF SMALL COVERED ENTITIES IN THE SMALLEST REVENUE SIZE CLASS

NAICS code	Type of entity	Firms with annual revenue below $100,000 (2022 dollars)[a]	Firms with annual revenue below $100,000 (2022 dollars) as % of total small firms[b]	Average annual revenue (2025 dollars)[c]	3% of average annual revenue (2025 dollars)[d]	Estimated first year cost per firm[e]	Estimated annualized (at 7%) cost per firm[f]
524114	Direct Health and Medical Insurance Carriers	157	19.7%	$58,022	$1,741	$925	$298
524292	Third Party Administrators	43	11.1%	$56,292	$1,689	$933	$300
622	Hospitals	68	5.0%	$51,988	$1,560	$925	$298
44611	Pharmacies and Drug Stores	560	3.0%	$55,681	$1,670	$927	$298
6211-6213	Office of Drs. & Other Professionals	55,947	13.2%	$57,801	$1,734	$926	$298
6215	Medical and Diagnostic Laboratories	1,097	13.1%	$54,741	$1,642	$925	$298
6214	Outpatient Care Centers	3,384	13.0%	$54,755	$1,643	$928	$299
6219	Other Ambulatory Health Care Services	1,357	12.6%	$51,822	$1,555	$925	$298
623	Nursing and Residential Care Facilities	4,449	10.8%	$48,773	$1,463	$927	$298
6216	Home Health Care Services	6,361	23.6%	$40,023	$1,201	$926	$298
532283	Home Health Equipment Rental	33	7.4%	$56,063	$1,682	$925	$298
Total		**73,217**	**13.2%**			**$926**	**$298**

[a] Estimated using Census SUSB data by revenue size classes. *See* "2022 Statistics of U.S. Businesses (SUSB) Annual Data Tables by Establishment Industry," *supra* note 741. 2022 is the most recent data available.
[b] *Id.*
[c] Average in 2022 dollars inflated using 2022-2025 GDP deflator (+9.279 percent).
[d] *Id.*
[e] First year cost per firm = (cost /establishment) * (establishments / firm).
[f] Annualized cost per firm (discounted at 7 percent) = (cost /establishment) * (establishments / firm).

BILLING CODE 4153–01–C

Table 2 provides the data to explain that, before accounting for cost savings, the average estimated cost per covered entity establishment [807] is $925 in the first year ($783.98 million divided by 847,506) and $113 in the following years ($95.37 million divided by 847,506), or $298 in annualized cost at a 7 percent discount rate. After multiplying the costs per establishment by establishments per firm within the SUSB categories, the average cost per small firm increases slightly in the first year (from $925 to $926, see Table 22) and remains unchanged at $298 (because of rounding) in annualized terms (at 7 percent discount rate). More than 5 percent of the small covered entities listed under the NAICS codes in Table 6 are one-establishment firms with annual revenues below $100,000, so the analysis must determine how the effects of the quantified costs on one-establishment firms compare to their revenues. Only small firms whose revenues are below $30,833 [=$925/0.03] could experience an effect exceeding 3 percent in the first year, and none of the small firms with employees are affected to that extent. On an annualized basis, only small firms with annualized revenues below $9,933 [=$298/0.03] could experience an effect exceeding 3 percent.

The Department acknowledges that there may be very small firms—namely 1.5 million firms without employees [808]—with revenues below $30,833; however, a number of these firms are not covered entities because they do not engage in covered electronic transactions. For example, many established solo practitioners rely on private pay patients. As another example, very small providers who accept Medicare are not subject to electronic claims filing requirements.[809] We have relied on the principle of scalability throughout the rule, and expect that small entities will adopt less expensive and less complex privacy measures that comply with the rule than the measures adopted by large entities. For the lowest-revenue nonemployer firms that are covered entities, we believe that they will comply with the regulation by adapting resource materials or tools offered by professional and trade associations and free government resources, such as the model NPP, as suitable to their business. These considerations, combined with the analysis of employer firms, support the Department's conclusion that the final rule does not generate a change in revenues of more than 3 percent for at least 5 percent of small covered entities on an annualized basis for any of the relevant NAICS.

The data in Table 2 is used to calculate cost savings that already exceed costs in the first year—the average annual cost saving per covered entity is $17—and more substantially so in the following years after non-recurring costs are no longer incurred—the average annual cost savings per covered entity is $829 in year two and onward. The Department acknowledges that the cost savings vary based on the number of health care encounters, which means that the average cost savings figure may overestimate the cost savings of the smallest of the small business firms. However, because small businesses represent 96.6 percent of covered entities, the average (small) covered entity will experience net savings each year.

The Department also recognizes that even when cost savings have an economically significant effect—as it is the case for this final rule—net cost savings do not necessarily imply certification. However, the average (small) covered entity with employees will experience net savings each year, and, as explained above, we believe nonemployer firms will not incur net costs above the 3 percent of annual revenue; thus, the effects on the average small business would support certification in this instance. Accordingly, available data allow the Department to carry out sufficiently high-quality fact-based analysis (as shown above) to support certification. Thus, the Secretary certifies that this final rule will not negatively affect a substantial number of small entities.

D. Unfunded Mandates Reform Act

Section 202(a) of the UMRA requires the Department to prepare a written statement, including an assessment of anticipated costs and benefits, before issuing ''any rule that includes any Federal mandate that may result in the expenditure by state, local, and tribal governments, in the aggregate, or by the private sector, of $100,000,000 or more (adjusted annually for inflation) in any one year.'' [810] In 2025 dollars, that threshold is $193 million.[811] The Department does not anticipate that this final rule will have an effect only on state, local, or Tribal governments, in the aggregate that exceed this threshold; however, it may impose mandates on the private sector that will exceed this threshold in the first year of its effective date. Thus, we have prepared an analysis of the costs and benefits of the final rule.

E. E.O. 13132—Federalism

E.O. 13132 establishes certain requirements that an agency must meet when it promulgates a final rule (and preceding proposed rule) that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. The Department does not believe that this rulemaking will have any implications for federalism.

The federalism implications of the Privacy Rules were assessed as required by E.O. 13132. That assessment was published as part of the preambles to the final rules in 2000,[812] 2003,[813] and 2013.[814] Regarding preemption, the preamble to the 2013 Privacy Rule explains that the HIPAA statute dictates the relationship between state law and Privacy Rule requirements, and therefore the Rule's preemption provisions do not raise federalism issues. The HITECH Act provides that HIPAA's preemption provisions also apply to the HITECH Act.[815]

The Department anticipates that the most significant direct costs on state and local governments will be the cost for state and local government-operated covered entities to revise policies and procedures, including drafting, printing, and distributing NPPs for individuals with first-time health encounters, which will include the cost of mailing these notices for state health plans, such as Medicaid. The RIA above addresses these costs in detail.

In considering the principles in and requirements of E.O. 13132, the

[807] Firms and establishments represent different levels of aggregation. A firm can have one or more establishments, with larger firms (by employees, or by revenues) typically having multiple establishments and small firms typically having one establishment. The Department estimated costs using number of establishments to account for larger firms having higher costs. The per-establishment cost is an estimate of the cost for a small, one-establishment firm. Thus, for the analysis in this section, the Department's estimated cost per covered entity establishment is the Department's estimate of costs for a small covered entity firm.

[808] *See* U.S. Census Bureau, Nonemployer Statistics (NES), 2022, *https://www.census.gov/programs-surveys/nonemployer-statistics.html.* The Department uses 2022 data or consistency with SUSB data in Table 6.

[809] *See* 42 CFR 424.32.

[810] Public Law 104–4, 109 Stat. 64 (Mar. 22, 1995) (codified at 2 U.S.C. 1532).

[811] Aaron Kearsley, ''HHS Standard Values for Regulatory Analysis, 2026,'' Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services (Mar. 10, 2026), *https://aspe.hhs.gov/reports/standard-ria-values.*

[812] 65 FR 82462, 82797–98 (Dec. 28, 2000).

[813] 68 FR 8334, 8373 (Feb. 20, 2003).

[814] 78 FR 5566, 5686 (Jan. 25, 2013).

[815] *See* Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111–5, 123 Stat. 226, sec. 13421(a) (Feb. 17, 2009) (codified at 42 U.S.C. 201 note).

Department has determined that these modifications to the Privacy Rule will not significantly affect the rights, roles, and responsibilities of the states.

F. Assessment of Federal Regulation and Policies on Families

Section 654 of the Treasury and General Government Appropriations Act of 1999 requires Federal departments and agencies to determine whether a policy or regulation could negatively affect family well-being.[816] If the determination is affirmative, then the Department or agency must prepare an impact assessment to address criteria specified in the law. The Department does not anticipate negative effects on family well-being from this regulation.

G. Paperwork Reduction Act of 1995

The PRA [817] requires the Department to submit to the OMB for review and approval any reporting or record-keeping requirements inherent in a proposed or final rule, and to publish such proposed requirements for public comment. To fairly evaluate whether an information collection should be approved by the OMB, section 3506(c)(2)(A) of the PRA requires that the Department solicit comment on all of the following issues:

- Whether the information collection is necessary and useful to carry out the proper functions of the agency.
- The accuracy of the agency's estimate of the information collection burden.
- The quality, utility, and clarity of the information to be collected.
- Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

The PRA requires consideration of the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section.

In this RIA, the Department is revising certain information collection requirements associated with this final rule after consideration of the comments on the 2021 Privacy Rule NPRM and comments on the 2022 Part 2 NPRM that addressed certain proposed modifications to the Privacy Rule and, as such, is revising the information collection last prepared in 2024 and approved under OMB control #0945–0003. The revised information collection describes all new and adjusted information collection requirements for covered entities pursuant to the implementing regulation for HIPAA at 45 CFR parts 160 and 164, the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (''HIPAA Rules'').

The estimated annual labor burden presented by the regulatory modifications in the first year of implementation, including nonrecurring and recurring burdens, is 6,464,621 burden hours at a cost of $770,757,757, and $95,194,170 of estimated annual recurring labor costs in years two through five. The estimated annual capital costs burden presented by the regulatory modifications in the first year of implementation, including nonrecurring and recurring burdens, is $13,221,725 and $180,513 recurring capital costs in years two through five. Estimated annual costs savings of $798,126,000 reduce annual burdens, resulting in first year net cost savings of $14,146,519; net annual cost savings are $702,751,317 in years two through five.

The overall total burden for respondents to comply with the information collection requirements of all of the HIPAA Rules, including nonrecurring and recurring burdens presented by program changes, previously unrecognized burdens, and reduced burdens resulting from a court decision, is 984,129,331 burden hours at a labor cost of $121,661,926,211, plus $148,540,234 in capital costs, for a total estimated annual burden of $121,810,466,445 in the first year following the effective date of the final rule. Details describing the burden analysis for the proposals associated with this RIA are presented below and explained further in the Information Collection Request (ICR) associated with this final rule.

Explanation of Estimated Annualized Burden Hours

Below is a summary of the significant program changes and adjustments made since the ICR was approved in 2024. Because the ICR addresses regulatory burdens associated with the full suite of HIPAA Rules, the changes and adjustments include updated data and estimates for some provisions of the HIPAA Rules that are not affected by this final rule. These program changes and adjustments form the bases for the burden estimates presented in the ICR associated with this RIA.

Adjusted Estimated Annual Burdens of Compliance

- Increasing the number of covered entities (*i.e.,* respondents) from 774,331 to 847,506 based on program change.
- Increasing the multiplier for the annual number of individual access requests for copies of PHI requiring labor (through non-internet-based method) from 615,000 to 4,802,000 based on program change.
- Adding a previously unrecognized recurring labor burden of 18 hours per covered entity for determinations of the minimum necessary PHI for treatment, payment, and health care operations.
- Adding a previously unrecognized recurring burden of 3 minutes per request pursuant to the right of access to direct by separately enumerating requests to direct copies to a person other than a health care provider or health plan and requests to direct copies to a health care provider or health plan as follows:
  - Adding an estimate of 6,027,000 annual requests under the right of access to direct for copies of ePHI sent to health care providers and health plans based on program change, resulting in 301,350 burden hours.
  - Adding an estimate of 14,046,078 annual requests under the right of access to direct for copies of ePHI sent to persons designated by the individual other than health care providers and health plans based on program change, resulting in 702,304 burden hours.
- Updating capital costs for sheets of paper, toner for printing, envelopes, and postage using the values in this final rule.
- Removing a nonrecurring burden of 1 hour for updating each of 350,000 business associate agreements that applied to changes in the first year of implementing the 2024 Privacy Rule that has already passed.

Reductions in Burden Resulting From Program Change

This final rule decreases the estimated hourly burden for disseminating the NPP and obtaining an acknowledgment of receipt pursuant to 45 CFR 164.520, from 3 minutes to 1 minute and 15 seconds as a result of program change.

New Burdens From Program Changes

In addition to burden reductions and updated data, the Department added new estimated burdens as a result of program changes in the final rule:

- A burden of 1 minute and 15 seconds for each of 4,245,996 NPPs that will be disseminated to individuals who are inmates within the first year of compliance with the final rule, and an

[816] *See* Public Law 105–277, div. A, sec. 101(h), 112 Stat. 2681, 2681–480, 2681–528 (Oct. 21, 1998), as amended by Public Law 108–271, sec. 8(b), 118 Stat. 814 (July 7, 2004) (codified at 5 U.S.C. 601 note).

[817] Public Law 104–13, 109 Stat. 163 (May 22, 1995) (codified at 44 U.S.C. 3501–3521).

annual burden of 1 minute and 15 seconds for each of 3,026,662 NPPs that will be disseminated to individuals who are inmates in years two through five.

- A nonrecurring burden of 60 minutes per covered entity to update the required content of its NPP.
- A nonrecurring burden of 15 minutes per covered entity for posting an updated NPP online pursuant to 45 CFR 164.520.
- A nonrecurring burden of 15 minutes per covered entity for posting a fee schedule for copies of PHI online pursuant to 45 CFR 164.525.
- A nonrecurring burden of 30 minutes for 5 percent of covered entities to update policies and procedures related to identity verification pursuant to 45 CFR 164.530 and 2 hours and 10 minutes for all covered entities to update the remainder of updated policies and procedures under 45 CFR 164.530 (excluding updating NPP content, listed separately above).
- A nonrecurring burden of 10 minutes for 5 percent of covered entities to update HIPAA training related to changes in identity verification procedures pursuant to 45 CFR 164.530 and 2 hours and 20 minutes for all covered entities to update training for the remainder of updated policies and procedures.
- A nonrecurring burden of 5 minutes for a medical records specialist who is a workforce member of each covered entity to receive additional training on changes to the right of access.
- A nonrecurring burden for mailing an updated NPP to a percentage of health plan subscribers at a rate of 240 notices per hour pursuant to 45 CFR 164.520.
- An increase in the recurring burden for each of an estimated 4,802,000 individual access requests by 1 minute for covered entities to account for providing access within a shorter time pursuant to 45 CFR 164.524.
- A recurring burden of 1 minute for each of an estimated 14,046,078 requests pursuant to the right of access to direct that are for sending copies to a designated person other than a health care provider or health plan though a non-internet-based method within a shorter time period pursuant to 45 CFR 164.524.
- A recurring burden of 1 minute for each of an estimated 6,027,000 requests pursuant to the right of access to direct that are for sending copies to a health care provider or health plan through a non-internet-based method within a shorter time period pursuant to 45 CFR 164.524.
- A recurring burden of 7 minutes for each of an estimated 6,130,000 requests by individuals to discuss the NPP pursuant to 45 CFR 164.520.

Reductions in Burden Resulting From Court Decision

The court in *Carmen Purl* v. *U.S. Department of Health & Human Services,*[818] vacated the attestation requirement introduced in the 2024 Privacy Rule at 45 CFR 164.509, which had added an estimated 235,125 recurring burden hours. To reflect the effects of the court's decision the ICR will show the following burden reductions:

- Removing entirely a burden of 5 minutes per request for certain copies of PHI for workforce members to determine whether an attestation is required for disclosure pursuant to 45 CFR 164.509.
- Removing entirely a burden of 1 hour per request for legal review of certain requests identified by workforce members as potentially pertaining to the lawfulness of reproductive health care pursuant to 45 CFR 164.509.
- Removing entirely a burden of 3 hours per request for a percentage of requests requiring legal review that might require additional manager review pursuant to 45 CFR 164.509.

List of Subjects

45 CFR Part 160

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health professions, Health records, Hospitals, Investigations, Medicaid, Medical research, Medicare, Penalties, Preemption, Privacy, Public health, Reporting and recordkeeping requirements, Security.

45 CFR Part 164

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health professions, Health records, Hospitals, Medicaid, Medical research, Medicare, Privacy, Public health, Reporting and recordkeeping requirements, Security.

For the reasons stated in the preamble, the Department of Health and Human Services amends 45 CFR subtitle A, subchapter C, parts 160 and 164 as set forth below:

[818] *Purl,* 87, F. Supp. 3d 284.

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

■ 1. The authority citation for part 160 is revised to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d–1320d–9; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)); 5 U.S.C. 552; secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279 (42 U.S.C. 17921, 17931–17954); and sec. 1104 of Pub. L. 111–148, 124 Stat. 146–154.

■ 2. Amend § 160.103 by adding a new paragraph (4)(v) to the definition of ''Business associate'' to read as follows:

§ 160.103 Definitions.

* * * * *

Business associate * * *

(4) * * *

(v) A provider of telecommunications relay services, as defined in 47 U.S.C. 225(a)(3), with respect to enabling communications through services regulated under 47 CFR part 64.

* * * * *

PART 164—SECURITY AND PRIVACY

■ 3. The authority citation for part 164 is revised to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d–1320d–9; sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)); and secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279 (42 U.S.C. 17921, 17931–17954).

■ 4. Amend § 164.501 by:

■ a. Adding in alphabetical order a definition for ''Electronic health record'';

■ b. Revising and republishing the definition of ''Health care operations''; and

■ c. Adding in alphabetical order a definition for ''Personal health application''.

The additions and revision read as follows:

§ 164.501 Definitions.

* * * * *

Electronic health record means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. Such clinicians shall include, but are not limited to, health care providers that have direct or indirect treatment relationships with individuals as defined at § 164.501, such as physicians, nurses, pharmacists, and other allied health professionals. For purposes of this definition, ''health-related information on an individual'' covers the same scope of information as the term *individually identifiable health*

information as defined at § 160.103 of this subchapter.

* * * * *

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable.

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.

(6) Business management and general administrative activities of the entity, including, but not limited to, any of the following:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter.

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances.

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity.

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

* * * * *

Personal health application means an electronic application used by an individual to access health information about that individual, which can be drawn from multiple sources, provided that all of the following conditions apply:

(1) Such information is managed, shared, and controlled by or primarily for the individual.

(2) Such information is not managed, shared, or controlled in any of the following manners:

(i) By or primarily for a covered entity.

(ii) Primarily for another person.

* * * * *

■ 5. Amend § 164.502 by:
■ a. Revising paragraph (a)(2);
■ b. Revising paragraph (a)(4)(ii);
■ c. Redesignating paragraphs (a)(5)(ii)(B)(*2*)(*vii*) and (a)(5)(ii)(B)(*2*)(*viii*) as (a)(5)(ii)(B)(*2*)(*viii*) and (a)(5)(ii)(B)(*2*)(*ix*), respectively; and
■ d. Adding paragraph (a)(5)(ii)(B)(*2*)(*vii*).

The revisions and addition read as follows:

§ 164.502 Uses and disclosures of protected health information: General Rules.

(a) * * *

(2) *Covered entities: Required disclosures.* A covered entity is required to disclose protected health information in each of the following circumstances:

(i) To an individual, when requested under, and required by, § 164.524 or § 164.528.

(ii) To a person designated by the individual, when requested under, and required by, § 164.524.

(iii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

* * * * *

(4) * * *

(ii) To the covered entity or, when specified in the written contract or other written arrangement with a business associate required by § 164.502(e)(2), to the individual or the individual's designee, as necessary to satisfy a covered entity's obligations with respect to § 164.524(c)(2)(ii) or § 164.524(d)(1).

(5) * * *

(ii) * * *

(B) * * *

(*2*) * * *

(*vii*) To a person designated by an individual, when requested under § 164.524;

* * * * *

■ 6. Amend § 164.506, by adding new paragraph (c)(6) to read as follows:

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

* * * * *

(c) * * *

(6) A covered entity may disclose an individual's protected health information to a social services agency, community-based organization, home and community based services provider, or similar third party that provides health or human services to specific individuals, for individual-level care coordination and case management activities (whether such activities constitute treatment or health care operations as those terms are defined in § 164.501) with respect to that individual.

* * * * *

■ 7. Amend § 164.512 by:
■ a. Revising paragraph (d)(3);
■ b. Revising the heading for paragraph (k)(1);
■ c. Revising and republishing paragraphs (k)(1)(i) and (ii);
■ d. Revising paragraph (k)(2); and
■ e. Adding paragraph (m).

The revisions and addition read as follows:

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

* * * * *

(d) * * *

(3) *Joint activities or investigations.* Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity

for purposes of paragraph (d) of this section.

* * * * *

(k) * * *

(1) *Uniformed Services and veterans activities*—(i) *Uniformed Services personnel.* A covered entity may use and disclose the protected health information of individuals who are Uniformed Services personnel for activities deemed necessary by appropriate command authorities to assure the proper execution of the applicable Uniformed Service's mission, if the appropriate command authority has published by notice in the **Federal Register** all of the following information:

(A) Appropriate command authorities.

(B) The purposes for which the protected health information may be used or disclosed.

(ii) *Separation or discharge from Uniformed Service.* A covered entity that is a component of the Departments of Defense, Homeland Security, Commerce, or Health and Human Services may disclose to the Department of Veterans Affairs (VA) the protected health information of an individual who is a member of the Uniformed Service upon the separation or discharge of the individual from Uniformed Service for the purpose of a determination by the VA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

* * * * *

(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 3001, *et seq.*) and implementing authority (*e.g.,* Executive Order 12333).

* * * * *

(m) *Standard: Disclosures to Telecommunications Relay Services.* (1) A covered entity may disclose protected health information to a Telecommunications Relay Service Communications Assistant, as defined at 47 CFR 64.601(a)(12), as necessary to conduct covered functions.

(2) Notwithstanding § 164.502(a)(3), a business associate may disclose protected health information to a Telecommunications Relay Service Communications Assistant, as defined at 47 CFR 64.601(a)(12), as necessary to conduct covered functions for or on behalf of a covered entity.

* * * * *

■ 8. Amend § 164.514 by adding paragraph (h)(2)(v).

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

* * * * *

(h) * * *

(2) * * *

(v) *Exercise of individual rights.* A covered entity may not impose unreasonable verification measures on an individual that would impede the individual from exercising a right under this part. An unreasonable measure is one that causes an individual to expend unnecessary effort or resources when a less burdensome verification measure is practicable for the covered entity. Practicability considerations include a covered entity's technical capabilities, its obligations to protect the privacy of protected health information under § 164.530(c) and the security of electronic protected health information under § 164.306, and the costs of implementing measures that are more convenient for individuals.

■ 9. Amend § 164.520 by:

■ a. Revising paragraph (a)(1);

■ b. Removing paragraph (a)(4);

■ c. Revising paragraphs (b)(1)(i), (b)(1)(iii)(B), (b)(1)(iv)(C), (b)(1)(iv)(E), and (b)(1)(iv)(F);

■ d. Adding paragraph (b)(1)(iv)(G);

■ e. Revising paragraph (b)(1)(vii);

■ f. Adding paragraph (b)(2)(iii);

■ g. Removing paragraph (c)(2)(ii);

■ h. Redesignating paragraphs (c)(2)(iii) and (iv) as paragraphs (c)(2)(ii) and (iii), respectively;

■ i. Revising paragraph (c)(3)(iii); and

■ j. Revising paragraph (e).

The revisions and additions read as follows:

§ 164.520 Notice of privacy practices for protected health information.

(a) *Standard: Notice of privacy practices*—(1) *Right to notice.* Except as provided by paragraph (a)(3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

* * * * *

(b) * * *

(1) * * *

(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed:

NOTICE OF PRIVACY PRACTICES OF [NAME OF COVERED ENTITY, AFFILIATED COVERED ENTITIES, OR ORGANIZED HEALTH CARE ARRANGEMENT, AS APPLICABLE]

THIS NOTICE DESCRIBES:

- HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED.
- YOUR RIGHTS WITH RESPECT TO YOUR HEALTH INFORMATION.
- HOW TO EXERCISE YOUR RIGHT TO GET COPIES OF YOUR RECORDS AT LIMITED COST OR, IN SOME CASES, FREE OF CHARGE.
- HOW TO FILE A COMPLAINT CONCERNING A VIOLATION OF THE PRIVACY OR SECURITY OF YOUR HEALTH INFORMATION, OR OF YOUR RIGHTS CONCERNING YOUR INFORMATION, INCLUDING YOUR RIGHT TO INSPECT OR GET COPIES OF YOUR RECORDS UNDER HIPAA.
- YOU HAVE A RIGHT TO A COPY OF THIS NOTICE (IN PAPER OR ELECTRONIC FORM) AND TO DISCUSS IT WITH [ENTER NAME, TITLE, OR OFFICE] AT [PHONE AND EMAIL] IF YOU HAVE ANY QUESTIONS.

* * * * *

(iii) * * *

(B) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the plan sponsor;

(iv) * * *

(C) The right of access to inspect and obtain a copy of protected health information at limited cost or, in some cases, free of charge; and the right of access to direct a covered entity to transmit an electronic copy of protected health information in an electronic health record to a person designated by the individual, as provided by § 164.524;

* * * * *

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528;

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request; and

(G) The right to discuss the notice with a designated contact person or office identified by the covered entity pursuant to § 164.520(b)(1)(vii).

* * * * *

(vii) *Contact.* The notice must contain the name or title, telephone number, and email address for a designated person or office responsible for providing further information and answering questions about the covered entity's privacy practices, as required by § 164.530(a)(1)(ii).

* * * * *

(2) * * *

(iii) A covered entity may provide in its notice information about how an individual who seeks to direct a copy of protected health information to another person, when the request does not meet the conditions of § 164.524(d), can instead obtain a copy of protected health information directly under § 164.524(a)-(c) and (e) and send the copy to the person themselves, or request the covered entity to send a copy of protected health information to the person using a valid authorization under § 164.508.

* * * * *

(c) * * *

(2) * * *

(ii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iii) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(ii) of this section, if applicable.

(3) * * *

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service.

* * * * *

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity.

* * * * *

■ 10. Revise and republish § 164.524 to read as follows:

§ 164.524 Access of individuals to protected health information.

(a) *Standard: Access to protected health information*—(1) *Right of access.* Except as otherwise provided in paragraphs (a)(2) or (3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for either of the following:

(i) Psychotherapy notes.

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in any of the following circumstances:

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial.* A covered entity may deny an individual access provided that the individual is given a right to have such denials reviewed, as required by paragraph (e)(4) of this section, in any of the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (e)(4) of this section.

(b) *Implementation specifications: Requests for access and timely action*—

(1) *Individual's request for access.*

(i) The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set.

(ii) The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement. For purposes of this paragraph, in writing means that the request itself serves as documentation of the individual's exercise of the right of access, including when the request is submitted electronically or on paper.

(iii) The covered entity may not impose measures on individuals making requests for access that impede an individual from obtaining access when there is a measure for making such requests that is less burdensome for the individual and practicable for the entity.

(2) *Timely action by the covered entity.*

(i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access as soon as practicable, but no later than 15 calendar days after receipt of the request, and the following conditions must be met:

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance

of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (e)(2) of this section.

(ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 calendar days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(iii) Where another federal or state law requires a covered entity to provide an individual with access to the protected health information requested in less than 15 calendar days, that shorter time period is deemed practicable for purposes of paragraph (b)(2)(i) of this section.

(c) *Implementation specifications: Provision of access.* If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Providing the access requested.* The covered entity must provide the access requested by an individual, including inspection or obtaining a copy, or both, of the protected health information about the individual in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) *Form of access requested.* (i) The covered entity must provide an individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

(iii) Where another federal or state law applicable to the covered entity requires the provision of access in a particular electronic form and format, the protected health information is deemed readily producible in such form and format for purposes of paragraphs (c)(2)(i) and (ii) of this section.

(iv)(A) The covered entity may provide an individual with a summary of the protected health information requested, in lieu of providing access to the protected health information, or may provide an explanation of the protected health information to which access has been provided, if:

(*1*) The individual agrees in advance to such a summary or explanation; and

(*2*) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(B) The covered entity must inform an individual to whom it offers to provide a summary in lieu of a copy of protected health information that the individual retains the right to obtain a copy of the requested protected health information if the individual does not agree to receive such summary. This requirement does not apply if a covered entity is offering to provide a summary in lieu of a copy of protected health information because the covered entity is denying an individual's request for a copy; however, the covered entity still must follow the denial procedures under § 164.524(e).

(3) *Time and manner of access.* The covered entity must provide the access as requested by an individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or at the individual's request, mailing or electronically transmitting the copy of the protected health information to the individual, including by email, or to or through the individual's personal health application, if a copy is readily producible to or through such application. The covered entity may discuss with an individual the scope, format, and other aspects of the individual's request for access as necessary to facilitate the timely provision of access; however, such discussion shall not extend the time allowed for the covered entity to provide access.

(4) *Fees.* (i) If an individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(A) Labor for copying the protected health information requested by the individual, whether in non-electronic (*e.g.,* paper, film) or electronic form;

(B) Supplies for creating a non-electronic copy;

(C) Postage, when the individual has requested that a non-electronic copy, or the summary or explanation, be mailed; and

(D) Labor of preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iv) of this section.

(ii) A covered entity may not impose a fee in either of the following circumstances:

(A) An individual inspects the protected health information about the individual, as described at (a)(1) of this section.

(B) An individual accesses electronic protected health information maintained by or on behalf of the covered entity using an internet-based method, such as a personal health application.

(d) *Standard: Directing an electronic copy of certain protected health information to a person designated by the individual*—(1) *Right of access to direct.* Subject to the limitations of paragraph (a)(1) of this section, and except as otherwise provided in paragraphs (d)(2) and (3) of this section, an individual has the right of access to direct a covered entity to transmit an electronic copy of protected health information about the individual (''right of access to direct'') in an electronic health record to a person designated by the individual.

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual's request to exercise the right of access to direct a covered entity to transmit an electronic copy of protected health information in an electronic health record directly to a person designated by an individual under paragraph (d)(1) of this section, without providing an opportunity for review, in the following circumstances:

(i) The protected health information is excepted from the right of access to

direct by paragraph (d)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to exercise of the right of access to direct, if transmitting such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's ability to exercise of the right of access to direct may be temporarily suspended by a covered entity in the course of research that includes treatment for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered entity has informed the individual that the right of access to direct will be reinstated upon completion of the research.

(iv) An individual's request to exercise the right of access to direct may be denied if the protected health information is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, and if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's request to exercise the right of access to direct may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and providing the copy to the person designated by the individual would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial of a request to exercise the right of access to direct.* A covered entity may deny an individual's request to exercise the right of access to direct under paragraph (d)(1) of this section, provided that the individual is given a right to have such denials reviewed, as required by paragraph (e)(4) of this section, in either of the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access is reasonably likely to endanger the life or physical safety of the individual or another person.

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access is reasonably likely to cause substantial harm to such other person.

(4) *Implementation specification: Summary or explanation prepared by covered entity.* (i) The covered entity may transmit, to a person designated by an individual pursuant to the right of access to direct, a summary of requested protected health information in an electronic health record, in lieu of transmitting a copy of the protected health information, or may transmit an explanation of the requested protected health information in an electronic health record in addition to such protected health information, if all of the following conditions apply:

(A) The individual agrees in advance to such a summary or explanation.

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(ii) The covered entity must inform an individual with respect to whose protected health information it offers to transmit a summary to a person designated by the individual in lieu of a copy of protected health information that the individual retains the right of access to direct an electronic copy of the requested protected health information in an electronic health record if the individual does not agree to direct such summary. This requirement does not apply if a covered entity is offering to provide a summary in lieu of a copy of protected health information because the covered entity is denying an individual's request to exercise the right of access to direct; however, the covered entity still must follow the denial procedures under § 164.524(e).

(5) *Implementation specification: Requests for access and timely action.* (i) *Individual's request for access.* The covered entity must permit an individual to exercise the right of access to direct where the request is clear, conspicuous, and specific. The covered entity may require individuals to make requests for such access in writing, provided that it informs individuals of such a requirement. For purposes of this paragraph, in writing means that the request itself serves as documentation of the individual's exercise of the right of access to direct, including when the request is submitted electronically or on paper.

(ii) *Timely action by the covered entity.* (A) Except as provided in paragraph (d)(5)(ii)(B) of this section, the covered entity is required to provide an electronic copy requested under paragraph (d)(1) of this section as soon as practicable, but no later than 15 calendar days after receipt of an individual's request, and the following conditions must be met:

(*1*) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (d) of this section.

(*2*) If the covered entity denies the individual's request to exercise the right of access to direct, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (e)(2) of this section.

(B) If the covered entity is unable to take an action required by paragraph (d)(5)(ii)(A)(*1*) or (*2*) of this section within the time required by paragraph (d)(5)(ii)(A) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 calendar days, provided that:

(*1*) The covered entity, within the time limit set by paragraph (d)(5)(ii)(A) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the individual's request to exercise the right of access to direct; and

(*2*) The covered entity may have only one such extension of time for action on the individual's request to exercise the right of access to direct.

(C) Where another federal or state law requires a covered entity to provide an individual with an electronic copy of the protected health information in an electronic health record in less than 15 calendar days, that shorter time period is deemed practicable for purposes of paragraph (d)(5)(ii)(A) of this section.

(e) *Implementation specifications: Denial of access.* If a covered entity denies an individual's right of access, in whole or in part, to protected health information pursuant to paragraph (a) or (d) of this section, the covered entity must comply with the following requirements.

(1) *Making other information accessible.* The covered entity must, to the extent possible, give the individual, or a person designated by the individual, access to any other protected health information requested pursuant to paragraph (a) or (d) of this section, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) *Denial.* The covered entity must provide a timely, written denial to the individual. The denial must be in plain language and contain all of the following:

(i) The basis for the denial.

(ii) If applicable, a statement of the individual's right of review under paragraph (e)(4) of this section, including a description of how the individual may exercise such right.

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306 of this subchapter. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) *Other responsibility.* If the covered entity (or its business associate on the covered entity's behalf) does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested protected health information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) *Right to review of denial.* If the individual requests a review of a denial on a ground permitted under paragraphs (a)(3) or (d)(3) of this section, the covered entity must designate a licensed health care professional who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) or (d)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(f) *Implementation specification: Documentation.* A covered entity must document all of the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to the right of access under paragraph (a) of this section.

(2) The electronic health records that are subject to the right of access to direct under paragraph (d) of this section.

(3) The titles of the persons or offices responsible for receiving and processing requests for access made pursuant to paragraphs (a) and (d) of this section.

* * * * *

■ 11. Add § 164.525 to subpart E to read as follows:

§ 164.525 Notice of access and authorization fees.

If a covered entity imposes fees for copies of protected health information requested under this subpart, the covered entity must post a fee schedule on its website, if it has one, and make the fee schedule available to individuals at the point of service and upon request. The fee schedule must specify all of the following:

(a) All types of access to protected health information available free of charge.

(b) Standard fees for all of the following copies, where the covered entity generally charges for such copies:

(1) Copies of protected health information provided under § 164.524(a) and § 164.524(d), with respect to all available electronic and non-electronic forms and formats for such copies.

(2) Copies of protected health information disclosed pursuant to the individual's valid authorization under § 164.508, with respect to all available forms and formats for such copies.

■ 12. Amend § 164.532 by revising paragraph (e) to read as follows:

§ 164.532 Transition provisions.

* * * * *

(e) *Implementation specification: Deemed compliance*—(1) *Qualification.* Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to November 19, 2026, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of § 164.314(a) or § 164.504(e) that were in effect on such date; and

(ii) The contract or other arrangement is not renewed or modified from January 19, 2027, until July 19, 2027.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after July 19, 2027; or

(ii) January 18, 2028.

(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

* * * * *

Robert F. Kennedy, Jr.,

Secretary, Department of Health and Human Services.

[FR Doc. 2026–23429 Filed 11–16–26; 4:15 pm]

BILLING CODE 4153–01–P