Health Industry Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Proposed Rule Would Make Far-Reaching Changes to HIPAA Privacy Regime

February 26, 2021

On January 21, 2021, the far-reaching HIPAA Privacy Proposed Rule, initially released on December 10, 2020, was published in the Federal Register.[1] Despite speculation that the publication timeline would be altered when the Biden administration came into power, the Proposed Rule has not been withdrawn and the initial comment deadline remains in effect as we move into March. In the absence of a change in course by the current administration, comments will be due March 22, 2021.

The Proposed Rule would affect how individuals may exercise their rights to access and share their protected health information (PHI), limit and adjust the fees covered entities may charge for access, introduce new concepts such as "electronic health record" (EHR) and "personal health application" (PHA) into a health information ecosystem already awash in acronyms, broaden data sharing by modifying the "minimum necessary" standard and adjusting the definition of "health care operations," and reduce administrative burdens relating to the ubiquitous HIPAA notice of privacy practices, among other changes.[2]

The Proposed Rule comes two years after the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued a broad request for information on how the agency could update the HIPAA Privacy Rule to make it easier to share PHI among health care providers, payers, patients and caregivers. The Proposed Rule also comes amidst the ongoing pandemic, during which a number of issues related to privacy and public health have taken on new significance, and follows on the heels of the sweeping HHS interoperability and information blocking rules. In this new rulemaking, OCR endeavors to remove barriers to sharing PHI the agency deemed counterproductive, support individuals' engagement in their care, and reduce regulatory burdens.

Key provisions of the rulemaking focus on:

- **Access and Fees:** Overhauling individual access rights, including major changes to the right to direct PHI to a third party, clarifying fees for access, and expanding the existing regulatory framework by adding new definitions for "electronic health record" and "personal health application."

Contact Information

If you have any questions concerning this alert, please contact:

Jo-Ellyn Sakowitz Klein
Senior Counsel
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Daniel David Graver
Counsel
dgraver@akingump.com
Washington, D.C.
+1 202.887.4562

Mallory A. Jones
Associate
jonesm@akingump.com
Washington, D.C.
+1 202.887.4259

Caroline D. Kessler
Associate
ckessler@akingump.com
Washington, D.C.
+1 202.887.4514

- **Notice of Privacy Practices:** Reducing administrative burden by eliminating the requirement for individuals to provide written acknowledgement of receipt of notice of privacy practices and updating content requirements.
- **Changes to "Minimum Necessary" and "Health Care Operations":** Loosening restrictions and providing clarifications on requests for, as well as uses and disclosures of PHI for care coordination and case management.
- **Shifting from "Professional Judgment" to "Good Faith" Standard for Certain Disclosures:** Loosening the standard for disclosure of PHI without authorization in emergency circumstances and certain other situations.
- **Uses and Disclosures to Avert Threats to Health or Safety:** Expanding the ability to use or share PHI to avert a threat to health or safety by shifting the disclosure threshold from situations involving a "serious and imminent" threat to those involving a "serious and reasonably foreseeable" threat to health or safety.
- **HIPAA Status of Telecommunications Relay Service (TRS):** Clarifying the scope of the exclusion for TRS providers.

In addition to these proposals, OCR has specifically requested comment on nearly 100 issues, including its proposed compliance deadline of 180 days after the effective date of a Final Rule.

Overview of Key Proposals

Overhauling Individual Access Rights. OCR proposes a number of changes to the individuals' right of access to PHI under 45 C.F.R. § 164.524, including:

- **Express Right to Take Notes, Videos and Photos of PHI.** OCR proposes adding a new individual access right at 45 C.F.R. § 164.524(a)(1)(ii) that would expressly permit an individual to take notes, videos and photos to capture PHI in a designated record set as part of the right to inspect PHI in person.[3] Covered health care providers would be required to allow individuals to inspect PHI in this manner during an appointment, and OCR requests comment on whether it should impose any conditions or limitations on this right to avoid workflow disruptions. Covered entities would be permitted to establish some guardrails, including prohibiting individuals from connecting flash drives or other devices directly to their information systems.

  The Proposed Rule specifically solicits comment on whether covered entities should be permitted to provide copies of PHI in lieu of in-person inspection when deemed necessary to protect public health and safety, such as during a pandemic. Interestingly, the agency found that the existing regulations do "not provide covered entities with the opportunity to deny or delay (beyond 30 days plus one 30-day extension) the right to inspect PHI in person to prevent the spread of an infectious disease, or address the ability to provide a reasonable alternative based on the need to protect the health or safety of the individual or others due to a pandemic or other health emergency."[4]
- **Shorter Timeframe for Providing PHI Access.** OCR proposes shortening the timeframe in which covered entities are required to respond to access requests under the HIPAA Privacy Rule from 30 days to 15 days. Under the Proposed Rule, covered entities would be required to provide access "as soon as practicable," but in no case later than 15 calendar days after receipt of the request, with the

possibility of one 15 calendar-day extension.[5] Covered entities would also be required to establish a policy for prioritizing urgent or other high-priority access requests, particularly those related to health and safety, in order to use any 15-day extensions.[6] OCR further clarified that any follow-up with the individual to clarify an access request would not extend the initial 15-day deadline. In other words, regardless of any needed clarifications, covered entities would be required to provide access within the prescribed timeframe.[7]

Notably, because HIPAA does not preempt state law related to the privacy of individually identifiable health information that is "more stringent" than the HIPAA Privacy Rule, covered entities would still need to comply with any state law provisions that require them to provide access in fewer than 15 days.[8] OCR would view any such state requirement as "practicable" for HIPAA purposes.[9]

- **Prohibition on Creating Certain Barriers to Access and Other Individual Rights.** OCR proposes adding an express prohibition restricting covered entities from imposing "unreasonable measures" on individuals exercising their access rights that create barriers or unreasonably delay access.[10] In the proposed regulatory text, OCR sets forth non-exhaustive examples of reasonable and unreasonable measures. Unreasonable measures cited include using a request form that solicits extensive information that is not necessary to fulfill the request or requiring the individual to submit a written request only in paper form, only in person, or only through an online portal.

  Furthermore, OCR proposes modifying the identity verification requirements set forth in the HIPAA regulations to include an express prohibition on imposing unreasonable identity verification measures on an individual.[11] The proposed regulatory text includes specific examples of unacceptable measures, such as requiring individuals to obtain notarization of requests for access and to exercise other individual rights or requiring individuals to provide proof of identity in person when a more convenient method for remote verification is practicable.[12]

- **Changes to the Right to Direct Disclosure of PHI to a Third Party.** OCR proposes creating a separate set of provisions (at 45 C.F.R. § 164.524(d)) to contain expansive changes to the individual right to direct PHI to a third party.

  OCR needed to address third party access rights because a January 2020 court ruling, *Ciox v. Azar*,[13] struck down key aspects of the existing access regulations promulgated in 2013[14] as well as elements of related guidance published in 2016.[15] The existing regulations required covered entities to transmit PHI to a third party upon request of the individual, without reference to the form of PHI.[16] In January 2020, the *Ciox* court limited the scope of this requirement to include *only* electronic PHI contained in an electronic health record.[17] The Proposed Rule would limit the scope of the individual right to direct transmission to a third party to include only electronic PHI (consistent with the ruling in *Ciox v. Azar*), but make it easier to invoke.

  Under the Proposed Rule, individuals would have the right to direct covered health care providers (but not other covered entities) to transmit an electronic copy of PHI in an "electronic health record" (EHR) directly to a third party within 15 days, subject to potential 15-day extension. Notably, the Proposed Rule specifies that covered health care providers must provide this access when the request is "clear, conspicuous, and specific," whether it be oral or in writing.[18]

Requiring transmission to a third party based on verbal instructions is fraught with the possibility for miscommunication. Moreover, the proposed changes will likely add to confusion over when HIPAA-compliant authorization versus third party access forms and processes can and should be used for disclosures to third parties.

The Proposed Rule would also expand this access right by carrying it further downstream. Under the Proposed Rule, current and prospective patients of covered health care providers, as well as enrolled members and dependents of health plans, would have the right to request that their health care provider or health plan submit an access request for electronic copies of PHI in an EHR to a covered health care provider. The first health care provider or health plan (called a "Requester-Recipient") would be required to submit clear, conspicuous, and specific requests as soon as practicable, but no later than 15 days (with no extensions available). The requirement would be limited to requests to send the electronic PHI back to the Requestor-Recipient.[19]

OCR seeks stakeholder input on a number of issues relating to these rights. Questions raised include whether providers should be required to inform individuals requesting transmission of PHI to a "personal health application" of the privacy and security risks of transmitting PHI to an entity that is not covered by HIPAA, and asking stakeholders to weigh in on the benefits or drawbacks of requiring entities to act on certain oral requests.[20]

- **New Definition for "Electronic Health Record" (EHR)**. OCR proposes to add a definition of "electronic health record" (EHR) to 45 C.F.R. § 164.501 based upon the definition of EHR in the HITECH Act with some "clarifying" additions.[21] The agency proposes to define EHR, in part (and generally consistent with HITECH), as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

  OCR proposes to deem "health-related information on an individual" as covering "the same scope of information as the term 'individually identifiable health information'" (IIHI), which is defined at 45 C.F.R. § 160.103. However, by aligning the definition with the broader defined term IIHI, instead of PHI (a subset of IIHI), this new definition would expand an EHR to include education records covered by the Family Educational Rights and Privacy Act, adult student medical records, and employment records held by a covered entity in its role as an employer.[22] Among other questions raised, OCR specifically asked for comment as to whether it should align the definition of EHR with the scope of information captured in a designated record set.

- **New Definition for "Personal Health Application" (PHA).** OCR proposes to define "personal health application" (PHA) in 45 C.F.R. § 164.501 as "an electronic application used by an individual to access health information about that individual in electronic form, which can be drawn from multiple sources, provided that such information is managed, shared and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer."[23] OCR proposes to require covered entities to provide access to PHI through an individual's PHA, if requested by the individual and "if a copy [of the PHI] is readily producible to or through such application."[24]

Importantly, PHAs would not be acting on behalf of, or at the direction of covered entities, so they would "not be subject to the privacy and security obligations of the HIPAA Rules."[25] This proposal could essentially force covered entities responding to patient access requests to disclose patients' medical records to third-party application developers providing PHAs, even though such developers would be outside the reach of HIPAA. These entities may, of course, be regulated by other authorities, such as the Federal Trade Commission (FTC) and state regulators. OCR has requested comment on the definition of PHA.

- **New Requirements Related to Access Fees.** The Proposed Rule would make changes to the provisions regarding fees covered entities may impose for providing individuals access to their PHI. Under the proposal, covered entities would be prohibited from charging a fee for certain categories of access, including in-person inspection and using a PHA to request and obtain PHI. For other categories of access, such as receiving a hard copy of PHI and requesting electronic PHI in an EHR be sent to a third party, covered entities would be permitted to charge a reasonable cost-based fee, with certain limitations.[26]

  OCR also proposes to add a new 45 C.F.R. § 164.525 that would require covered entities, upon request, to provide advance notice of fees for copies of PHI requested under the access right or via valid authorization.[27] Covered entities would be required to post their fee schedules (including certain required elements) online and make the schedule available at the point of service upon request.[28] Covered entities would also be required, upon request, to provide an individualized estimate of the approximate fee for requested copies of PHI and an itemized list of specific charges for labor as well as supplies and postage, if applicable.[29]

  Among other requests for comment, OCR solicits feedback on potential burdens to individuals associated with its access fee proposals. Specifically, OCR asks whether the rule should prohibit covered entities from charging fees for copies of PHI when requested by certain categories of individuals (e.g., Medicaid beneficiaries) or when the copies are directed to particular types of entities (e.g., entities conducting clinical research).[30] OCR also requests comment on whether it should prohibit covered entities from denying access to copies of PHI when the individual is unable to pay the access fee.

Eliminating the Requirement for Individuals to Provide Written Acknowledgement of Receipt of Notice of Privacy Practices and Updating Content Requirements. In a helpful move to reduce unnecessary administrative tasks, the Proposed Rule would eliminate the current obligation on providers to obtain written acknowledgement of receipt of the provider's Notice of Privacy Practices (NPP) and store it for six years.[31] OCR proposes to eliminate this requirement and replace it with an individual right to discuss the NPP with a person designated by the covered entity.[32]

Additionally, OCR proposes modifying the content requirements for NPPs. For example, the Proposed Rule would amend the prescribed header language, in part to reflect the new right to discuss the NPP with a designated person.[33] Among other updates, OCR also proposes several changes to bring the required statements on individual rights into alignment with the related substantive proposals.[34]

Loosening Restrictions and Providing Clarifications on the Disclosure of PHI for Care Coordination and Case Management. To promote the disclosure of PHI for care coordination and case management, OCR proposes to add an exception to the minimum necessary standard—i.e., the requirement that covered entities generally make reasonable efforts to use, disclose, or request only the minimum PHI necessary—for disclosures to, or requests by, a health plan or covered health care provider for individual-level care coordination and case management.[35]

Additionally, the Proposed Rule would add a new subsection to 45 C.F.R. § 164.506(c) to expressly permit covered entities to disclose PHI to social services agencies, community based organizations, home and community based services (HCBS) providers and other similar third parties that provide health or human services to specific individuals for individual-level care coordination and case management.[36] Health plans and covered health care providers would be permitted to make such disclosures without authorization as a treatment or health care operations activity, regardless of whether the third-party is a health care provider. OCR explains that it believes these disclosures are already generally permitted under the HIPAA Privacy Rule for treatment or certain health care operations, but that this additional, express permission would provide greater regulatory clarity.[37]

OCR also proposes to change the punctuation from commas to semi-colons in the definition of "health care operations" to clarify that the term encompasses all care coordination and case management activities, whether population-based or focused on particular individuals.[38]

Changing the Standard for Disclosure of PHI from Use of "Professional Judgment" to "Good Faith" in Emergencies and Other Circumstances. To encourage covered entities to share PHI with family members and caregivers of individuals—especially those experiencing substance use disorder, serious mental illness or an emergency situation—OCR proposes to replace the "professional judgment" standard with a "good faith" standard for certain determinations that disclosure is in the individual's best interest or otherwise appropriate. The Proposed Rule would effectuate this change through updates to five separate regulatory provisions.[39]

OCR explains that the current "professional judgment" standard could be interpreted as only permitting disclosure when a person who is licensed or can rely on professional training makes the determination that disclosure is in the individual's best interest.[40] The agency anticipates that changing the standard to "good faith" would allow for disclosure under a broader set of circumstances.[41] Importantly, the Proposed Rule would also add a presumption of compliance with the "good faith" standard when covered entities make a disclosure based on the belief that it is in the best interest of the individual with regard to the five amended provisions.[42]

Expanding the Ability to Use or Share PHI to Avert a Threat to Health or Safety. Currently, the HIPAA Privacy Rule permits covered entities to make certain uses and disclosures of PHI if they have a good faith belief that the use or disclosure "is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public," if the recipient is "reasonably able to prevent or lessen the threat."[43] OCR proposes to replace the "serious and imminent" standard with a "serious and reasonably foreseeable" standard to allow covered entities to use or

disclosure PHI without having to determine whether the threatened harm is imminent.[44]

Clarifying the Scope of Exclusion for Telecommunications Relay Service Providers. OCR proposes to clarify the scope of the exception under which covered entities and their business associates may disclose PHI to Telecommunications Relay Service (TRS) providers to conduct covered functions without a business associate agreement. OCR would implement this provision by adding a new public policy exception to 45 C.F.R. § 164.512 and updating the definition of "business associate" in 45 C.F.R. § 160.103 to expressly exclude TRS service providers from the definition of business associate.[45] OCR's goal was to help ensure that workforce members (like hospital staff) and individuals who are deaf, hard of hearing, or deaf-blind, or who have a speech disability, would be able to communicate easily using TRS for care coordination and other purposes.

Under current OCR guidance, because TRS is a public service that is available for free without the need to establish a business relationship, TRS providers are not acting for or on behalf of the covered entity and thus are not business associates. The guidance further explains that disclosure of PHI to TRS providers is permitted because patients have the opportunity to agree or object pursuant to 45 C.F.R. § 164.510(b).[46] In the Proposed Rule, OCR explains that advances in technology have made it such that patients may not be aware of the use of a TRS provider when interacting with a covered entity, such as during a phone call.[47] The Proposed Rule would codify the existing exclusion of TRS providers from the definition of business associate and clarify that covered entities are permitted to disclose PHI to a TRS provider without patient authorization, even when there is no opportunity to agree or object.

Conclusion

This Proposed Rule includes changes that reduce unnecessary administrative burdens and add clarity to the HIPAA Privacy Rule, as well as changes that appear to complicate the health information ecosphere. Many questions remain about how the proposed changes would impact individual privacy and covered entities' operations, which the agency should be encouraged to consider. For example, will requiring covered entities to honor oral requests to provide access to PHI to third parties increase the likelihood of data breaches (e.g., due to miscommunications about how much PHI to share and with whom)? And is it counter to the interoperability policy goals to create so many different defined data sets and terms, now including "electronic health record" as newly added per the proposal in addition HIPAA's traditional "designated record set," the ONC Interoperability and Information Blocking Rule's "electronic health information" (and "qualified electronic health record") and the FTC Breach Notification Rule's "personal health record"? Indeed, the agency itself raised nearly 100 questions concerning different aspects of the proposal.

Health industry participants should consider taking the opportunity to provide feedback on relevant provisions, offering support for those that are favorable as well as weighing in on those that seem problematic. The proposals are far-reaching and could have a material impact on many entities' operations.

[1] The new rulemaking sets forth modifications to the privacy regulations adopted under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (together, HIPAA), known as the HIPAA Privacy Rule.

[2] Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement; Proposed Rule, 86 Fed. Red. 6446 (Jan. 21, 2021) [hereinafter "Proposed Rule"].

[3] *Id*. at 6457–58.

[4] *Id*. at 6457.

[5] *Id*. at 6459.

[6] *Id*. at 6460.

[7] *Id*.

[8] 45 C.F.R. § 160.203(b); HHS OCR, How do I know if a state law is "more stringent" than the HIPAA Privacy Rule? (last reviewed July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/403/how-do-i-know-if-a-state-law-is-more-stringent-than-hipaa/index.html.

[9] Proposed Rule at 6459.

[10] *Id*.

[11] *Id*. at 6470.

[12] *Id*. at 6470–71.

[13] *Ciox Health, LLC v. Azar*, 435 F. Supp. 3d 30, 65 (D.D.C. 2020).

[14] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pt. 160, 164) [hereinafter "2013 HIPAA Omnibus Rule"].

[15] HHS, Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524 (2020), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html?language=es [hereinafter "2016 Access Guidance"].

[16] Specifically, the HIPAA regulations currently provide that "[i]f an individual's request for access directs the covered entity to transmit the copy of [PHI] directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual," and clarify that "[t]he individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of [PHI]." *See* 45 C.F.R. § 164.524(c)(3)(ii); *see also* 2016 Access Guidance.

[17] The *Ciox* court vacated the 2013 HIPAA Omnibus Rule to the extent that it expanded the HITECH Act's third party directive beyond requests for a copy of "an [EHR] with respect to [PHI] of an individual . . . in an electronic format." *Ciox Health, LLC v. Azar*, 435 F. Supp. 3d 30, 68-69 (D.D.C. 2020).

[18] Proposed Rule at 6463. Interestingly, regulatory language allowing covered entities to require that an individual request access to their PHI in writing would remain unchanged by the proposal. *See* 45 C.F.R. § 164.524(b)(1); *see also* Proposed Rule at 6471 (discussing covered entity obligations with respect to oral access requests).

[19] Proposed Rule at 6463–64.

[20] *Id*. at 6468–70.

[21] *Id*. at 6455. The HITECH Act defines "electronic health record" as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." 42 U.S.C. § 17921(5). Notably, this definition is different from the definition of "qualified electronic health record" set forth in the Public Health Service Act. See 42 U.S.C. § 300jj(13).

[22] *See* 45 C.F.R. § 160.103 (defining "protected health information" to exclude these categories of individually identifiable health information).

[23] Proposed Rule at 6456–57.

[24] *Id*. at 6536.

[25] *Id*. at 6457.

[26] *Id*. at 6464–67. In *Ciox*, the court held that OCR could not impose fee limitations on an individual request to send PHI to a third party without undertaking notice-and-comment rulemaking. 435 F. Supp. 3d at 66–67.

[27] Proposed Rule at 6467–68.

[28] *Id*. at 6467.

[29] *Id*. at 6467–68.

[30] *Id*. at 6469.

[31] 45 C.F.R. § 164.520(c)(2)(ii).

[32] Proposed Rule at 6485.

[33] *Id*.

[34] *Id*.

[35] *Id*. at 6474.

[36] *Id*. at 6476.

[37] *Id*. at 6477.

[38] *Id*. at 6472.

[39] OCR proposes to replace the "professional judgment" standard with the "good faith" standard in 45 C.F.R. §§ 164.502(g)(3)(ii)(C) (disclosures to a parent or guardian who is not the individual's personal representative), 164.510(a)(3)(i)(B) (facility directories), 164.510(b)(2)(iii) (disclosures to those involved in the individual's care, with the individual present and available), 164.510(b)(3) (limited uses and disclosures when the individual is not present or is incapacitated), 164.514(h)(2)(iv) (identity verification). *See* Proposed Rule at 6480–81.

[40] *Id*. at 6481.

[41] *Id*. at 6481–82.

[42] *Id*. at 6482.

[43] *Id*.; 45 C.F.R. § 164.512(j)(1)(i)(A).

[44] Proposed Rule at 6482–83.

[45] *Id*. at 6487.

[46] HHS OCR, When a covered entity, such as a doctor, uses a certified Telecommunications Relay Service to contact patients with hearing or speech impairments, is the Relay Service a business associate of the doctor? (last reviewed July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/500/is-a-relay-service-a-business-associate-of-a-doctor/index.html.

[47] Proposed Rule at 6486–87.