December 18, 2023

Looking Forward to 2024 for HIPAA Privacy

by Martha L. Sewell

Over the last two years, the Office for Civil Rights ("OCR") has released a number of proposed regulations and new guidance relating to the HIPAA privacy rules. Not to be left out, recently, the Federal Trade Commission ("FTC") has also proposed updates to the health breach notification rule. This article will list and discuss each update and set forth its current status as it affects health plans and other stakeholders.

HIPAA Privacy Coordinated Care and Individual Engagement Proposed Regulations

In the last days of the Trump Administration, OCR issued proposed regulations intended to improve coordinated care and increase engagement in an individual's own health care. See, 86 Fed Reg 6446 (January 21, 2021). Comments were due in March 2021. Since that time, OCR has been relatively silent about the current status of these proposed regulations. However, informally, we understand that they intend to finalize the proposed regulations in 2024 – but potentially not exactly in their proposed form.

The proposed regulations would make a number of changes to the situations in which a provider or plan could release PHI without the individual's written authorization. These situations typically involve emergencies, health crises, serious mental illness and substance use disorder crises. The goal is to achieve a greater coordination of care among providers. To further promote this goal, the proposed regulations would adopt an exception to the minimum necessary standard for care coordination and case management.

The proposed regulations also include several proposed revisions relating to the right to access PHI, including the following –

- Shortening a covered entity's required response time to an access request to no later than 15 calendar days (from the current 30 days),
- Removing barriers to sharing electronic PHI by allowing individuals to request that covered entities share electronic PHI directly,

- Strengthening individual rights to inspect PHI in person, and
- Requiring covered entities to post estimated fee schedules on their websites for access requests.

Last, the proposed regulations make a number of revisions to the Notice of Privacy Practices ("NPP") requirement, as follows –

- Eliminating the requirement for a provider to obtain an individual's written acknowledgement of the receipt of a provider's NPP, and
- Modifying the required wording of an NPP, including changes in the access rights noted above, changes in the situations in which PHI can be shared without written authorization as noted above, and other changes to the form, format and contact information requirements of the NPP.

If the above proposals are adopted in their current form, health plans and business associates would be required to update their HIPAA policies and procedures, NPP, and potentially business associate agreements, as applicable.

Online Tracking Guidance

Just in time for the holiday season last year, OCR issued guidance under the HIPAA privacy rules for the use of online tracking technologies by HIPAA covered entities and business associates (the "Online Tracking Guidance"). See, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (December 1, 2022). From the moment it was issued, the Online Tracking Guidance was controversial – not only for its purported requirements – but also for its sweeping application. The controversy has recently reached a fever pitch and culminated in a recent lawsuit filed by the American Hospital Association and various other regional hospitals against OCR to enjoin OCR's enforcement of the guidance (the "Complaint"). See, Case 4:23-cv-01110-P, filed on November 2, 2023 in the United States District Court for the Northern District of Texas.

Tracking technologies collect information and track users in various ways, many of which are not apparent to the website or mobile app user. Websites commonly use tracking technologies such as cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts to track and collect information from users. Mobile apps generally include/embed tracking code within the app to enable the app to collect information directly provided by the user, and apps may also capture the user's mobile device-related information.

In general, the Online Tracking Guidance recognizes that the tracking technologies obtain information, such as an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such

information collected on a covered entity's website or mobile app is PHI pursuant to the Guidance, even if the individual does not have an existing relationship with the covered entity and even if the information, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. OCR provides that when a covered entity collects the individual's information through a website or mobile app, the information connects the individual to the entity, and thus relates to the individual's past, present, or future health or health care or payment for care.

This is a sweeping statement because it does not simply relate to information obtained behind a login wall, such as when a patient logs in to the patient's account on a provider website. But, rather also to the public facing website of the entity. For example, if an individual searches "strep throat" and clicks through to a provider's public website which discusses in general terms what is strep throat, its causes and treatment options, all information gleaned from that web encounter must be treated as PHI, even if all the provider has is the individual's IP address and geographic location from the use of a tracking technology. If the provider uses a vendor to operate its public website, this would make the vendor a business associate, requiring a business associate agreement.

This out-of-the-blue Online Tracking Guidance was issued apparently without consulting any covered entities or business associates. Eleven months later, the American Hospital Association and other regional hospitals sued OCR to enjoin its enforcement of the Online Tracking Guidance. A number of key points can be gleaned from the Complaint. First and foremost, the Complaint alleges and provides proof that the federal government's own websites that are subject to HIPAA also violate the Online Tracking Guidance, including medicare.gov, the veterans' administration and the department of defense health system. The Complaint states that OCR has done nothing to enforce the Online Tracking Guidance against these entities. This lawsuit has just been filed and currently is only in the initial stages of litigation. However, covered entities and business associates should keep a close eye on this litigation as it progresses.

HIPAA and Part 2 Proposed Regulations

OCR in coordination with the Substance Abuse and Mental Health Services Administration issued proposed regulations to update the decades old regulations on the confidentiality of substance use disorder records (referred to as "Part 2" as in 42 CFR Part 2). See, 87 Fed Reg 74216 (December 2, 2022). The Part 2 proposed regulations are sweeping in nature and should be finalized in 2024.

Some health plan sponsors may have not heard of the Part 2 regulations before. Part 2 imposes different requirements for substance use disorder treatment records protected by Part 2 than the HIPAA privacy rules. The regulatory schemes apply to different types of entities and create dual obligations and compliance challenges for HIPAA covered entities and business associates that maintain PHI and Part 2 records, and thus are subject to both sets of rules. In the proposed regulations, OCR intends to revise the Part 2 regulations to

reflect applicable standards in the HIPAA privacy rules, and reflect language used in the HIPAA privacy rules. OCR also proposes to revise the NPP to clarify how Part 2 and the HIPAA privacy rules align.

Even with the above proposals, Part 2 still only applies to those providers and business associates who have substance abuse treatment records. For self-insured health plan sponsors, this typically means that Part 2 will be discussed in an EAP business associate agreement for example. Because self-insured health plan sponsors are responsible for HIPAA privacy compliance, the revised Part 2 regulations may need to be addressed in the HIPAA policies and procedures due to the revised interaction between Part 2 and the HIPAA privacy rules. The NPP also will need to be updated as well. Last, conservative health plan sponsors will want to address the Part 2 regulations in their health plan HIPAA privacy plan document language. This is because technically the sponsor could obtain the records as part of plan administration. So, a blanket statement that a health plan sponsor does not maintain or create any records that are subject to Part 2 should be sufficient to indicate that Part 2 should not apply to a self-insured sponsor, as it relates to HIPAA plan administration.

HIPAA Proposed Regulations regarding Reproductive Health Care

In April 2023, OCR issued HIPAA privacy proposed regulations to strengthen reproductive health care privacy. See, 88 Fed Reg 23506 (April 17, 2023). These proposed regulations were issued in response to the United States Supreme Court's ruling in *Dobbs v. Jackson Women's Health Organization*, which pushed the purview of abortion regulation back to each individual state. These regulations should also be finalized in early 2024.

Health Breach Notification Rule Proposed Regulations

The FTC recently issued proposed regulations to the health breach notification rule ("HBNR"), including a proposal to clarify the HBNR application to health applications and similar technologies. See, 88 Fed Reg 37819 (June 9, 2023).

As background, the HBNR requires vendors of personal health records ("PHR") and related entities that are not covered by the HIPAA privacy rules to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data. It also requires third-party service providers to vendors of PHRs and PHR-related entities to provide notification to such vendors and PHR-related entities following the discovery of a breach.

In general, a PHR is an electronic record of health information on an individual that has the technical capacity to draw information from multiple sources. Even if a HIPAA covered entity provides a PHR to an individual, that covered entity will only be subject to the HIPAA privacy rules (including the HIPAA breach of unsecured PHI rules), and not the HBNR. Thus, only entities that are not covered by the HIPAA privacy rules are subject to the HBNR.

The HBNR proposed regulations include a number of revisions, including the following –

- Revising several definitions to clarify the HBNR's application to health apps and similar technologies not covered by the HIPAA privacy rules.

- Clarifying that a "breach of security" under the HBNR includes an unauthorized acquisition of identifiable health information that occurs as a result of a data security breach or an unauthorized disclosure.

- Revising the definition of "PHR related entity" in ways that pertain to the scope of the HBNR. For example, it makes clear that only entities that access or send unsecured PHR identifiable health information to a personal health record qualify as PHR related entities subject to the HBNR.

- Expanding the required content that should be provided in the notice to consumers. For example, the notice would be required to include information about the potential harm stemming from the breach and the names of any third parties who might have acquired any unsecured personally identifiable health information.

Conclusion

As noted above, there are a number of proposed regulations and other guidance affecting covered entities and business associates that are in a state of flux. Therefore, health plan sponsors should stay tuned to these developments, as 2024 is shaping up to be a pivotal year for HIPAA privacy.