HIPAA Proposed Rule – Summary of Key Proposals (May 2021)

Background

On January 21, 2021, the last day of the Trump administration, the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) issued a proposed rule on HIPAA to modify the standards for the privacy of individually identifiable health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). **NOTE:** This is a proposed rule. Nothing in this rule is in effect until HHS issues a final rule.

Proposed Changes of Notable Interest

- Provides patients access to their records within 15 business days rather than 30
- Allows patients to direct their PHI in an EHR to third parties including other providers creating a second pathway for patients to obtain their data under the right of access authority, in addition to one available under treatment, payment & healthcare operations (TPO).
- Requires that covered entities (CEs) allow every app that wants to register with an API to provide access for an individual assuming this is practical for the CE and barring any security concerns.
- Any CE or business associate that makes a secure, standards-based API available cannot deny the app registration because that would be denying individual access
- Replaces "the exercise of professional judgement" standard with a standard based on "good faith belief" concerning an individual's interests
- Replaces the provision that lets a CE use or disclose PHI based on a "serious and imminent threat" with a "serious and reasonably foreseeable threat" standard
- Changes the fee structure for accessing PHI
- Prohibits unreasonable patient identity verification requirements
- Replaces the "exercise of professional judgment" with "good faith belief" as the standard pursuant to which CEs would be permitted to make certain uses and disclosures of PHI in the best interests of individuals
- Removes the requirements for a CE to obtain a written acknowledgment of receipt of the NPP and to remove the current requirement to retain copies of such documentation

Regulatory History

- HIPAA was signed into law in 1986
- First HIPAA privacy rule published in 2000 and modified several times thereafter
- Right of Access established in 2000
- HITECH changes Right of Access in 2013 Omnibus rulemaking

Care Coordination

- Changes predicated on Trump Administration's efforts to reduce burden and improve care coordination
- Rule offers a non-exhaustive list of care coordination & case management for purposes of this rule

Individual Right of Access

OCR has made several proposed changes related to a patient's right of access policies which are highlighted below.

Proposed Additions of Definitions for EHR and Personal Health Application

- OCR says they are proposing to incorporate definitions into the privacy rule that are needed to meet the Health Information Technology for Economic and Clinical Health (HITECH) Act
- Privacy Rule currently does not define an EHR.
- OCR is proposing to define this to say:

> *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 a direct treatment relationship with individuals, as defined at § 164.501, such as physicians, nurses, pharmacists, and other allied health professionals. For purposes of this paragraph, ''health-related information on an individual'' covers the same scope of information as the term ''individually identifiable health information'' as defined at § 160.103.*

- Currently the Privacy Rule also does not currently contain a definition for "authorized health care clinicians and staff," OCR proposes that it include, at least:

> *covered health care providers who are able to access, modify, transmit, or otherwise use or disclose PHI in an EHR, and who have direct treatment relationships with individuals; and their workforce members (as workforce is defined at 45 CFR 160.103) who support the provision of such treatment by virtue of their qualifications or job role.*

- This definition is different from the definition in the ONC Information Blocking Rule.
- OCR proposes to define for "Personal health application" as the following:

> *An electronic application used by an individual to access health information about that individual in an 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.

Strengthening the Access Right to Inspect and Obtain Copies of PHI

- OCR proposes to add a new right to enable an individual to take notes, videos and photographs, and use other personal resources to view and capture PHI in a designated record set as part of the right to inspect PHI in person.

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

- Current policy allows individuals to request access to or copies of their PHI in a designated record set and that individuals may be required to make this request in writing. Access must be granted withing 30 days (1, 30-day extension permitted)
- Proposal shortening the window to respond to an access request from 30 days to 15 calendar and allowing no more than a single 15 calendar day extension
- Proposal also expressly prohibits a CE from imposing unreasonable measures (i.e unreasonable identity verification that creates a barrier to or unreasonably delay the individual from obtaining access.
- CEs will be allowed to require individuals to make requests for access in writing but may not do so in a way that impedes access.
- OCR also proposes requiring CEs to have written policies in place to prioritize urgent or other high-priority requests (especially those related to safety) to limit the number of extensions.

Addressing the Form of Access

- Current policy requires a CE to provide access to an individual to PHI:
  - in the form and format requested,
  - if readily producible in that form / format, and
  - if not then in a readable hard copy form, or other form / format agreed to by the individual.
- If the individual requests electronic access and the CE maintains the PHI electronically, then the CE must provide them with access to the information in the requested form and format etc.
- The agency is also examining how best to address individuals' privacy and security interests when they use a personal health application that receives PHI from a CE.
- OCR proposes that if another federal or state law requires an entity to implement a technology or policy that provides an individual with access to his or her PHI in a particular electronic form and format (e.g. standards-based API), such form and format would be deemed "readily producible" for purposes of compliance in fulfilling requests.

- If a CE has implemented a secure, standards-based API like the one required under the Cures Act, OCR considers ePHI to be readily producible in that form and format and that this is the manner in which the ePHI is transmitted.
- In other words, API would = readily producible

Addressing Individual Access Rights to Direct Copies of PHI to Third Parties

- Under the rule HHS propose to expand an individual's right related to sending their records to a third party by allowing them to:
    1. Direct only copies of PHI in an EHR (as opposed to records in any type of electronic system) to a third party;
    2. Submit oral, electronic or written requests for a covered entity to transmit an electronic copy of PHI in an EHR to a designated third party; and
    3. Direct a healthcare provider or health plan to obtain electronic copies of their PHI in an EHR to a third party. **NOTES on this point:**
    - On this proposal, OCR is also proposing to the place the burden for obtaining the records requested by third parties on the Provider/Plan (referred to in the rule as "Requester-Recipient"). Thus, the Requester-Recipient would be required to help a patient submit their request to the Discloser.
        - In short, this proposal creates a second pathway for obtaining records, in addition to one available under treatment, payment & healthcare operations (TPO). Under TPO, providers may share PHI without a patient's consent. Under this new proposal the PHI release would occur after a patient requests disclosure
        - This patient right of access policy is totally separate from the one that allows a CE to send PHI to another entity under the uses and disclosures policy.
        - OCR is also proposing that the Requester-Recipient would be required to help a patient submit their request to the Discloser
        - PHI should be shared as soon as possible but no later than 15 calendar days after request is made and all information needed to act on the request is supplied.

Adjusting Permitted Fees for Access to PHI and ePHI

- OCR is formally proposing changes to the fee structure. Specifically, they are calling for a fee structure based on the type of access request:
    - Categories of access when a fee CANNOT be charged; and
    - Allowable costs that may be included when an access fee is permitted.
- The current patient right of access policy allows an individual to transmit a copy of their PHI to another person or entity when requested (aka third-party).
- In 2016 HHS released guidance which:

- Said third parties who were directed by patients to obtain copies of their medical records were now restricted to what is commonly referred to as the "patient rate" or also known as a "reasonable, cost-based fee."
- A flat fee of up to $6.50 was permitted unless covered entities calculated the actual or average costs for reproducing the medical record. Prior to this guidance third parties were not restricted by the patient rate.
- Changed the way labor was calculated under the patient rate.

- HHS was challenged in court over decisions made in the 2016 guidance including that HHS did not go through formal rule and comment to make these changes.
- Prop

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 & 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) [129].	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.

Notice of Access & Authorization Fees

- OCR calls for CEs to provide advance notice for the expected costs for copies of PHI
- Will have to post fee schedules online that include:
  - All types of access available free of charge
  - Fees for:
    - PHI readily producible electronic & non-electronic forms & formats
    - Copies of PHI in an HER and directed to third parties
    - Copies of PHI directed to third parties
- Must make fee schedule available upon request both on paper and electronically, as well as, at the point of care
- Table of permitted fees below

Type of Access	Recipient of PHI	Allowable Fees
PHI copied onto electronic media through the U.S. Mail or via certified export functionality)[129]		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.

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 & 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	Individual	Reasonable cost-based fee, limited to labor for making copies and costs of preparing a summary or

Reducing Identity Verification Burden for Individuals Exercising the Right of Access

- Under current policy CEs must take reasonable steps to verify the identity of a person requesting PHI before disclosure
- OCR does not mandate a particular form of verification. Verification can be done orally, in writing, over the phone, by fax, email, portal, etc. using the CEs own form
- OCR continues to get questions about verification
- OCR assumes that if a CE has PHI for an individual in an EHR has established a treatment relationship with a patient and imposing added verification is not needed
- OCR proposes to expressly prohibiting a CE from imposing "unreasonable identity verification measures"
- These are defined as those requiring an individual to expense unnecessary effort or expense when a les burdensome method is practicable
- OCR will take into account a CE's obligations under the security rule
- Directing PHI to a 3rd party can be orally if clear and specific
- Unreasonable examples include:
    - Requiring notarization
    - Making a request for in writing can't be done in burdensome way
    - Requiring 3rd parties that are not Bas to enter into a BAA
    - Preventing a patient's 3rd party app from registering with an endpoint (i.e. API) that the CE has made public, absent a security concern
- OCR not proposing a single type of verification be used
- OCR says CEs must allow every app that wants to register with an API to provide access for an individual assuming this is practical for the CE and barring any security concerns.
- Any CE or BA that makes a secure, standards-based API available cannot deny the app registration because that would be denying individual access
- Can't deny access simply because CE doesn't have a business associate relationship or because the app offers another service that is in competition with the CE

Amending the Definition of Health Care Operations to Clarify the Scope of Care Coordination and Case Management

- OCR proposes to clarify the definition of healthcare operations to be "… 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."

Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-level Care Coordination and Case Management

- OCR proposes to add an express exception to the minimum necessary standard for disclosures to, or requests by, a health plan or covered healthcare provider for care coordination and case management. This would apply only for individual-level, not population-level requests.

Clarifying the Scope of CE's Abilities to Disclose PHI to Certain 3rd Parties for Individual Level Care Coordination and Case Management That Constitutes Treatment or Health Care Operations

- OCR proposes to expressly permit CEs to disclose PHI 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 healthcare operations activity of a covered healthcare provider or health plan.
- Under this provision a health plan or a covered healthcare provider could only disclose PHI without authorization to a third party that provides health-related services to individuals; however, the third party does not have to be a healthcare provider.

Encouraging Disclosures of PHI when Needed to Help Individuals Experiencing Substance Use Disorder (Including Opioid Use Disorder), Serious Mental Illness, and in Emergency Circumstances

Judgement Standards

- OCR says family members, friends and caregivers are a critical component to helping people who suffer from substance abuse disorder (SUD) and mental illness.
- There remains fear among providers that sharing information about these patients will violate HIPAA.
- OCR proposes to amend five provisions of the Privacy Rule 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 of PHI in the best interests of individuals. These five provisions include:
    1. Disclosures to personal representatives;
    2. Uses and disclosures requiring an opportunity for the individual to agree or object;
    3. Identity verification;
    4. Uses and disclosures to avert a serious threat to health or safety; and 5) relevant guidance encouraging disclosures of PHI to help individuals experiencing opioid use disorder or mental illness.

- Additionally, OCR also proposes a presumption that a CE has complied with the good faith requirement, absent evidence that the covered entity acted in bad faith.

Threat Standards

- Within the proposed rule, OCR proposes an amendment to the Privacy Rule replacing the "serious and imminent threat" standard with a "serious and reasonably foreseeable threat" standard, allowing providers more flexibility in invoking the threat standard at the time of PHI disclosure and the reasonableness of the threat determination.
- OCR also proposes a non-substantive revision to change "preventing or lessening a threat" to "preventing a harm or lessening a threat."

Eliminating Notice of Privacy Practices Requirements Related to Obtaining Written Acknowledgement of Receipt, Establishing an Individual Right to Discuss the NPP with a Designated Person, Modifying the NPP Content Requirements, and Adding an Optional Element

- Current OCR policy requires providers to make a good faith effort to obtain a written acknowledgment of receipt of the provider's Notice of Privacy Practices (NPP).
- OCR proposes to eliminate the requirements for a CE to obtain a written acknowledgment of receipt of the NPP and to remove the current requirement to retain copies of such documentation for six years.
- OCR proposes to replace the written acknowledgment requirements with an individual right to discuss the NPP with a person designated by the CE.