Proposed Rule Amending the HIPAA Privacy Rule

10-Minute Read

3/9/2021 Update: OCR extended the due date for public comments on the proposed rule to May 6, 2021.

The Office for Civil Rights (OCR) under the Department of Health and Human Services (HHS) (collectively, the Department) issued a proposed rule modifying the Privacy Rule under the Health Insurance Portability and Accountability Act (HIPAA) to support HHS' Regulatory Sprint to Coordinated Care initiative. The Privacy Rule is one of several rules that are collectively known as the HIPAA Rules that protect the privacy and security of individuals' medical records and other protected health information (PHI). PHI is individually identifiable health information maintained or transmitted by or on behalf of HIPAA covered entities (i.e., health care providers who conduct health care transactions electronically, health plans, and health care clearinghouses). The HIPAA Privacy Rule imposes federal requirements to protect PHI held by covered entities and their business associates, gives patients' rights with respect to that information, and permits covered entities and business associates to disclose PHI for patient care and other important purposes.

If finalized, this rule would take effect 60 days after any final rule is published in the Federal Register. Covered entities and their business associates would have until the "compliance date" (180 days from the effective date of any finalized changes under the rule) to establish and implement policies and practices to achieve compliance with any new or modified standards in accordance with this rule.

Public comments on the proposed rule were originally due on March 22, 2021; however, OCR extended the deadline to May 6, 2021.

Individual Right of Access to PHI

Under the Privacy Rule individuals generally have the right to access, upon request, the PHI about them in one or more designated record sets maintained by or for the individuals' covered entities. Designated record sets include medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals.

The Department proposes to modify the Privacy Rule to increase permissible disclosures of PHI and to improve care coordination and case management by:

- Adding and interpreting definitions to help clarify the proposed modifications to the right of individuals to access their PHI.
    - *Electronic health record (EHR)* 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. Clinicians include, but are not limited to, health care providers that have a direct treatment relationship with individuals, as defined at 45 CFR §164.501, such as physicians, nurses, pharmacists, and other allied health professionals. For purposes of this definition, "health-related information on an individual" would include health information collected from an individual that is created or received by a covered entity and relates to the past, present, or future physical or mental condition or payment for care of an individual that identifies the individual or can be reasonably believed that such information can be used to identify the individual.
    - *Authorized health care clinicians and staff.* The Department proposes to interpret authorized health care clinicians and staff to at least include covered health care providers who can access, modify, transmit, or otherwise use or disclose PHI in an EHR, and who have direct treatment relationships with individuals; and their workforce members who support the provision of such treatment by virtue of their qualifications or job role. Entities that do not have direct treatment relationships with individuals would not be included in an EHR. For example, the term EHR would not include health-related electronic records of covered health care providers that only supply durable medical equipment to other providers, who then provide the equipment to individuals, and thus do not have direct treatment relationships with individuals.
    - *Personal health application.* The Department proposes to define personal health application in the HIPAA Rules 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."
- Modifying provisions regarding an individual's right of access to PHI by:
    - clarifying that while an entity may require individuals to make requests for access in writing, an entity would not be permitted to do so in a way that impedes access (the proposed rule contains examples of unreasonable measures such as requiring use of a form containing unnecessary information, requiring notarization of an individual's signature, only accepting written requests in paper form, or only accepting requests at the covered entity's facility or through the covered entity's online portal).
    - prohibiting covered entities from imposing an unreasonable identity verification requirement on individuals exercising their access rights. Unreasonable verification requirements are those that require an individual to expend unnecessary effort or expense when a less burdensome verification measure is practicable for the covered entity. Proposed examples of unreasonable requirements include requiring individuals to obtain notarization of requests and requiring individuals to provide proof of identity in person when a more convenient method is practicable.

- strengthening individuals' rights to inspect their PHI in person without a fee, which would include allowing individuals to take notes, videos, and photographs, or use other personal resources (not including personal devices that connect to a covered entity's information systems, such as a thumb drive) to view and capture images of their PHI.
- shortening covered entities' required response time to individual access requests to no later than 15 calendar days (from the current 30 days) with the opportunity for an extension of no more than 15 calendar days (from the current 30-day extension). The proposed rule would also require covered entities to establish written policies for prioritizing urgent or other high priority access requests to limit the need to use the 15-calendar-day extensions for such requests. The proposed rule would clarify that a covered entity may discuss the individual's access request with the individual, but this would not extend the time limit for providing the individual with access.
- clarifying the form and format required for responding to individuals' requests for their PHI. For example, if a covered entity has chosen to implement a secure standards-based application programming interface (API), upon an individual's request, covered entities must produce "readily producible" copies of PHI including copies of electronic PHI (ePHI) through the secure standards-based API using applications chosen by individuals and copies in any form and format required by applicable state and other laws.
- requiring covered entities to inform individuals that they retain their right to obtain or direct copies of PHI to a third party when a summary of PHI is offered in lieu of a copy.
- creating a pathway for individuals to direct the sharing of PHI in an EHR among covered health care providers and health plans, by requiring covered health care providers and health plans (Requestor-Recipient) to submit an individual's access request (request can be made orally if the request is clear, conspicuous, and specific) to another health care provider (Discloser), requesting that the Discloser transmit the PHI maintained by or on behalf of the Discloser in its EHR to the Requestor-Recipient. The proposed rule would require the Requestor-Recipient to submit access requests to Discloser as soon as practicable, but no later than 15 calendar days after receiving the individual's direction and any information necessary to submit the request. The Discloser would be required to provide the requested PHI to the Requestor-Recipient as soon as practicable, but no later than 15 calendar days after receiving the request.
- specifying that covered entities cannot charge a fee for the individual's right to inspect PHI and to obtain copies of PHI about the individual except that a reasonable cost-based fee may be imposed for the cost of (See the chart in the Appendix):
    - Labor for copying the PHI requested by the individual through other than an internet-based method (internet-based method would include portals and APIs, as well as similar technologies) 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 means other than an internet-based method

- specifying that a health care provider may charge a reasonable cost-based fee for an access request to direct the health care provider to transmit an electronic copy of PHI in an EHR to a third party through other than an internet-based method. The fee may only include the cost of (See the chart in the Appendix):
    - Labor for copying the PHI requested by the individual in electronic form
    - Preparing an explanation or summary of the electronic PHI, if agreed to by the individual

Business Associate Disclosure of PHI

The proposed rule would clarify that a business associate is required to disclose PHI to the covered entity so the covered entity can meet its access obligations. However, if the business associate agreement provides that the business associate will provide access to PHI in an EHR directly to the individual or the individual's designee, the business associate must then provide such direct access.

Notice of Individual Access and Authorization Fees

The proposed rules would require covered entities to provide advance notice of the approximate fees for copies of PHI requested 1) under the individual's access right and 2) with an individual's valid authorization. Covered entities would be required to post a fee schedule online (if they have a website) and make the fee schedule available to individuals at the point of service (as well as orally over the phone) upon an individual's request, in paper or electronic form. The notice would be required to include:

- all types of access available free of charge;
- the fee schedule for the fees described above under the individual's access right; and
- the fee schedule for copies of PHI sent to third parties with the individual's valid authorization with respect to all available forms and formats for such copies.

Additionally, the proposed rule would require covered entities to provide an individualized estimate to an individual of the approximate fees to be charged for the requested copies of PHI, upon request. A covered entity must provide the individualized estimate before it provides the PHI to the individual and must notify the individual if it needs a 15-day extension. The proposed rule would 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 constitute the total fee charged to the individual for copies of PHI.

Proposed Clarification to the Definition of Health Care Operations

The Privacy Rule permits certain uses and disclosures of PHI to be made without an individual's authorization for the purpose of treatment, payment, and health care operations (referred to as TPO). The proposed rule would clarify that the definition of health care operations includes all care coordination and case management by health plans, whether individual-level or population based. For example, a telephone call by a nurse in a doctor's office to a patient to discuss follow-up care is a treatment activity while the same call by a nurse working for a health plan would be a health care operation activity.

Proposed Exception to the Minimum Necessary Standard

The Privacy Rule generally requires that covered entities use, disclose, or request only the minimum PHI necessary to meet the purpose of the use, disclosure, or request. There are some exceptions from the minimum necessary standard. For example, disclosures of PHI to health care providers for treatment,

including for case management and care coordination, are excluded from the minimum necessary standard. Currently, uses and disclosures of PHI for care coordination and case management that are considered health care operations are subject to the minimum necessary standard. Therefore, under the current Privacy Rule, any care coordination or case management activity conducted by a health plan is generally a health care operation subject to the minimum necessary standard. The proposed rule would add 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 activities with respect to an individual, regardless of whether such activities constitute treatment or health care operations.

This additional exception would relieve covered entities from making minimum necessary determinations 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. For example, when a health plan requests a disclosure for care coordination or case management to facilitate an individual's participation in the plan's new wellness program, a requesting health plan would be relieved of the responsibility for determining the minimum necessary amount of PHI for that purpose and the disclosing health care provider would be relieved of the responsibility of assessing whether reliance on the health plan's determination of the minimum necessary PHI for its purpose is reasonable under the circumstances.

Proposed Clarification on the Scope of Covered Entities' Abilities to Disclose PHI to Third Parties for Individual-Level Care Coordination and Case Management that Constitutes Treatment or Health Care Operations

The proposed rule would clarify that covered entities may disclose PHI, without individual authorization, to social services agencies, community-based organizations, home and community-based services (HCBS) providers, and other similar third parties that provide health-related services to specific individuals for individual-level care coordination and case management, either as a treatment activity of a covered health care provider or as a health care operations activity of a health care provider or health plan.

Proposed Amendment to Change "Professional Judgment" to "Good Faith Belief"

The Privacy Rule 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. Furthermore, the Privacy Rule permits a covered entity to disclose relevant PHI about an individual who cannot agree or object due to 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 determines based on *professional judgment* that the disclosure is in the best interests of the individual. There are five provisions in the Privacy Rule using this professional judgment standard: 45 CFR 164.502(g)(3)(ii)(C), 164.510(a)(3), 164.510(b)(2)(iii), 164.510(b)(3), 164.514(h)(2)(iv).

The proposed rule would amend the five provisions contained in the Privacy Rule that use the phrase "professional judgment" and replace it with the phrase "good faith belief" as the standard by which covered entities would be permitted to make certain uses and disclosures in the best interests of individuals. An example of good faith belief would be relying on knowledge of the facts of the situation, including any prior expressed privacy preferences of the individual, or representations of a person or persons who reasonably can be expected to have knowledge of relevant facts. Good faith belief may be exercised by a workforce member that has been trained on the covered entity's HIPAA policies and procedures and is acting within the scope of their authority. The proposed good faith belief standard

would create a presumption that a covered entity has complied with the good faith requirement unless there is evidence that the covered entity acted in bad faith.

Proposed Amendment to Change "Serious and Imminent Threat" to "Serious and Reasonably Foreseeable Threat"

The Privacy Rule allows covered entities to rely on a good faith belief to use or disclose PHI when necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. The recipient of the PHI must be reasonably able to prevent harm or lessen the threat, or the use or disclosure must be necessary for law enforcement to identify or apprehend an individual. The proposed rule would replace the phrase "serious and imminent threat" with the phrase "serious and reasonably foreseeable threat." The proposed rule defines "reasonably foreseeable" as whether a similarly situated covered entity could believe that a serious harm is reasonably likely to occur. The proposed modification would permit covered entities to use or disclose PHI without having to determine whether the threatened harm is imminent and instead allow covered entities to determine whether it is reasonably foreseeable that the threatened harm might occur.

Proposed Amendment to the Notice of Privacy Practices (NPP) Requirement

Under the Privacy Rule, covered entities generally must provide an NPP to each individual for which the covered entity has access to the individual's PHI. There are certain exceptions for fully insured plans. For example, if a fully insured plan does not have access to PHI (except for summary health information and enrollment information) the insurer is responsible for complying with the NPP requirement. If a fully insured plan has access to PHI (in addition to summary health information and enrollment information), then the plan must maintain an NPP, but it is only required to provide the notice upon request. The DOL provides a model NPP for group health plans.

The proposed rule would include an additional provision in the NPP that clarifies that individuals have a right to discuss the NPP with a person designated by the covered entity. The proposed rule would also modify the header of the NPP to specify that the NPP provides information to individuals about:

- How to access their health information
- How to file a HIPAA complaint
- individuals' right to receive a copy of the NPP and to discuss its contents with a designated person. The header would specify whether the designated person is available onsite and must include a phone number and email address for the designated person.

The proposed rule would also modify the NPP 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 to direct a covered health care provider to transmit an electronic copy of PHI in an EHR to a third party. The proposed rule would add an optional element to the NPP to include information to address instances in which individuals seek to direct their PHI to a third party, when their PHI is not in an electronic health record or is not in an electronic format.

Proposed Rule on using Telecommunications Relay Services (TRS)

The proposed rule would permit covered entities and their business associates to disclose PHI to TRS communications assistants for persons who are deaf, hard of hearing, or deafblind, or who have a speech disability, to perform the covered entity's or business associate's functions without obtaining specific

authorization from the individual. The proposed rule would also exclude TRS providers from the definition of a business associate.

Proposed Expansion to Use and Disclose the PHI of Uniformed Services Personnel

Under the Privacy Rule, a covered entity may use and disclose the PHI of Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, without obtaining the individual's specific authorization, provided the conditions under 45 CFR 164.512(k) are met. The proposed rule would expand this Armed Forces permission to use or disclose PHI to all Uniformed Services personnel whether serving in the U.S. or abroad, which then would include the U.S. Public Health Service (USPHS) Commissioned Corps and the National Oceanic and Atmospheric Administration (NOAA) Commissioned Corps.

1/7/2021

Appendix

Type of Access	Recipient of PHI	Allowable Fees
In-person inspection – including viewing and self-recording or -copying	Individual (or personal representative)	Free
Internet-based method of requesting and obtaining copies of PHI (e.g., using View-Download-Transmit functionality (VDT), or a personal health application connection via a certified API technology)	Individual	Free
Receiving a non-electronic copy of PHI in response to an access request	Individual	Reasonable cost-based fee, limited to labor for making copies, supplies for copying, actual postage and shipping, and costs of preparing a summary or explanation as agreed to by the individual
Receiving an electronic copy of PHI through a non-internet-based method 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)	Individual	Reasonable cost-based fee, limited to labor for making copies and costs of preparing a summary or explanation as agreed to by the individual
Electronic copies of PHI in an EHR received in response to an access request to direct such copies to a third party	Third party as directed by the individual through the right of access	Reasonable cost-based fee, limited to labor for making copies and for preparing a summary or explanation agreed to by the individual