DORSEY
DORSEY+WHITNEY LLP

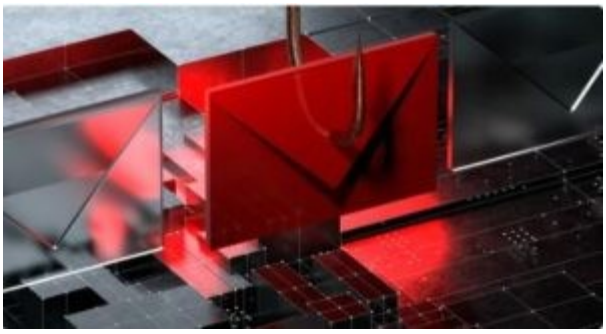
HIPAA on the Horizon in the New Year: Important Lessons from an Active 2023 and Regulatory Initiatives to Watch for in 2024

January 3, 2024 – Dorsey Health Law
by Alissa Smith and Seamus Taylor

2023 marked 20 years since the first compliance deadline under the Health Insurance Portability and Accountability Act's ("HIPAA") privacy rule. Despite the two decades of experience with HIPAA, compliance continues to remain a challenge for HIPAA-covered entities as well as for their business associates. 2023 brought a large number of important HIPAA-related developments and lessons-learned that privacy/security officials and health care attorneys should be aware of when planning for HIPAA compliance activities in 2024.

This article features lessons learned in some of the most significant HIPAA-related enforcement actions and guidance documents from the U.S. Department of Health and Human Services' Office for Civil Rights' ("OCR") in 2023, and ends with a summary of some of the ongoing OCR regulatory initiatives to monitor in 2024.

OCR's First Enforcement Action Related to a Phishing Attack



On December 7, 2023, the OCR announced a $480,000 settlement with Lafourche Medical Group ("LMG"), a Louisiana-based medical group specializing in emergency medicine, occupational medicine, and laboratory testing. The settlement marks the first time that OCR resolved a phishing attack under HIPAA. According to OCR Director Melanie Fontes Rainer, phishing is "the most common way that hackers gain access to health care systems to steal sensitive data and health information."

In March 2021, a staff member of LMG was the victim of a phishing attack that compromised the staff member's email account containing the electronic protected

Related People

- Alissa Smith

Related Capabilities

- Healthcare & Life Sciences
- Healthcare Transactions & Regulations
- Healthcare Litigation
- Medical Devices

health information ("PHI" or "ePHI") of as many as 34,000 patients. LMG reported the incident to OCR in May 2021, and OCR began its investigation in January 2022. After OCR investigated the breach, it determined that LMG had failed to comply with the following basic HIPAA requirements: (i) conducting a risk analysis to determine vulnerabilities to PHI, and (ii) creating and maintaining policies and procedures to regularly review information system activity and to safeguard PHI against cyberattacks. As a result of these findings, LMG entered into a resolution agreement with OCR on November 3, 2023, which requires LMG to pay a $480,000 penalty to OCR and implement a two-year corrective action plan ("CAP") to address the HIPAA violations identified in OCR's investigation. As part of the CAP, LMG has agreed to undertake HIPAA compliance activities that are required of health care providers:

- Establish and implement security measures to reduce security risks and vulnerabilities;
- Develop, maintain, and revise written policies and procedures as necessary to comply with HIPAA; and
- Provide training to all staff members who have access to patient PHI on HIPAA policies and procedures.

OCR's report of this first-of-a-kind settlement noted that in 2023 (through November), based on data breaches reported to it, over 89 million individuals had been affected by large data breaches (those involving 500 or more individuals). This was up from 2022, in which over 55 million individuals were affected by these large data breaches. To drive home the significance of OCR's enforcement action, OCR noted in its press release about the settlement, "Phishing attacks can result in identity theft, financial loss, discrimination, stigma, mental anguish, negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's protected health information."

Lesson learned: Covered entities should regularly update and review the risk analysis and ensure the organization has adopted business grade security measures to protect ePHI. Covered entities should also routinely review and update written HIPAA privacy and security policies and procedures, and, most importantly, deliver frequent staff training to ensure staff remain vigilant and skeptical of any suspicious emails or other contact, and report the emails or other contact immediately to the privacy and security officers. Staff training is a critical line of defense against phishing attacks.

Embedded Tracking Technologies- HIPAA Covered Entities and Business Associates Should Carefully Review Their Websites

In December 2022, OCR issued a bulletin that warned HIPAA covered entities and business associates against the use of embedded

tracking technologies that could track individually-identifiable health information on the covered entities' or business associates' websites. OCR defined "tracking technology" as "a script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app." While some covered entities track online user activity internally, many covered entities contract with third-party analytics companies to track and analyze the data about the individual users' access to and interaction with the covered entity's website. Common third-parties used to track website use data include: Meta Pixel, Google Analytics and Adobe Analytics. Tracking technologies allow the covered entity to gain insights about users' online activities for marketing purposes, and to help improve patient experience on the website and to improve patient care, among other reasons. However, the third-parties who track the data are also able to use the data to target ads and to otherwise profile the users.

The guidance points out that individually identifiable health information (such as a person's appointment date, home or email address, or IP address) is "protected health information" that is governed by HIPAA, even if the individual does not have a pre-existing relationship with the covered entity and even if the information does not include sensitive information like treatment information, diagnosis or billing data. As OCR noted in its guidance, the risk that the data being tracked is HIPAA-protected PHI is highest on those portions of a covered entity's website that have user-authenticated pages (where the individual logs in) because the information on those pages are more likely to include sensitive health information like diagnosis, prescription and other treatment information. OCR's bulletin warned that the use of individually identifiable health information that is tracked on a covered entity's website must be in compliance with HIPAA's privacy and security rules. This means, for example, that any third-party data tracker/analyst who the covered entity engages must have a written business associate agreement in place with the covered entity.

Prior to, and after OCR's bulletin, twenty or more class action lawsuits were filed against hospitals and health systems across the U.S. based on allegations that the hospitals were inappropriately sharing patient data with companies like Google, Facebook, Adobe and others for marketing purposes. Some of the cases have settled and others are ongoing.

In response to the OCR bulletin, hospitals and health systems expressed alarm due to the proliferation of the use of website data trackers in use at nearly every hospital in the nation. Some have joined a legal challenge against the OCR bulletin. In November 2023, the American Hospital Association, the Texas Hospital Association and others filed suit against OCR claiming that the OCR bulletin improperly imposes HIPAA restrictions on information that is not "protected health information" as that term is defined under HIPAA.

In February 2023, the Federal Trade Commission ("FTC") began enforcing a lesser-known law called the FTC Health Breach Notification Rule (the "HBN Rule") against companies that use website-embedded tracking technologies and disclose the data being tracked through these technologies to third-party tracking companies. The HBN Rule applies to non-HIPAA covered entities that are vendors of personal health records

(or who are a related entity or service provider of a vendor of personal health records). The HBN Rule requires that a breach notification be filed with the FTC if there is an unauthorized disclosure of personal health information, such as to a third party that has embedded tracking technologies on the company's website. Under this law, the FTC took enforcement action against well-known companies such as BetterHelp, GoodRx and Premom, requiring the payment of large civil money penalties and requiring that the companies adopt and enforce internal prohibitions on sharing user health data with third parties for advertising purposes. Additionally, the FTC issued industry guidance as a warning to others who use embedded tracking technologies on their websites.

In July 2023, the OCR and FTC teamed up and issued a joint letter to 130 hospitals and telehealth providers about the risks and concerns regarding the use of the website tracking technologies, and issued a press release with a general warning to the hospital system and telehealth industry against the use of embedded tracking technologies.

Lesson learned: HIPAA covered entities should carefully review their websites to ensure that any third party with embedded tracking technologies has signed a HIPAA-compliant business associate agreement, and to ensure that the use or disclosure of any data gleaned from tracking access to the company website is compliant with the HIPAA privacy rule. See our prior articles on this topic here and here.

Rights of Access Initiative- Still a Top Priority for OCR

In 2023, the OCR reached several new resolution agreements with entities alleged to have violated patients' rights to timely access of their medical records. Under HIPAA, covered entities, like health care providers and payors, have a maximum of 30 days (which OCR describes as an "outer limit") to provide patients with a copy of their medical record upon request. The "Right of Access Initiative" became an enforcement priority for OCR at the end of 2019, in an attempt to address patient complaints about difficulties they encountered in obtaining timely copies of their medical records. In fact, OCR's final resolution agreement of 2023 in the amount of $80,000 marked OCR's 46th such settlement in a little over three years. In response to what OCR views as a widespread issue of non-compliance, OCR has published guidance for covered entities' implementation of this individual HIPPA right to access.

Lesson learned: Review and audit the administrative processes your organization has in place for responding to requests for patient records to ensure they meet HIPAA's requirements.

Major Source of Risk: Covered Entity and Business Associate Failure to Conduct Enterprise-Wide Security Risk Analysis

In May and June 2023, OCR entered into resolution agreements with two separate business

associates who, in similar fact patterns, were found to have lacked a sufficient enterprise-wide risk analysis of their security function, leading to the breach of hundreds of thousands of patient records. In one situation, the business associate provided billing, coding and IT services to health care providers and, through a compromise in the business associate's systems, the PHI of hundreds of individuals was exfiltrated from an unsecured server by an unauthorized person. In the other situation, a business associate that provides practice management, practice analytics and revenue cycle management services to health care providers inadvertently allowed a file transfer protocol ("FTP") server containing hundreds of thousands of individuals' data to be openly accessible on the internet.

OCR also cited a covered entity for non-compliance with the risk analysis standard. In February 2023, OCR entered into a resolution agreement with a large health system in order to resolve a data breach impacting 2.81M individuals following a hacking incident. When OCR investigated the incident, it found that the health system lacked a risk analysis to determine the risks and vulnerabilities to its patients' ePHI. OCR also found a number of important security rule violations that stemmed from the initial failure to conduct risk analyses, including failing to implement an authentication process, failing to monitor the activity of users on the system, and failure to have security measures in place for ePHI that was being transmitted electronically.

In September 2023, OCR and the Office of the National Coordinator for Health Information Technology ("ONC") published an updated version of a do-it-yourself security risk assessment tool, intended for small and medium-sized covered entities. The updated tool is intended to make it easier for covered entities and business associates to assess the security risk to ePHI and to mitigate that risk.

Lesson learned: In resolution agreements, OCR routinely cites companies for failing to complete an enterprise-side security rule risk analysis. In fact, this is one of the most common sources of HIPAA violations that lead to subsequent settlement agreements with OCR. The bottom line is that there is no substitute for an enterprise-wide security rule risk analysis. This type of risk analysis should be conducted routinely by covered entities and by their business associates in order to identify and mitigate the security risks to all repositories of electronic PHI. Another lesson that comes out of this pair or resolution agreements in 2023 is that covered entities should carefully vet and audit the HIPAA compliance program and practices of their potential and current business associates. In the end, although business associates have their own liability under HIPAA, the patient data and patient relationships at risk are those of the covered entity served by the business associate.

Even Small Breaches Can Result in Liability

In 2023, OCR settled two cases that contained fact patterns OCR has addressed in guidance and settlement agreements repeatedly: snooping and social media breaches. Notably, these cases each also involved a small number of patients, and the enforcement actions signal to covered entities and business associates that even small breaches can result in liability. One resolution agreement was with a hospital related to

its security staff snooping in patient records. The other resolution agreement was with a physician practice that responded to a negative review on Google in a way that acknowledged the patient relationship and disclosed patient information.

Lessons learned: Ongoing staff training regarding impermissible uses and disclosures of patient information is a critical element of a provider's HIPAA compliance activities. Include basic reminders in HIPAA workforce training through, for example, use of the resolution agreements in the way that OCR intends them to used- as an example for others to help prevent similar conduct in the future.

COVID-19 HIPAA Enforcement Discretion Ends and OCR Emphasized its Enforcement Priority and Strategy for Cybersecurity

In August 2023, years of HIPAA-related enforcement discretion by OCR related to the COVID-19 pandemic came to an end. The enforcement discretion that OCR exercised throughout the early days of the COVID-19 pandemic related to matters such as the use of non-HIPAA compliant telehealth technologies, and non-HIPAA compliance related to COVID-19 vaccine patient scheduling, public health and health oversight disclosures, and community based testing sites. OCR published notifications and guidance to the public to prepare HIPAA covered entities and business associates for an end to the waiver of enforcement discretion.

OCR also announced the development of a new enforcement division at OCR, called the Health Information Privacy, Data and Cybersecurity Division, which will focus on OCR's work and role in cybersecurity. Additionally, citing a 93% increase in large data breaches due to cybersecurity events between 2018-2022 (with a 278% increase in large breaches involving ransomware), the Department of Health and Human Services published a concept paper outlining the Department's cybersecurity strategy for health care providers. The strategy calls for new voluntary health care-specific cybersecurity goals; developing incentives and supports with Congress that will be used to help hospitals improve cybersecurity; and strategies for increasing accountability and coordination within the health care sector.

Ongoing OCR Regulatory Initiatives- Changes are Coming

OCR has introduced several HIPAA regulatory initiatives that are still under consideration by the agency, and many of which may become finalized in 2024. It is important for privacy/security officials and health care counsel to be familiar with the proposed regulations in order to understand OCR's perspective because that helps in steering internal compliance protocols, training and accountability at the organization:

1. Reproductive Health Care

OCR issued a Notice of Proposed Rulemaking ("NPRM") on April 12, 2023 to prohibit the use or disclosure of PHI to identify, investigate, prosecute, or sue patients, providers, and others involved in the provision of legal reproductive health care, including abortion. The public comment period closed on June 16, 2023 and OCR received over 25,000

comments. A final rule has not yet been published.

2. Substance Use Disorder ("SUD") Treatment Records

In coordination with the Substance Abuse and Mental Health Services Administration (SAMHSA), OCR issued a NPRM on November 28, 2022 to align certain aspects of 42 CFR part 2 (Part 2) with HIPAA. Part 2 protects patient records maintained in connection with substance abuse education prevention, training, treatment, rehabilitation or research in order to ensure privacy for SUD patients. The public comment period closed on January 31, 2023 and OCR received over 200 comments. A final rule has not yet been published.

3. HITECH Request for Information ("RFI") Regarding Mitigating Security Practices and the Sharing of Monetary Settlements with Individuals Harmed

OCR published a RFI on April 6, 2022, seeking public input on portions of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The RFI specifically requests input on: (i) recognized security practices that OCR will consider when determining potential fines, audit results, or other remedies for resolving potential violations of HIPAA; and (ii) the methodology under which an individual harmed by a potential HIPAA violation may receive a percentage of a monetary penalty/settlement collected with respect to such violation. The public comment period closed on June 6, 2022. OCR has yet to announce further action on this RFI.

4. HIPAA Privacy Rule Updates

OCR issued a NPRM on January 1, 2021 to modify the HIPAA Privacy Rule to encourage patient engagement in health care, remove barriers to coordinated care, and decrease regulatory burden. The public comment period closed on May 6, 2021 and OCR received over 1,300 comments. A final rule has not yet been published.

The proposed new rules, if finalized, would require some significant changes at HIPAA covered entities and business associates, such as: allowing patients to inspect their PHI in person and take notes or photographs of their PHI; changing the maximum time to provide access to PHI from 30 days to 15 days; new rules about costs for records including certain circumstances when ePHI must be provided at no cost, requirements to provide estimates of fees for copies, and requirements to post fee schedules for records access on the website; individuals will be permitted to request that their PHI be transferred to a personal health application or direct ePHI to be send to another covered entity; covered entities will be required to inform individuals that they

have the right to obtain or direct copies of their PHI to a third-party when a summary of PHI is offered instead of a copy; the requirement for HIPAA-covered entities to obtain written confirmation that a Notice of Privacy Practices has been provided will be removed; covered entities will be allowed to disclose PHI to avert a threat to health or safety when harm is “seriously and reasonably foreseeable” (as opposed to the current, more stringent standard that only allows such disclosure when harm is “serious and imminent," and expansion of permissible uses and disclosures by covered entities based on care coordination, case management and based on a good faith belief that the disclosure it is in the best interest of the individual.

While the pending HIPAA updates are intended to ease the administration burden on HIPAA-covered entities in the long run, there will be a significant short term burden associated with changes to policies and procedures, changes related to notices of privacy practices, changes to medical record access processes and others.

The authors will continue to monitor these initiatives for updates and changes in 2024. If you have any questions about HIPAA, cyber-attacks, OCR investigations, or regulatory changes, reach out to your regular Dorsey attorney or to any member of the Dorsey & Whitney LLP Healthcare Transactions and Regulations practice group.