HIPAA Privacy Rule Changes: Just in time for the New Year?

By **Christopher S. Lockman** on November 29, 2023

In 2021, the Department of Health and Human Services (HHS) proposed changes to the Privacy Rule under the Health Insurance Portability and Accessibility Act of 1996 (HIPAA) that would significantly alter the current regulations (Proposed Rules). The Proposed Rules are supposed to be finalized in 2023. Once the Proposed Rules are finalized, covered entities – such as group health plans and health care providers – will have only 180 days to implement any required changes. With only a month remaining in 2023, we provide this summary overview of the portion of the Proposed Rule that most affects sponsors of group health plans to help them prepare for the anticipated new requirements.

Background

The HIPAA Privacy Rule[1] provides comprehensive federal protection for the privacy and security of health information about an individual, including any part of an individual's medical record or payment history, referred to as protected health information (PHI).

In coordination with its law enforcement arm, the Office for Civil Rights (OCR), HHS published a Notice of Proposed Rulemaking (NPRM) in January 2021 describing the Proposed Rules. Following the close of the comment period on the Proposed Rules in March 2021, the regulatory agenda published by the Office of Management and Budget (OMB) in 2022 stated that the Proposed Rules were scheduled to be finalized in March 2023. There has since been intervening guidance, with OCR issuing an NPRM in April 2023 prohibiting the use or disclosure of PHI to identify, investigate, prosecute, or sue entities involved in the provision of legal reproductive health care, but, to date, no announcement has been issued regarding the broader changes contained in the Proposed Rules. Accordingly, the Proposed Rules could be finalized at any time.

Proposed Changes to the HIPAA Privacy Rule

The proposed changes to the Privacy Rule that should most concern group health plan sponsors fall into two general categories: (1) changes that increase the right of individuals to access their PHI, and (2) changes that allow covered entities and

[1] The "Privacy Rule" sets forth the standards for the privacy of individually identifiable health information and is codified at 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subpart A and Subpart E.

business associates to share PHI more easily while safeguarding against a breach. HHS states that the changes align with “HHS’s Regulatory Sprint to Coordinated Care," which seeks to promote value-based care by eliminating regulatory hurdles and reducing cost barriers to providing coordinated care.

Examples of changes in the Proposed Rules that increase individual access to PHI are:

- Reducing the current deadline for allowing an individual to access their PHI from a maximum of 30 days, plus a single 30-day extension, to within 15 days of the individual’s request plus a single 15-day extension.
- Requiring covered entities to respond to certain record requests made by other health care providers and health plans when the request is directed by an individual pursuant to their right to access PHI.
- Requiring covered entities and business associates who charge a reasonable fee for copies of PHI to post fee schedules on their websites and provide fee estimates in response to an individual’s request to access PHI.
- Prohibiting covered entities from charging fees for an individual to access PHI when the individual will view the PHI in person or through “an internet-based application method.”
- Allowing an individual to take notes, photographs, and videos to more easily view and capture their PHI during in-person visits to a covered entity.
- Modifying the required content of the Notice of Privacy Practices (NPP), which is a notice designed to inform individuals about their rights and protections under HIPAA, by including information in the heading about how individuals can access their PHI, ask questions about their PHI, and file a complaint.

Examples of changes in the Proposed Rules that are intended to encourage coordinated care are:

- Amending the definition of "health care operations" through a punctuation change to clarify that PHI may be disclosed for care coordination and case management activities, not only for an entire population but also for activities that concern particular individuals.
- Creating a new exception to the minimum necessary standard, which generally requires covered entities to limit the use and disclosure of PHI to the "minimum necessary" needed to accomplish the purpose of the use or disclosure for situations when health plans or providers make disclosures for care coordination and case management that concern particular individuals.
- Replacing the "exercise of professional judgment" standard that appears in five places in the Privacy Rule with a lower "good faith belief" standard to permit covered entities to make certain disclosures in the best interest of individuals.
- Changing the standard regarding disclosures of PHI to avert a threat to health and safety to "serious and reasonably foreseeable" from the stricter "serious and imminent" to allow covered entities to disclose PHI without having to determine whether a threatened harm is "imminent."

Conclusion and Recommended Actions

The most recent HIPAA Omnibus Rule was published in January 2013, and given the changes in the healthcare marketplace and technology since then, the new round of updates feels timely. Nevertheless, change creates an administrative burden for group health plan sponsors, and we hope this summary will help plan sponsors avoid being caught off guard by the Proposed Rules. In addition to acquiring a general understanding of the Proposed Rules, plan sponsors should take the following actions to prepare in the event the Proposed Rules are finalized in their current form:

- Reach out to internal resources and vendors who assist with HIPAA compliance to ensure the plan sponsor will be made aware of the date final rules are issued and can timely implement the required changes.
- Reach out to their group health plan's business associates to ensure the business associates will timely implement the required changes.
- Plan to amend their HIPAA privacy policies and procedures document(s), NPP, and template forms to reflect the required changes.

- Work with internal resources and external vendors, as needed, to update HIPAA training materials so that retraining on HIPAA policies and procedures can be provided within a “reasonable time” following the effective date of the changes, as required by the HIPAA Privacy Rule.

If you have questions regarding the Proposed Rules or would like additional information regarding the HIPAA Privacy Rule, please contact a member of Verrill’s Employee Benefits & Executive Compensation Group.

Christopher S. Lockman
Partner
T (207) 253 4712
email