HHS Proposes Significant Changes to the HIPAA Privacy Rule

December 22, 2020

As part of its Regulatory Sprint to Coordinated Care, the US Department of Health and Human Services (HHS) recently proposed important changes to the Health Insurance Portability and Accountability Act (HIPAA) privacy rule. The changes are designed to enhance individuals' involvement in their care, remove barriers to coordinated care and ease administrative burdens under the HIPAA privacy rule. If finalized, the changes would require significant modifications to regulated entities' policies and procedures, training and notice of privacy practices (NPP). Interested stakeholders have until 60 days after the publication of the Notice of Proposed Rulemaking (NPRM) in the federal register to provide comments.

Key proposals include:

- extensive changes to enhance individuals' rights of access to protected health information (PHI) (including allowing individuals to take notes or photos of their PHI as part of the right of inspection, prohibiting a covered health care provider from delaying the right to inspect if PHI is readily available at the point of care in conjunction with a health care appointment, shortening response time for providing access from 30 to 15 days, reducing identity verification burdens, limiting individuals' rights to direct a copy of PHI to a third party to a right to direct an electronic copy of PHI in an electronic health record (EHR) to a third party, creating a pathway for a covered health care provider or health plan to obtain an electronic copy of PHI in an EHR from a covered health care provider through a required disclosure initiated under the individual's right of access, adjusting the permitted fees for copies of PHI, and requiring advance notice of approximate fees);
- clarifying that "health care operations" encompasses all care coordination and case management by health plans, whether individual-level or population-based;
- creating an exception to the minimum necessary standard for individual-level care coordination and case management uses and disclosures;
- clarifying covered entities' abilities to disclose PHI to social service agencies, community-based organizations, home- and community-based services (HCBS) providers and others that provide health-related services to facilitate care coordination and case management for individuals;
- easing the standard that permits covered entities to make certain uses and disclosures of PHI based on their professional judgment;
- expanding the ability of covered entities to disclose PHI to avert a threat to health or safety;
- eliminating the requirement to obtain an individual's written acknowledgement of receipt of the notice of privacy practices (NPP);
- modifying the content of the NPP to clarify the individuals' rights and how to exercise them; and

- permitting disclosure to Telecommunications Relay Services communications assistance without a business associate agreement and expanding the permission to use and disclose PHI of armed forces personnel to cover all uniformed services personnel.

The NPRM takes into consideration comments received to HHS's 2018 request for information, discussed here.

1. Individual Right of Access

Adding Definitions for "Electronic Health Record " and "Personal Health Application"

The NPRM adds definitions for "electronic health record" and "personal health application." These definitions are important in clarifying the scope of the modified right of individuals to direct a covered entity to transmit an electronic copy of PHI "in an EHR" to a designated third party, as discussed below.

Specifically, the NPRM would define an EHR as an electronic record of health-related information (i.e., individually identifiable health information as defined by the privacy rule, including clinical, billing and other such information) on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff. An EHR would include electronic records consulted by any covered health care provider, or a workforce member of such health care provider, so long as the provider has a *direct* treatment relationship with individuals. The term would not include covered health care providers with *indirect* treatment relationships with individuals. For example, an EHR would not include health-related electronic records of covered health care providers that only supply durable medical equipment to other providers. HHS solicits comment on this key definition, including whether, as defined, an electronic record can only be an EHR if it is created or maintained by a health care provider (versus a health plan), whether the definition of EHR is too broad or narrow, and whether to further align the definition with that of a "designated record set" or other definitions of electronic health records.

Given the increase in individuals using personal health applications to access and manage their PHI, HHS also proposes defining "personal health application" to mean "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."

Under this definition, a personal health application is not acting on behalf of, or at the direction of a covered entity and, therefore, would not be subject to HIPAA's privacy and security obligations, though HHS supports providing individuals with information that will support them in making the best choices when selecting a personal health application. See the preamble to the Office of National Coordinator for Health Information Technology (ONC) Cures Act Final Rule at 85 FR 25642, 25814 (May 1, 2020) ("*Interference Versus Education When an Individual Chooses Technology to Facilitate Access*") for a discussion of how a covered entity may provide such information. HHS seeks comment on whether a covered health care provider and/or health plan should be required to inform an individual who requests that PHI be transmitted to the individual's personal health application of the privacy and security risks of transmitting PHI to an entity that is not covered by HIPAA.

Strengthening the Access Right to Inspect and Obtain Copies of PHI

HHS proposes incorporating part of its 2016 Access Guidance into the privacy rule to create a new right of individuals to take notes, videos, and photographs, and use other personal resources to view and capture PHI in a designated record set, without a fee, as part of the right to inspect PHI in person at mutually convenient times. HHS expects that a health care appointment where PHI in a designated record set is readily available for viewing at the point of care (for example, an ultrasound at an ultrasound appointment), would be considered a convenient time and place, and therefore, the NPRM would prohibit a covered health care provider from delaying the right to inspect in those circumstances. A covered entity would not be required to allow an individual to connect a

personal device to its information systems and could establish reasonable policies and safeguards, provided they do not impose unreasonable barriers to individual access.

Prohibiting "Unreasonable Measures" That Impeding the Right of Access; Shortening Response Time

The NPRM would prohibit covered entities from imposing "unreasonable measures" on an individual's right of access, such as by requiring the use of a form that requires extensive, unnecessary information from an individual, requiring notarized signatures, or accepting written requests only in paper form, only in person at the entity's facility or only through the covered entity's online portal. The NPRM does not provide an exhaustive list of "unreasonable measures."

The NPRM would also shorten covered entities' response time upon receiving a request for PHI from an individual. Currently, covered entities have 30 days to address a request, with the option for a 30-day extension. The proposed modifications would decrease the response time to "as soon as practicable" and no later than 15 days, with the possibility of one optional 15-day extension, provided that the covered entity has established written policies for prioritizing "urgent or other high priority" access requests (a category of request that HHS does not define). HHS proposes to deem "practicable" any shorter period established by another federal or state law.

Addressing the Form of Access

Currently, if an individual requests electronic access to PHI that the covered entity maintains electronically, the covered entity must 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 an agreed upon alternative, readable electronic format.

HHS also proposes to provide that if other federal or state laws require an entity to implement a technology or policy that would have the effect of providing an individual with access to his or her PHI in a particular electronic form and format, such as through secure, standards-based APIs using applications chosen by individuals, such form and format would be deemed "readily producible" for purposes of fulfilling the access request. Thus, if a covered health care provider refused to provide an electronic copy of PHI in response to an individual's request for access via a secure API, despite the provider's having implemented a secure API established within the provider's EHR for this purpose, the provider would be violating the privacy rule's access requirements. The NPRM clarifies that if the same covered provider required all apps to register before providing access via its secure API, imposing this requirement would not constitute a denial of access in the form and format requested, provided that the registration process did not exclude or prevent a personal health application that was capable of securely connecting to the secure API from doing so. HHS seeks comment on a number of related situations.

When offering a summary in lieu of access in accordance with the privacy rule, HHS proposes to require covered entities to inform the individual that the individual retains the right to obtain a copy of the requested PHI (or direct an electronic copy of PHI in an EHR to a third party), if they do not agree to receive the summary. This requirement would not apply when the covered entity offers a summary because it is denying the request for a copy on unreviewable or reviewable grounds.

Addressing the Individual Access Right to Direct Copies of PHI to Third Parties

HHS proposes to expand an individual's right to direct to a covered entity to transmit an electronic copy of PHI in an EHR to a third party. Though HHS interprets the court's order in Ciox v. Azar to preclude a proposal that requires covered entities to provide electronic copies of PHI to third parties designated by the individual in the form and format requested by the individual (rather than in the EHR format), HHS encourages covered entities to provide copies to third parties in the electronic format requested by the individual to facilitate the individual's meaningful exercise of the right of access.

HHS would expand the right of access by requiring covered entities to respond to an individual's request to direct an electronic copy of PHI in an EHR to a third party designated by the individual when the request is "clear, conspicuous, and specific" — whether made orally or in writing (including electronically, such as through a personal health application or patient portal). This would replace the current requirement that the request be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.

HHS also would create a requirement within the right of access for a covered entity to facilitate an individual's request to direct an electronic copy of PHI in an EHR to a third party designated by the individual, which in this case would be the covered entity facilitating the request. Under this proposal, if an individual were to make a clear, conspicuous and specific request that his or her health care provider or health plan (Requestor-Recipient) obtain an electronic copy of PHI in an EHR from one or more covered health care providers (Discloser), the Requestor-Recipient would be required to assist the individual by submitting the individual's request to the Disclosers identified by the individual. Importantly, this requirement would essentially create a second pathway (in addition to permitted disclosure for treatment, payment and healthcare operations purposes) for a covered health care provider or health plan to obtain an electronic copy of PHI in an EHR from a covered health care provider through a required disclosure initiated under the individual's right of access. HHS expressly requests comments on different potential approaches to clarify that the privacy rule permits covered entities to use health information exchanges (HIEs) to make "broadcast" queries on behalf of an individual to determine which covered entities maintain that individual's PHI and request copies of that PHI (for example, HHS notes that a covered entity may disclose PHI for its own health care operations purposes, including customer service activities, which could include forwarding an access request to other providers using a trusted exchange network).

HHS proposes that this new requirement would apply when an individual is an existing or prospective new patient or current member (or dependent) of a Requester-Recipient. The requirement would be limited to directing electronic copies of PHI in an EHR back to the Requestor-Recipient. A Requester-Recipient would be required to submit such access requests as soon as practicable but no later than 15 days (with no potential for extension) after receiving the individual's direction and any necessary information required for the Discloser to process the request.

Finally, the proposal would require covered entities to inform individuals of their right to direct the requested electronic copies of PHI in an EHR to a designated third party when a covered entity offers summary of PHI in lieu of the copy.

Adjusting the Permitted Fees for Access to PHI and ePHI

HHS proposes to modify the access fee provisions as follows, based on the type of access request.

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.

Type of Access	Recipient of PHI	Allowable Fees
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 US 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 as agreed to by the individual.

HHS solicits comments on the proposed fee modifications and related issues, such as whether the privacy rule should prohibit the charging of fees when the individual is a Medicaid beneficiary/applicant, recipient of SSDI, or when copies are directed to certain entities, such as those conducting clinical research.

Notice of Access and Authorization Fees

HHS proposes requiring covered entities to provide advance notice of approximate fees for copies of PHI requested under the access right and with an individual's valid authorization. Specifically, covered entities would be required to post a fee schedule on their website and make the fee schedule available to individuals at the point of service, upon an individual's request. Covered entities also would be required to provide, upon request, individualized fee estimates for an individual's request for copies of PHI, along with itemized bills for completed requests. An individual's request for a fee estimate would not automatically extend the time permitted for the covered entity to provide copies of PHI under the right of access.

2. Reducing Identity Verification Burdens for Individuals Exercising the Right of Access

HHS proposes that the privacy rule expressly prohibit a covered entity from imposing unreasonable identity verification measures on an individual exercising a privacy rule right. Examples of unreasonable identity verification measures may include requiring an individual to receive their PHI in person, to fill out a form with the extensive information contained in a HIPAA authorization, or to obtain notarization of the individual's signature on a request for access. HHS notes that unreasonable measures would also include applying onerous registration requirements for personal health applications beyond what is necessary for compliance with the HIPAA security rule, such as requiring a third party that does not meet the definition of a business associate to execute a business associate agreement with the covered entity, or preventing an individual's personal health application from registering with an endpoint (e.g., an API) that the covered entity makes public, absent an identified security risk.

3. Clarification of Definition of Health Care Operations

HHS proposes to amend the definition of health care operations to clarify that "health care operations" encompasses *all* care coordination and case management by health plans, whether individual-level or population-based. HHS does not define "care coordination" or "case management," though the NPRM provides numerous

examples of how these and similar terms are used by HHS, other federal regulatory agencies, and third parties. HHS solicits comments on whether additional examples or definitions would be helpful.

4. Proposed Exception to the Minimum Necessary Standard for Individual-Level Care Coordination and Case Management

To support disclosures for care coordination and case management purposes, HHS proposes to create an exception to the privacy rule's "minimum necessary" standard for uses and disclosures for individual-level care coordination and case management purposes.

Currently, covered entities may only use, disclose and request the minimum necessary PHI to accomplish a permitted purpose, with certain exceptions, such as for disclosures to or requests by (*but not uses by*) a health care provider for treatment purposes (which would include disclosures to or requests by a health care provider for individual-level case management and care coordination). Also, care coordination and case management activities that are considered health care operations activities (such as when performed by a health plan) are subject to the minimum necessary standard. For example, the privacy rule currently permits a covered health care provider or health plan to use and disclose only the minimum necessary PHI for population-based case management, such as to identify all patients or enrollees with diabetes and send them information about a recommended healthy diet to facilitate diabetes self-management. The rule also currently imposes greater restrictions on disclosures to and requests by health plans than covered health care providers when conducting care coordination or case management, because health plans don't generally perform treatment, so any care coordination or case management performed by a health plan is generally a health care operations activity and subject to minimum necessary.

The NPRM proposes to exempt covered entities from the minimum necessary requirement 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. In recognition of increased privacy concerns, the NPRM does not extend the minimum necessary exception to population-level care coordination or case management activities. Thus, health plans and covered health care providers would still need to satisfy the privacy rule's minimum necessary standard for (1) disclosures of PHI for health care operations activities other than individual-level care coordination and case management; (2) disclosures of PHI for care coordination and case management to most entities other than health care providers and health plans, such as social service agencies; (3) internal uses of PHI for these purposes, whether for treatment or health care operations; and (4) uses, requests and disclosures of PHI for other health care operation purposes, including all population-based activities.

Interaction of the Proposed Exception with ONC Cures Act Final Rule

HHS clarifies that covered entities would continue to be able to agree to an individual's request not to use or disclose PHI for these purposes in accordance with the privacy rule and the related ONC Cures Act Final Rule's information blocking exception. For example, when a covered health care provider contracts with a health plan to coordinate potential mental health treatment referrals *for a specific patient*, the provider would not need to consider what information is the minimum necessary to disclose to the health plan for this purpose. Further, HHS confirms that the ONC Cures Act Final Rule would prohibit a health care provider from limiting a permissible disclosure to what the provider believes to be the minimum necessary info when the privacy rule specifically exempts the disclosure from the minimum necessary standard. However, the provider could still honor the individual's request for restrictions on disclosures of PHI consistent with the ONC Cures Act Final Rule privacy sub-exception. The proposed change responds to concerns that having to determine what is or is not the minimum necessary for requests by, and disclosures to, health plans and health care providers in these cases may impede value-based care delivery and dis-incentivize information sharing. OCR seeks comment on its proposed changes to the minimum necessary standard.

5. Clarification of Ability to Disclose PHI to Service Agencies That Provide Health-Related Services for Individual-Level Care Coordination and Case Management

The NPRM also proposes to clarify covered entities' abilities to disclose PHI to social services agencies, community-based organizations, HCBS providers and other similar third parties that provide health-related services for individual-level care coordination and case management.

Currently, a covered health care provider may disclose PHI for treatment purposes to a third party when the third party is part of the broader health treatment plan, or is participating in the coordination of care for an individual (subject to minimum necessary if the recipient is not a health care provider). For example, a health care provider may currently disclose minimum necessary PHI to a senior center to arrange for a home health aide to help an individual with prescriptions at home. Similarly, a disclosure could facilitate care coordination and case management as part of a covered health plan's health care operations, such as when a health plan discloses an enrollee's PHI to a senior wellness center as part of the plan's wellness program. HHS notes that, despite this flexibility, many covered entities only make disclosures to social service organizations and to HCBS providers after receiving the individual's authorization, and some never disclose PHI to these types of health-related providers. To address this, HHS proposes to expressly permit covered entities to disclose PHI to social services agencies, community-based organizations, 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 covered health care provider or health plan. As proposed, a covered entity 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 health care provider. For example, the third party may be providing health-related social or supportive services, such as food or sheltered housing needed to address health risks. Thus, this provision would permit a covered entity to disclose the PHI of a chronically ill individual to a senior center attended by the individual to check on his or her health, and to ask the senior center to give disease self-management reminders.

6. Modification of the Standard for Disclosures Involving Individuals with a Substance Use Disorder or Opioid Disorder (collectively, SUD) or Serious Mental Illness (SMI), and in Emergency Circumstances.

Recognizing that individuals' family members and caregivers cannot help people experiencing SUDs or SMI if those family members and caregivers are not informed about the individual's status, HHS proposes several amendments to the privacy rule designed to encourage covered entities to share PHI in individuals' best interests, without fear of HIPAA penalties. Specifically, HHS proposes to amend five provisions of the privacy rule to replace "the exercise of professional judgment" standard (which presupposes that a decision is made by a health care professional, such as a licensed practitioner) with a standard permitting certain disclosures based on a "good faith belief" about an individual's best interests (which may be exercised by a covered entity's other workforce members who are trained on the covered entity's HIPAA policies and procedures and who are acting within the scope of their authority). The "good faith belief" standard is coupled with a presumption that a covered entity has complied with the good faith requirement, absent evidence that the covered entity acted in bad faith. Together, HHS believes these proposed modifications should improve care coordination by expanding the ability of covered entities to disclose PHI to family members and other caregivers when they believe it is in the best interests of the individual, without fear of violating HIPAA.

According to HHS, a "good faith belief" standard anticipates that a covered entity or workforce member would exercise a degree of discretion appropriate for its role when deciding to use or disclose PHI, and comply with any other conditions contained in the applicable permissions. For example, "good faith" would permit a licensed health care professional to draw on experience to make a good faith determination that it is in the best interests of a young adult patient, who has overdosed on opioids, to disclose PHI to a parent who is involved in the patient's treatment

and who the young adult would expect, based on their relationship, to participate in or be involved with the patient's recovery from the overdose. Here, HHS intends that the professional's good faith belief be informed by professional judgment, but HHS would not question or second-guess the decision, for example, by requiring the professional to prove that the decision was consistent with his or her professional training.

Other examples in the NPRM illustrate the operation of the "good faith belief" standard in connection with (1) disclosures (A) to a parent or guardian who is not the individual's personal representative, (B) in facility directories, (C) to an individual's emergency contacts, (D) in cases of an emergency or an individual's incapacity; and (2) verification of the identity of a person requesting PHI.

HHS requests comment on these proposals, including as to whether it should apply the "good faith" standard to any or all of the other nine provisions in the privacy rule that call for the exercise of professional judgment.

7. Modification of Ability to Disclose PHI to Prevent and Lessen Harm to Individuals or the Public.

The NPRM proposes a modification to the applicable standard for disclosures intended to prevent and/or lessen harm to individuals (for example, from suicide or other threatened violence) or the public from mass violence (for example, mass shootings, the use of explosive devices to attack a crowd, or other acts of terrorism). The proposed modification would replace the privacy rule's standard that currently permits a covered entity to use or disclose an individual's PHI based on a "serious and imminent threat" with a broader standard that would permit disclosure based on a "serious and reasonably foreseeable threat."

A covered entity (or a member of a covered entity's workforce) is not required to have specialized training, expertise, or experience in order to meet the "reasonably foreseeable" standard.

HHS acknowledges that timeliness of certain disclosures is directly impacted by covered entities' uncertainty regarding whether any threatened harm is "imminent," and believes a "serious and reasonably foreseeable threat" standard could, for example, further enable a health care provider to timely notify a family member that an individual is at risk of suicide, even if the provider cannot predict that a suicide attempt is likely to occur "imminently." Additionally, for an individual who poses a threat to public safety, a "serious and reasonably foreseeable threat" standard may afford a health care provider sufficient time to notify a person, such as a law enforcement official, who is in a position to avert a serious harm that may occur and ensure the safety of the individual and others.

HHS requests comment on the above changes, including any potential unexpected consequences.

8. Proposed Modifications to the Requirements Related to Notices of Privacy Practices (NPP)

The privacy rule currently requires a covered health care provider that has a direct treatment relationship with an individual to make a good faith effort to (1) obtain a written acknowledgment of receipt of the provider's NPP, (2) document its good faith efforts and the reason(s) for not obtaining an individual's written acknowledgment if the provider is unable to do so, and (3) maintain such documentation for six years. HHS understands that the requirements impose unnecessary burdens and may create confusion. For example, individuals may erroneously believe they are signing an authorization or waiver of some kind, and front office staff may erroneously believe that individuals must sign the acknowledgment to obtain care. Accordingly, the NPRM proposes to replace all three of the written acknowledgment requirements with a new individual right to discuss the NPP with a person designated by the covered entity.

For all covered entities, HHS proposes to modify the content requirements of the NPP to help increase individuals' understanding of a covered entity's privacy practices and the individuals' rights with respect to their PHI. The NPRM proposes modifications to the required header of the NPP to advise individuals that the NPP provides information

about (1) how to access individuals' health information; (2) how to file a HIPAA complaint; and (3) individuals' rights to receive a copy of the NPP and to discuss its contents with a designated contact person. The header (as modified) would have to (1) specify whether the designated contact person is available onsite, and (2) include a phone number and email address for the designated contact person.

The right of an individual to access the individual's PHI also is under HHS's scrutiny. As modified by the NPRM, the NPP would need to describe (1) 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 (2) the right to direct a covered health care provider to transmit an electronic copy of PHI in an EHR to a third party.

Finally, HHS proposes to 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 the PHI is not in an EHR or is not in an electronic format. HHS believes this optional element would help make individuals aware that they retain the right to obtain the PHI directly and give it to a third party or they can request to send a copy of PHI directly to a third party using a valid authorization.

CONTACT

For more information, or help in submitting comments to the NPRM, please contact Katten's Health Care and Privacy, Data and Cybersecurity groups, or any of the following attorneys:

Megan Hardiman
+1.312.902.5488
megan.hardiman@katten.com

Lisa Christensen
+1.212.940.6575
lisa.christensen@katten.com

Jeremy Merkel
+1.212.940.6339
jeremy.merkel@katten.com