AMERICAN HEALTH LAW ASSOCIATION

HHS Proposes Modifications to HIPAA Privacy Rule Aimed at Increasing Patient Access and Enhancing Data Sharing for Care Coordination

This Briefing is brought to you by the Privacy and Security Risk Compliance and Enforcement Affinity Group of AHLA's Health Information and Technology Practice Group.

December 22, 2020

Valerie Breslin Montague, Nixon Peabody LLP | **Laurie T. Cohen**, Nixon Peabody LLP | **Jena M. Grady**, Nixon Peabody LLP

On December 10, 2020, the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) recommending changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. As part of HHS' Regulatory Sprint to Coordinated Care, HHS intends that the proposed changes will improve patient care by enhancing care coordination and reducing regulatory burdens. Specifically, the proposed rule seeks to increase patients' access to their health information and expand information sharing for care coordination and case management purposes. HHS believes that it will allow greater family and caregiver involvement for those facing emergency situations or health crises, as well as improve flexibilities for disclosures in life-threatening or emergency situations, including opioid overdoses or COVID-19 emergencies. Finally, the proposed changes are intended to reduce administrative obstacles on health care providers and health plans, while continuing to protect health information.

With a change in administration taking place on January 20, 2021, it is possible that President-elect Biden's new HHS team will withdraw the NPRM, or propose a second NPRM with significant modifications. This briefing will examine what changes HIPAA-regulated entities can expect should the current NPRM be implemented. Nonetheless, HIPAA-regulated entities' ability to use and disclose health information may very well be left unchanged even if the NPRM is implemented due to many entities still having to comply with more restrictive state laws governing the sharing of general health information as well as sensitive health information or having to comply with 42 C.F.R. Part 2 which governs substance use disorder patient records.[1]

Background

HHS enacted its first regulation to implement the Privacy Rule on December 28, 2000.[2] It has been modified by HHS several times following the enactment of new statutory requirements, as well as to clarify or add flexibility to privacy requirements in specific instances.[3] The Privacy Rule serves as a safeguard for individuals' medical records, in addition to other individually identifiable health information created, obtained, maintained, or transmitted by or on behalf of covered entities (together, this information is defined as "PHI").[4] The Privacy Rule also established certain individual rights, including the right for individuals to receive privacy notices from their health care providers and health plans and the right to inspect and request a copy of their PHI.[5]

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act),[6] and the 2013 Omnibus Final Rule[7] expanded individuals' right to access their PHI. In 2016, to provide further clarification regarding an individual's right to access their PHI, as well as the duties of covered entities to provide such access, OCR issued guidance (2016 Access Guidance) on how it interprets and implements the access provisions in the Privacy Rule.[8]

In December 2018, HHS issued a Request for Information on Modifying HIPAA Rules to Improve Coordinated Care (RFI). The RFI asked stakeholders to comment on provisions in the HIPAA rules that present obstacles to the promotion of coordinated, value-based health care, including those that place barriers to patients and families struggling with the opioid crisis. In the NPRM, HHS stated that many of the proposed changes to the Privacy Rule stem from input received following the RFI.[9]

Individual Right of Access

Central to the care coordination concept is an individual's ability to access and authorize disclosures of their health information. Despite extensive guidance and public and provider outreach by HHS, as well as its Right of Access Initiative prioritizing enforcement of access violations,[10] HHS continued to receive complaints by individuals facing hurdles in their ability to timely obtain PHI in the requested form and format, at a reasonable fee.[11] Access struggles can lead to issues in coordinating care and possibly contribute to poor health outcomes. The NPRM addresses the ways in which access is provided, the form and format of the PHI, access requests directing PHI to a third party, verification of the identity of the requestor, and the fees related to the provision of access to PHI.

Right to Inspect PHI

The NPRM adds a new subsection in the Privacy Rule's right of access provision that offers greater detail on an individual's right to inspect the individual's PHI. This provision describes how an individual may view their PHI and take notes, videos, and photographs, as well as use other personal resources to view and capture PHI that a covered entity holds in a designated record set.[12] The proposed modification clarifies that a covered entity is not required to permit an individual to connect

a device to the covered entity's information systems, and that the covered entity also may impose requirements on the inspection such that the individual only accesses the PHI to which they have the right to access.[13]

HHS also includes language within the NPRM that would provide individuals with the right to inspect their PHI at the point of care when the PHI is readily available; health care providers would not be permitted to delay fulfilment of a request to inspect if the PHI is readily available.[14] This would include a patient's request to view their x-ray, ultrasound, or lab results during their appointment with a health care provider. In the NPRM commentary, HHS states its belief that the time and location where an individual receives treatment "generally would be considered a convenient time and place for the individual to inspect the PHI that is immediately available in the treatment area."[15] Acknowledging the potential that this may be challenging for health care providers who treat a high volume of patients, HHS seeks comments on whether to implement limitations to prevent workflow disruptions, as well as how to determine when PHI is "readily available."[16] Without additional guidance, expanding the inspection right in this way represents a fundamental change that could have significant practical consequences for high-volume health care providers, with the potential to increase the administrative burden of clinical encounters.

Timely Response to Access Requests

HHS proposes to decrease the current response time for a covered entity to provide access to an individual's PHI from 30 days to 15 calendar days, also decreasing the extension timing from 30 days to 15 calendar days.[17] HHS also proposes that covered entities adopt a policy to prioritize urgent or other high-priority access requests, particularly those related to the health and safety of the requestor or another person, with the intent that the covered entity would limit the use of an extension for these requests.[18] The NPRM provides some examples of what would be considered an urgent or high-priority request, which include when an individual informs the covered entity that the PHI is necessary for urgent medical treatment or when a minor requires documentation of asthma in order to be permitted to bring medication to school.[19] Not every individual requesting access provides information as to the intended use of the PHI, so, if the NPRM is adopted as proposed, that will be an element that covered entities consider when developing a policy on urgent requests, particularly if HHS does not provide any further guidance.

Responding to criticism that certain covered entities wait until the end of the access response deadline before requesting clarifying information from the individual, thus delaying the response, HHS proposes to continue to allow covered entities to clarify access requests. However, the NPRM will not permit a clarification process to extend the time limit in which the covered entity must respond to the access request.[20] If the NPRM is adopted in its current form, covered entities should ensure that they have processes in place to review access requests shortly after receipt to allow for timely outreach to address any necessary clarifications.

Form of Access

The NPRM also proposes clarifications to the form and format required for a covered entity to respond to an individual's request for access to their PHI.

Summary of PHI

Under the current Privacy Rule, when an individual requests access to their PHI, a covered entity is permitted to offer a summary of the PHI in lieu of a copy.[21] Unless the covered entity is offering a summary because it is denying an individual's request for a copy of the PHI (done so in accordance with the Privacy Rule's requirements for denials), the NPRM requires the covered entity to inform the individual that the individual retains the right to obtain a copy of the requested PHI if they do not agree to receive a summary instead.[22]

Provision of Electronic Copy to PHA

HHS proposes to modify the Privacy Rule provision governing the time and manner of access to include references to electronic transmission of an individual's PHI, including via email or through the individual's personal health application (PHA) to the extent a copy of the PHI is readily producible to or through such application. The NPRM includes a definition of "personal health application" that builds on the HITECH Act's definition of "personal health record" and describes an application used by the individual to access their health information, where that information may be drawn from multiple sources, provided that the 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."[23]

If the health care provider has the ability to transmit the PHI to a patient's PHA and refuses to do so, the provider may be deemed to be improperly denying access. For example, if the provider has a secure application programming interface (API) within its electronic health records (EHR) system[24] that can be used to connect the EHR system with a patient's PHA, and refuses to transmit the electronic PHI to the patient's PHA, it may be deemed to have denied access. However, if the health care provider was willing to transmit electronic PHI to a patient's PHA via the provider's API, imposing a requirement that all applications register with the provider prior to receiving access from its API would not constitute a denial of access because the registration process is not excluding or preventing a PHA from connecting with the API.[25] If the NPRM is finalized, health care providers should ensure that any processes in place governing the electronic provision of access to a PHA do not restrict a patient's right of access.

Right to Direct PHI to Third Party

Directing Electronic PHI to Designee

Under the HITECH Act, when a covered entity maintains PHI in an EHR, an individual has the right to obtain a copy of such PHI[26] in an electronic format, and the individual has the ability to direct the covered entity to transmit an electronic copy to the individual's designee, assuming that the individual makes this designation in a clear, conspicuous, and specific manner.[27] In its Omnibus Final Rule,

HHS modified the Privacy Rule's access provision to permit individuals to direct PHI to third parties under the right of access provisions.[28] In *Ciox Health, LLC v. Azar et al.*, the U.S. District Court for the District of Columbia held that the HITECH Act granted a limited right to an individual to direct electronic PHI, held in an EHR, electronically to a third party.[29] HHS chose not to appeal the decision and, in the NPRM, HHS proposes the addition of a new section to the Privacy Rule's right of access provision that permits an individual to direct PHI to a third party, limited to only electronic copies of PHI that are maintained in an EHR, in effect codifying that aspect of the *Ciox Health* decision in the Privacy Rule.[30]

The NPRM requirement would continue to permit a written access request to direct electronic PHI found in an EHR to a third party, but the proposed regulation also permits oral requests that are "clear, conspicuous, and specific."[31] This does not appear to be a high bar to meet, as the HHS guidance explains that requests identifying the designated recipient and where to send the electronic PHI would be acceptable.[32] The NPRM also specifies that a "written" request may be in electronic form; for example, an individual may use their PHA to submit an access request directing their health care provider to send an electronic copy of their PHI to a third party.[33]

This proposed Privacy Rule modification also outlines a covered entity's unreviewable and reviewable grounds for denial of access.[34] The unreviewable grounds include if the PHI is excepted from the right of access and, with respect to an inmate, if transmitting the copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates or any officer, employee, or other person at the correctional institution or responsible for transporting the inmate. The unreviewable grounds also include temporary suspensions of the right to access during research if the research is in progress and the individual agreed to the denial of access when consenting to the research. A covered entity also may issue an unreviewable denial if the requested information contains records subject to the Privacy Act of 1974 (Privacy Act) and denial is permitted under the Privacy Act or if the PHI was obtained from a non-health care provider via confidential means and providing access would be "reasonably likely" to reveal the source of the PHI.

The NPRM also proposes two reviewable grounds for denial: (1) if 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," and (2) if the PHI makes reference to another person (excluding a health care provider) and a licensed health care professional determines, in the exercise of professional judgment, that the access "is reasonably likely to cause substantial harm to such other person."[35]

Similar to the access requirement for PHI provided directly to individuals, a covered entity may provide a summary or explanation of the PHI in lieu of transmitting a copy of the PHI to the third party designated by an individual if the individual agrees in advance to the provision of a summary or explanation, as well as any fees imposed for such summary or explanation.[36] The provider must inform the individual that the individual retains the right to direct an electronic copy of the PHI in an EHR if the individual does not agree to a summary. This would not apply if the summary is offered because the request for a copy is denied, presuming the covered entity follows the proper denial

procedures. The timing requirements for the transfer of PHI to a designated third party mirror those of the general access requirement (under the NPRM, no later than 15 calendar days, with a 15-day extension).[37]

Directing the Transfer of Electronic PHI Between Providers and Plans

The NPRM also proposes a new access provision that outlines an individual's right to direct the transfer of PHI between health care providers and/or health plans.[38] This proposed modification applies to a provider's existing or prospective new patients or current members (or dependents) of a health plan and applies only to electronic copies of PHI that are held in an EHR system. Similar to the ability to direct PHI to a third-party, an individual can direct a provider or plan to disclose electronic PHI maintained in an EHR to another provider or plan orally if the request is clear, conspicuous, and specific.[39] In its commentary, HHS states that, following receipt of a request from a patient, a provider or plan may submit the request to the designated provider or plan orally or electronically and the disclosing providers and plans may rely on existing procedures for accepting and verifying oral and electronic requests.[40]

Under the current Privacy Rule, these providers and plans have the ability to share PHI for certain permitted purposes, including for treatment of a patient or payment.[41] Covered entities also have the ability to disclose PHI pursuant to a patient's authorization.[42] Under the proposed changes to Privacy Rule's right of access provisions, the individuals can direct the covered entity's disclosure of PHI without specifying a particular purpose and subject to the timing provisions outlined in the Privacy Rule. In comparison, if an individual authorizes the disclosure of PHI through an authorization, the authorization must describe the purpose of the disclosure, and the covered entity is permitted, but not required, to disclose the PHI as requested by the individual. Further, the covered entity may be permitted to charge the individual more for providing the copies pursuant to an authorization then it would be able to under the individual's right to access.[43] As discussed above, requests subject to the access requirements in the Privacy Rule are subject to the proposed 15-calendar-day response requirement, which is not present for disclosures for treatment or payment purposes, or those made pursuant to an authorization.

Fees

The NPRM proposes a number of modifications to fees that may be charged related to access requests.

Electronic Copies of PHI

The HITECH Act limits fees that can be charged for providing an individual with a copy, or a summary or explanation, of PHI electronically; in particular, these costs are limited to the labor costs necessary to respond to the request.[44] In the NPRM, HHS proposes to exclude the costs of electronic media and postage for any access requests that require the disclosure of electronic copies of PHI (or summaries or explanations).[45]

Fees for PHI Directed to Third Parties

In its 2016 Access Guidance, OCR took the position that the access fee limitation set forth in Section 164.524(c)(4) of the Privacy Rule applied both to PHI requested by an individual and sent to the individual, as well as PHI that an individual directed a covered entity to send to a third party.[46] However, in the *Ciox Health* decision, the U.S. District Court for the District of Columbia opined that the extension of this "patient rate" for fees related to PHI provided to a third party was enacted without notice and the opportunity for comment through the rulemaking process.[47] In the NPRM, HHS proposes to apply the Privacy Rule's "patient rate" fee limitations to access requests directing copies of the individual's PHI to a third party, which include the cost of labor and preparing an explanation or summary.[48]

As discussed above, the NPRM includes a new provision allowing individuals to direct a health care provider or health plan to disclose electronic PHI to another provider or plan. In its commentary, HHS states that it is not proposing to change how covered entities charge for disclosing PHI to health plans and providers, which HHS understands frequently are not subject to charges.[49]

As information disclosures to third parties can continue to be made via individual authorization, the HHS commentary to the NPRM clarifies that covered entities responding to requests based on authorizations are not subject to the fee limitations applicable to a patient's right to access, but are subject to the Privacy Rule's limitations on the sale of PHI, as well as applicable state law.[50] The Privacy Rule limits fees for authorization-based disclosures to reasonable, cost-based fees that cover the costs to prepare and transmit the PHI, or a fee as expressly permitted by another law.[51]

No Fees Permitted

The NPRM proposes to add a requirement prohibiting covered entities from imposing fees when an individual inspects their PHI and when an individual accesses electronic PHI using an internet-based method such as a patient portal or PHA.[52] In its commentary, HHS clarifies that the fee prohibition for electronic access does not apply when an individual uses an online portal to submit a PHI request that directs the covered entity to provide access in a manner whereby the covered entity would incur supply, postage, or labor costs that may be charged under the Privacy Rule.[53]

Fee Notice

The NPRM proposes to add a new Section 164.525 to the Privacy Rule to require covered entities to provide advance notice of fees charged for PHI access requests, as well as PHI disclosed pursuant to an individual's authorization.[54] This section requires a covered entity, to the extent that it has a website, to post a fee schedule on its website and make that fee schedule available both at the point of service and upon request. The fee schedule must specify the types of access to PHI that are available to individuals free of charge, as well as the covered entity's fees for copies of PHI (electronic and non-electronic) provided to individuals, copies provided to third parties designated by the individual, and copies sent to third parties pursuant to an individual's authorization. This proposed Section 164.525 also would require a covered entity, upon request, to provide an individualized estimate of an approximate fee for providing a copy of PHI. Upon request, a covered entity also would be required to provide an individual with an itemized bill for specific charges for labor, postage, and supplies that

constitute the total fee charged for requests subject to the fee schedule described in this new section.[55] If finalized, this provision will require covered entities to provide much more transparency around fees charged for PHI copies and the makeup of such fees.

Limitations on Access Request Procedures

While covered entities are permitted to maintain certain practices surrounding the provision of access, the NPRM strives to remove any unreasonable burdens from individuals seeking access. For example, covered entities are permitted to require that individuals submit access requests in paper or electronic form and a covered entity can mandate the use of a specific form. However, the proposed regulation would prohibit an entity from requiring the completion of a form that requests information over and above what is required for the provider or plan to complete the request. Covered entities also would not be permitted to require a notarized signature or direct the specific manner through which the individual submits the request (i.e., online only, only in person).[56] Covered entities also would not be permitted to impose unreasonable measures to verify a requesting individual's identity, which may include requiring in-person proof of identity.[57] The requirements of the NPRM would mandate covered entities to find an appropriate balance of safeguarding PHI and allowing required access.

Fostering Care Coordination and Case Management

Minimum Necessary Standard

Currently, the Privacy Rule provides that covered entities must limit their internal uses, requests, or disclosures of PHI to the minimum necessary to accomplish the intended purpose of such use, request, or disclosure. As explained by HHS, the minimum necessary standard permits a covered entity to reasonably rely upon the request for PHI from another covered entity that the scope of PHI requested is what is needed by the requestor. Furthermore, although disclosures of PHI to health care providers for treatment, including for case management and care coordination, are excluded from the minimum necessary standard, internal uses of PHI for treatment must adhere to the minimum necessary standard. In addition, in those cases where the uses and disclosures of PHI for care coordination and case management by a health care provider or health plan are considered health care operations activities, the minimum necessary standard applies.

In an effort to propose consistency of disclosures for care coordination and case management purposes on an individual level, HHS proposes to add an express 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.[58] More specifically, covered entities would no longer need 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.[59] As an example, HHS states that a health care provider who

contacts a health plan to coordinate potential mental health treatment referrals for a patient would not need to consider what information is the minimum necessary to disclose to the health plan for this purpose.[60]

Health plans and covered health care providers would, however, still need to meet the minimum necessary requirements for: (1) disclosures of PHI for health care operations 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 services agencies or transitional supportive housing authorities; (3) uses of PHI for care coordination and case management, whether as part of treatment or health care operations; and (4) uses, requests, and disclosures of PHI for other purposes, including all population-based activities, when applicable.[61] HHS further points out that although the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program final rule (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 information when the Privacy Rule specifically excepts the disclosure from the minimum necessary standard, the provider could nonetheless honor an individual's request for restrictions on disclosures of PHI.[62]

Permissible Disclosures to Community Based Organizations

HHS also proposes to modify the uses and disclosures for treatment, payment, or health care operations (TPO) to clarify that covered entities may disclose PHI to social services agencies, community based organizations, Home and Community Based Services (HCBS) providers, and other organizations providing health-related services (collectively, CBO(s)), 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.[63] Under this provision, a health plan or a covered health care provider could only disclose PHI without authorization to a CBO that provides health-related services to individuals such as food or sheltered housing needed to address an individual's health risks.[64]

HHS asserts that such disclosures are already permitted under the Privacy Rule, which defines "treatment" to include "the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."[65] HHS cites to its 2018 guidance providing that "health care providers who believe that disclosures to [a social services agency] are a necessary component of, or may help further, the individual's health or mental health care may disclose the minimum necessary PHI to such entities without the individual's authorization."[66] Nonetheless, HHS notes that many covered entities' common practice is to only disclose PHI to social service agencies once that covered entity has obtained a HIPAA authorization from the individual.[67] In response to comments received from the RFI about the need for an express regulatory permission to disclose PHI to entities such as social services agencies, HHS proposes to modify 45 CFR 164.506(c) to add the following new subsection under uses or disclosures to carry out treatment, payment or health care operations:

> 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.[68]

HHS also proposes clarifying the definition of "health care operations" to make clear that it includes not only population-based care coordination and case management, but also includes individual-focused care coordination and case management activities.[69] The amendment to the use and disclosure for TPO would provide express permission for a health care provider or health plan to disclose PHI to CBOs when the provider or health plan determines that the disclosure is needed to provide health-related services to specific individuals for individual-level care coordination and case management activities that constitute either treatment or health care operations, as applicable.[70]

To the extent that the disclosures for care coordination and case management are made to business associates engaged by a covered entity, such as a health plan, to provide health-related services to an individual, the health plan would need to have a HIPAA compliant business associate agreement in place prior to disclosing the PHI for this purpose.[71] In those cases where the CBO receiving the PHI will be providing health-related services on its own behalf, and not performing covered activities or functions for or on behalf of the disclosing covered entity, a business associate agreement would not be required.[72]

Although the proposed change may provide affirmation that PHI may be disclosed for purposes of treatment or health care operations without a patient's authorization, it will not eliminate any state law consent requirements applicable to the disclosure of patient information to third parties providing services addressing the social determinants of health. Notably, HHS proposes to limit the scope of this permission to only individual-level care coordination and case management activities.[73] HHS' reasoning is that this limitation will ensure that the disclosure is "akin to disclosures for treatment, which individuals except to occur without their needing to provide an authorization or consent."[74] In its request for comments, HHS requests thoughts from stakeholders on whether care coordination and case management should exclude any population-based efforts.[75] If HHS moves forward with the disclosures for care coordination and case management for only individual purposes, such restriction may hinder data sharing among collaborations including social services agencies and health care providers that seek to use PHI in order to address social determinants of population health.

Encouraging PHI Disclosures to Address Substance Use Disorder, Serious Mental Illness, and Emergency Circumstances

HHS has posited that the support of family members, friends, and caregivers is critical for individuals experiencing substance use disorders (SUD) or serious mental illness (SMI) but such support cannot be properly provided if such people do not have access to an individual's applicable health information.

HHS noted that while it has issued guidance as required under the 21st Century Cures Act[76] and in response to the opioid epidemic, it still hears of instances where covered entities remain reluctant to disclose information to persons involved in the care of individuals who have a SMI or SUD in certain circumstances such as an emergency. In response to HHS' public input request in 2018 regarding whether and how to modify the Privacy Rule to combat the opioid crisis, treat SMI, and promote family involvement for individuals with a SMI or SUD, two types of commenters generally responded. Family member comments strongly supported that more information related to an individual's SMI or SUD should be disclosed to those involved in that individual's care. Those commenters that represented patients "universally opposed" modifying HIPAA to expand permitted disclosures or information related to SMI or SUD.[77] Nonetheless, HHS is seeking more ways to address family members' concerns and proposes modifications to the Privacy Rule to encourage covered entities to use and disclose PHI more broadly in scenarios that involve SUD and SMI and emergency situations.

HHS proposes to replace the "professional judgment" with a "good faith" standard for certain disclosures permitted under the Privacy Rule.[78] For example, currently under 45 CFR 164.510(b)(3), a covered entity may determine to use or disclose PHI of an individual when such individual is not present or the individual cannot agree or object to the use or disclosure (such as when an individual is incapacitated) so long as the covered entity in the exercise of "professional judgment" determines that the disclosure or use is in the best interest of the individual. HHS believes in part that the current "professional judgment" standard could be read to allow only licensed individuals or those with professional training to determine whether disclosure is in the best interest of the individual.[79] HHS notes that a "good faith" standard does not require a covered entity or its workforce members to have specialized education or professional education but instead assumes that such workforce members or the covered entity will draw on their experiences with an individual to make a good faith determination on what is in the best interest for an individual.[80] As an example, HHS indicated under the "good faith" standard, the front desk staff at a physician's office who have regularly seen an individual should be able to disclose PHI to an individual's family members about an upcoming appointment based on the staff's knowledge of the family's members involvement and "good faith" belief about the patient's best interest.[81]

HHS also proposes to revise the permissible disclosure requirement without an individual's authorization or opportunity to agree or object when such disclosure is to avert a serious threat to health or safety as currently provided under 45 CFR 164.512(j)(1). Specifically, HHS proposes that a covered entity can in good faith use or disclose PHI if in part it is necessary to prevent or lessen a "serious and reasonably foreseeable" threat to the health or safety of a person or the public rather than a "serious and imminent" threat.[82] HHS reasons that this change will allow covered entities to use or disclose PHI without having to analyze whether a threatened harm is imminent, which may be hard to determine.[83] HHS would also define "reasonably foreseeable" as "that an ordinary person could conclude that a threat to health or safety exists and that harm to health or safety is reasonably likely to occur if a use or disclosure is not made, based on facts and circumstances known at the time of the disclosure."[84] HHS' stated expectation is that circumstances such as a possible risk of suicide may be properly disclosed to an individual's family member even though a suicide attempt may not be imminent but is reasonably foreseeable.

In its request for comments for the above proposed revisions, HHS appears to foreshadow concerns some may have on whether such proposed revisions will lead to individuals not seeking behavioral health treatment. For example, HHS asks for comments on whether the proposed "good faith belief" standard and the change to "serious and reasonably foreseeable threat" will discourage individuals from seeking care.[85] Additionally, HIPAA does not preempt other laws, such as 42 CFR Part 2 and state laws, that are more protective of an individual's privacy. Covered entities that are licensed under state law such as behavioral health providers may have state laws more restrictive than HIPAA that will make the above proposed provisions inapplicable to them. Additionally, licensed professionals will still have to comply with their patient communication privilege laws from their licensing state. These proposed modifications may subsequently mostly affect primary care providers that are perhaps usually only subject to the Privacy Rule and not subject to stricter state laws. Since a significant portion of behavioral health care starts in the primary care setting, such proposed revisions should be carefully analyzed.

Additional Regulatory Changes

Proposed Changes to Notice of Privacy Practices (NPP)

HHS proposes eliminating the requirement that a covered entity make a good faith effort to obtain an acknowledgment that an individual received the covered entity's NPP.[86] The proposal also would remove the current requirement to retain copies of such documentation for six years.[87] In lieu of the written acknowledgement, a covered entity would need to give an individual the opportunity to discuss the NPP with a person designated by the covered entity.[88] HHS also proposes to modify the content requirements of the NPP. In this regard, HHS proposes that the NPP 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 MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED
- YOUR RIGHTS WITH RESPECT TO YOUR MEDICAL 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 MEDICAL 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 OR TITLE AT [PHONE AND EMAIL] IF YOU HAVE ANY QUESTIONS."[89]

HHS also proposes further modifying the NPP to require a description of 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.[90] Lastly, 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 their PHI is not in an electronic health record or is not in an electronic format.[91] HHS is seeking to enhance the understanding of individuals' rights as well as the potential uses of their PHI.

Telecommunications Relay Service (TRS) Programs

TRS is a federally mandated service required to provide individuals in the general public, who are deaf, hard of hearing, or deaf-blind, or who have a speech disability with facilitated telephone communication by using a communications assistant who transliterates conversations (or, in some cases, interprets using ASL).

OCR's FAQ currently states 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.[92] This is based on the premise that 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 identifying the communications assistant as involved in their care if they do not object. The FAQ also explains that the TRS provider is not acting for or on behalf of the covered entity when it provides such relay services, and therefore is not a business associate.[93]

As a result of advances in technology, the expectation that individuals would always have the opportunity to agree or object to a use or disclosure of PHI to a communications assistant is no longer true. Therefore, HHS proposes to expressly permit covered entities (and their business associates) to disclose PHI to TRS communications assistants to conduct covered functions. HHS also proposes amending the definition of a business associate to exclude TRS programs from such definition.

Use and Disclose the PHI of Armed Forces Personnel to Cover all Uniformed Services Personnel

With the stated goal of improving care coordination and case management for individuals serving in the Uniformed Services, HHS is proposing to expand to all Uniformed Services the Armed Services express permission for covered entities to use and disclose PHI for mission requirements and veteran eligibility.[94] Such disclosures would no longer require written authorization from the individual.

Effective and Compliance Dates and Comment Period

If enacted, the final rule would become effective 60 days after publication. HHS is proposing that HIPAA-covered entities and their business associates comply with the new policies and procedures within the standard 180-day period prescribed in 45 CFR 160.105. OCR enforcement for non-compliance would begin 240 days post-publication.

HHS seeks comments on the NPRM. The comment period will extend for 60 days after the NPRM is published in the *Federal Register* and comments may be submitted via mail or through the federal eRulemaking Portal.

Checklist for Implementation

If the changes to the Privacy Rule are implemented as proposed, health care providers should take note of some of the practical impacts that may require modifications to policies and processes, including:

- Post a fee schedule online for fees charged for access and pursuant to an authorization
- Adopt a policy to prioritize urgent or otherwise high-priority access requests
- Review and modify procedures related to fees for access and authorization requests
- Review procedures for access requests to ensure that processes do not require unreasonable burden
- Review and revise procedures regarding providing a summary or explanation of PHI in lieu of a copy
- Adopt a policy regarding access requests directing electronic PHI to health plans and providers
- Review or adopt a policy regarding inspection of PHI
- Review and modify policy regarding access requests directing electronic PHI to third parties
- Update Notice of Privacy Practices and eliminate process to obtain acknowledgement

The authors would like to acknowledge the assistance of Meredith LaMaster and Taylor Carter in preparing this briefing.

---

[1] As noted in the NPRM, Congress enacted in March 2020, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) which requires greater alignment of the 42 C.F.R Part 2 regulations with HIPAA. HHS will be implementing the CARES Act requirements relating to 42 C.F.R. Part 2 in a future rulemaking. U.S. Department of Health and Human Services, Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement (NPRM), p. 141, https://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf.

[2] *See* 65 Fed. Reg. 82462 (Dec. 28, 2000).

[3] *See* 67 Fed. Reg. 53182 (Aug. 14, 2002), 78 Fed. Reg. 5566 (Jan. 25, 2013), 79 Fed. Reg. 7289 (Feb. 6, 2014) and 81 Fed. Reg. 382 (Jan. 6, 2016).

[4] *See* NPRM, p. 21.

[5] *See* NPRM, p. 21.

[6] Pub. L. 111-5, 123 Stat. 115 (Feb. 17, 2009) (codified at 42 U.S.C. 201 note).

[7] 78 Fed. Reg. 5566 (Jan. 25, 2013).

[8] *See* Individuals' Right under HIPAA to Access their Health Information 45 C.F.R. § 164.524, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html (2016 Access Guidance).

[9] NPRM, p. 7.

[10] *See, e.g.,* OCR Settles Twelfth Investigation in HIPAA Right of Access Initiative, https://www.hhs.gov/about/news/2020/11/19/ocr-settles-twelfth-investigation-hipaa-right-access-initiative.html#:~:text=OCR%20announced%20this%20initiative%20as,under%20the%20HIPAA%20Privac

[11] NPRM, p. 38.

[12] NPRM, p. 348.

[13] NPRM, p. 348.

[14] NPRM, p. 350.

[15] NPRM, p. 50.

[16] NPRM, p. 51.

[17] NPRM, p. 349.

[18] NPRM, p. 349.

[19] *See* NPRM, p. 62.

[20] *See* NPRM, p. 63.

[21] *See* 45 C.F.R. § 164.524(c)(2)(iii).

[22] *See* NPRM, p. 350. Note that this requirement to inform the individual that they may receive a copy of the PHI also applies when the individual is requesting that the PHI be provided to a third party. *See* NPRM, p. 353.

[23] *See* NPRM, p. 339. HHS seeks comment on this proposed definition, including on the types of activities that are "managed," "shared," and "controlled," and HHS' assumptions about how individuals use PHAs.

[24] HHS also proposes to add a definition of "electronic health record" in 45 C.F.R. 164.501, expanding on the definition in the HITECH Act. *See* NPRM, p. 338.

[25] *See* NPRM, pp. 65-66.

[26] This does not apply to psychotherapy notes or information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative litigation. NPRM, p. 351.

[27] *See* HITECH Act, Section 13405(e).

[28] *See* 45 C.F.R. § 164.524(c)(3)(ii).

[29] *See Ciox Health, LLC v. Azar*, No. 18-cv-0040-APM (D.D.C. Jan. 23, 2020).

[30] *See* NPRM, pp. 29, 351.

[31] *See* NPRM, p. 351.

[32] *See* NPRM, p. 73.

[33] *See* NPRM, p. 73.

[34] *See* NPRM, pp. 351-352.

[35] *See* NPRM, p. 352.

[36] *See* NPRM, p. 352.

[37] *See* NPRM, p. 353.

[38] *See* NPRM, p. 354.

[39] *See* NPRM, p. 354.

[40] *See* NPRM, p. 74.

[41] *See* 45 C.F.R. § 164.502(a)(ii).

[42] *See* 45 C.F.R. § 164.502(a)(iv).

[43] *See* NPRM, pp. 68-69.

[44] HITECH Act, § 13405(e).

[45] *See* NPRM, pp. 350-351.

[46] *See* 2016 Access Guidance.

[47] *See Ciox Health, LLC v. Azar*, No. 18-cv-0040-APM (D.D.C. Jan. 23, 2020).

[48] *See* NPRM, p. 354.

[49] *See* NPRM, p. 89.

[50] *See* NPRM, p. 87.

[51] *See* 45 C.F.R. § 164.502(a)(5)(ii).

[52] NPRM, p. 351.

[53] NPRM, p. 84.

[54] *See* NPRM, p. 356.

[55] *See* NPRM, p. 356.

[56] *See* NPRM, pp. 348-349.

[57] *See* NPRM, p. 344.

[58] *See* NPRM, p. 117.

[59] *See* NPRM, p. 118.

[60] *See* NPRM, pp. 118-119.

[61] *See* NPRM, pp. 117-118.

[62] *See* NPRM, p. 119.

[63] *See* NPRM, p. 126.

[64] *See* NPRM, p. 126.

[65] *See* NPRM, p. 127.

[66] *See* NPRM, p. 122. *See also* 45 C.F.R. § 164.506.

[67] *See* NPRM, p. 200.

[68] *See* NPRM, p. 341.

[69] *See* NPRM, p. 198.

[70] *See* NPRM, p. 127.

[71] *See* NPRM, pp. 127-128.

[72] *See* NPRM, p. 128.

[73] *See* NPRM, p. 129.

[74] *See* NPRM, p. 129.

[75] *See* NPRM, p. 131.

[76] Pub. L. 114-255, 130 Stat. 1033 (Dec. 13, 2016) (codified at 42 U.S.C. 201 note).

[77] *See* NPRM, p. 142.

[78] The specific provisions are the following: 45 C.F.R. §§ 164.502(g)(3)(ii)(C), 164.510(a)(3), 164.510(b)(2)(iii), 164.510(b)(3), 164.514(h)(2)(iv).

[79] *See* NPRM, p. 145.

[80] *See* NPRM, pp. 145-146.

[81] *See* NPRM, p. 146.

[82] *See* NPRM, pp. 201-202.

[83] *See* NPRM, p. 229.

[84] *See* NPRM, p. 342.

[85] *See* NPRM, pp. 157-158.

[86] *See* NPRM, p. 163.

[87] *See* NPRM, p. 163.

[88] *See* NPRM, p. 163.

[89] *See* NPRM, p. 345.

[90] *See* NPRM, p. 203.

[91] *See* NPRM, p. 203.

[92] *See* NPRM, p. 168.

[93] *See* NPRM, p. 168.

[94] *See* NPRM, p. 205.

1099 14th Street NW, Suite 925, Washington, DC 20005 | P. 202-833-1100

For payments, please mail to P.O. Box 79340, Baltimore, MD 21279-0340