

Proposed Modifications to the HIPAA Privacy Rule

Timothy Noonan
Deputy Director for Health Information Privacy
HHS Office for Civil Rights

Ciox Health
May 18, 2021



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights



Agenda

- Right of Access
- Notice of Privacy Practices
- Disclosures of PHI in the Best Interests of Individuals
- Disclosures to Lessen or Prevent Threat of Harm
- Care Coordination and Exception to Minimum Necessary Standard
- Disclosures to Facilitate Care with Social and Community-Based Services
- Telecommunications Relay Services
- Uniformed Services

Overview of Right of Access Proposals

- New defined terms
- Shorter response timelines for access requests
- Transmitting PHI to a personal health application
- Preventing unreasonable measures for access and identity verification
- Viewing and capturing images of PHI
- Directing copies to a third party
- Individual-directed information sharing among covered providers and plans
- Fee limitations
- Posting fee schedules

Definition of *Electronic Health Record* (*EHR*)

- **EHR:** An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and their staff
 - **Clinicians:** Health care providers that have a *direct treatment relationship* with individuals
 - **Health-related information on an individual:** *Individually identifiable health information*

Definition of Personal Health App

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 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.



Time to Act on Requests for Access

- “As soon as practicable” but no later than 15 calendar days after receipt of request
- One possible extension of 15 calendar days, provided that the covered entity has implemented a policy to prioritize urgent or otherwise high priority requests (esp. those relating to the health and safety of individual or another person)
- Shorter timelines in other law are “practicable”

Access Request Measures

A covered entity may require access requests in writing, but only if the covered entity:

- Informs the individual of the requirement
- Does not impose unreasonable measures impeding the individual from obtaining access when a less burdensome measure is practicable for the CE

So, what would be a *reasonable* measure?



The NPRM says it's reasonable to require individuals to complete a standard form containing only the information the CE needs to process the request.



Identity Verification Measures

- Current identity verification requirements remain
- Prohibition on unreasonable identity verification requirements for individuals attempting to exercise their rights under the HIPAA Rules, including the right of access
- Unreasonable measures cause an individual to expend unnecessary effort or resources when a less burdensome verification measure is practicable for the covered entity

Right to Inspect

- Right to view, take notes and photographs, and use other personal resources to capture their PHI in a designated record set at a mutually convenient time and place, including in conjunction with a health care appointment
- A covered entity may establish limits:
 - Not required to allow connection of personal devices to CE's information systems
 - May impose measures to ensure individual only records PHI to which individual has right of access
 - May establish reasonable policies and safeguards to minimize disruption to operations

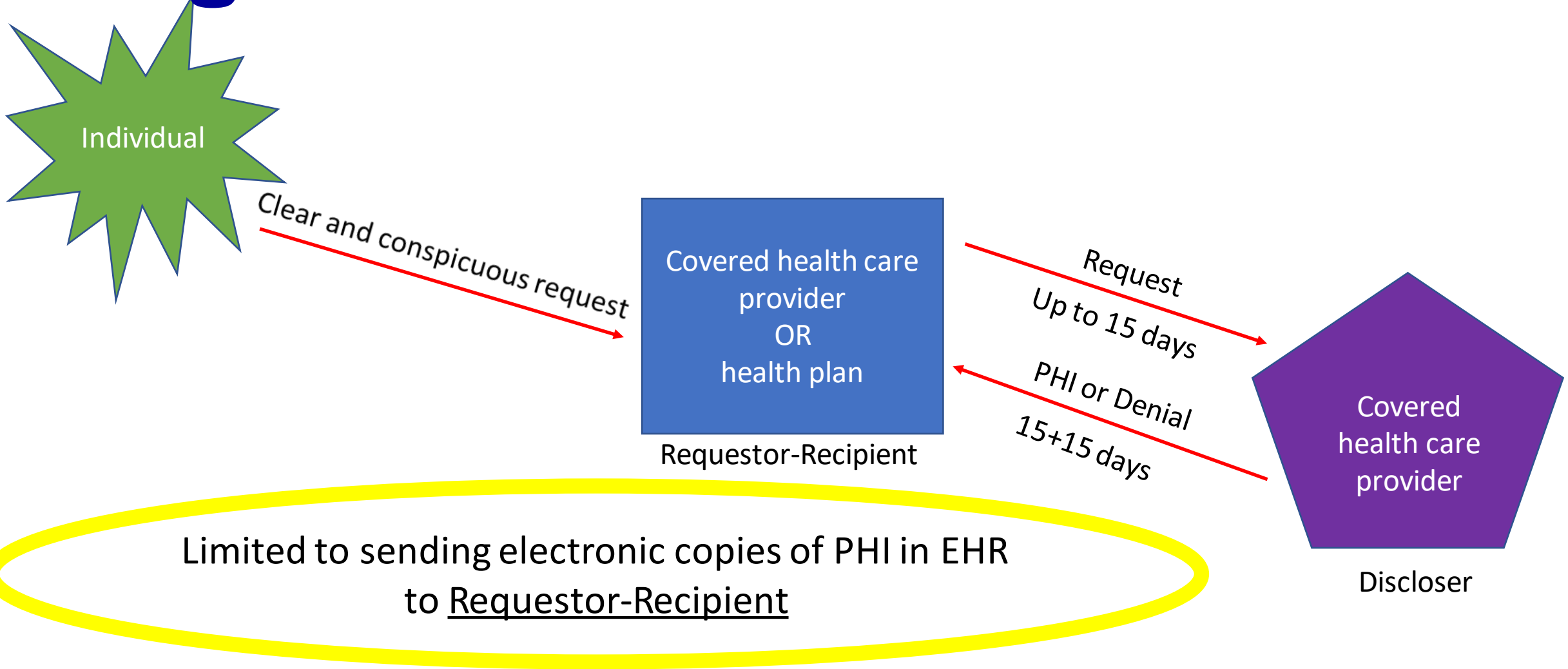
Form and Format

- Deem PHI “readily producible” in an electronic form and format where another applicable federal or state law requires that form and format
- If a covered entity or its EHR developer (business associate) has implemented a secure, standards-based API that is capable of providing access to ePHI in the form and format used by an individual’s personal health application, that ePHI is considered to be *readily producible* in that form and format

Right to Direct ePHI to a Third Party

- Right to direct a *covered health care provider* to transmit an *electronic copy* of PHI *in an EHR* to a third party
- “Clear, conspicuous, and specific” request
 - Orally or in writing (which may be electronically executed)
 - Individual may use an internet-based method, such as a *personal health application, to submit the access request*, so long as it is “clear, conspicuous, and specific”

Right of Access to Direct Disclosures



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., Personal Health App)	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	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 as agreed to by the individual.*



Notice of Access & Authorization Copy Fees

- Notice of fees for copies of PHI requested under the access right and with an individual's valid authorization
 - Website posting and available at point of service upon request
 - Include types of access available and fee schedule
- Upon the individual's request:
 - Individualized estimate of approximate fees to be charged for copies
 - Itemized list of charges for a specific request for copies

Notice of Privacy Practices (NPP)

- Eliminate written acknowledgment requirements for the NPP
- Establish an individual right to discuss the NPP with a person designated by the covered entity
- NPP explains how to contact the designated person

Notice of Privacy Practices (NPP)

- NPP content to inform individuals
 - How to access their health information
 - How to file a HIPAA complaint
 - Right to receive a copy of the notice and to discuss its contents with a designated person
 - How to contact the designated person

Disclosures of PHI in the Best Interests of Individuals

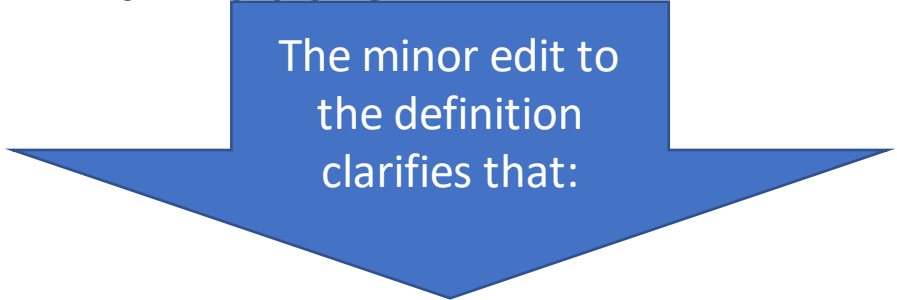
- Permit disclosure of PHI based on good faith belief that disclosure is in the best interests of the individual
- Presumption of good faith
- Proposed good faith standard may be exercised by workforce members who are trained on the covered entity's HIPAA policies and procedures and who are acting within the scope of their authority

Preventing Serious Harm

- Uses and disclosures for health or safety when harm is “serious and reasonably foreseeable,” instead of the current “serious and imminent” threat standard
- Reasonably foreseeable based on a reasonable person standard
- Still based on good faith belief of the covered entity, with presumption of good faith

Health Plan Clarification

The term *health care operations* encompasses all care coordination and case management by health plans, whether population-based or focused on particular individuals



The minor edit to
the definition
clarifies that:

Health plans may use and disclose PHI for population-based and individual level care coordination and case management under the permission to use and disclose PHI for health care operations

Exception to Minimum Necessary Standard

- 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 for individuals
- Exception would not apply to population-based care coordination and case management
- Covered entities would still be able to honor individuals' requests for privacy restrictions

Care Coordination Disclosures to Third Parties

- Express permission for covered entities to disclose PHI to third parties for care coordination and case management with respect to an individual
 - Social services agencies
 - Community-based organizations
 - Home and community based services providers (HCBS)
 - Similar third parties that provide or coordinate health-related services
- Individuals can still request restrictions on disclosures of PHI for treatment, payment, and health care operations

Telecommunications Relay Service (TRS)

- Expressly permit disclosures to TRS communications assistants for persons who are deaf, hard of hearing, or deaf-blind, or who have a speech disability
- Exclude TRS providers from the definition of *business associate*
- Ensure that workforce members of a covered entity or business associate can use TRS to share PHI with other workforce members or outside parties as needed to perform their duties

Uniformed Services Personnel

- Extend permission to disclose PHI of Armed Forces personnel to include all uniformed services, adding:
 - U.S. Public Health Service (USPHS) Commissioned Corps
 - National Oceanic and Atmospheric Administration (NOAA) Commissioned Corps.
- Allow disclosures necessary to assure proper execution of the mission

Resources

- OCR announced a 45-day extension on March 9, 2021, extending the deadline for the public to submit comments to May 6, 2021
 - <https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/index.html>
- OCR Webpage on HIPAA NPRM
 - <https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/index.html>
- OCR HIPAA NPRM Fact Sheet
 - <https://www.hhs.gov/sites/default/files/hipaa-nprm-factsheet.pdf>
- The NPRM is available for review and comment at <https://www.regulations.gov/document/HHS-OCR-2021-0006-0001>

Contact Us

Office for Civil Rights

U.S. Department of Health and Human Services



ocrmail@hhs.gov

www.hhs.gov/ocr



Voice: (800) 368-1019

TDD: (800) 537-7697

Fax: (202) 519-3818



200 Independence Avenue, S.W.

H.H.H. Building, Room 509-F

Washington, D.C. 20201



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights



Connect with Us

Office for Civil Rights

U.S. Department of Health and Human Services



www.hhs.gov/hipaa



Join our Privacy and Security listservs at

<https://www.hhs.gov/hipaa/for-professionals/list-serve/>



@HHSOCR



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

Questions?

