HIPAA Risks That You Might Not Have Expected

We find ourselves 20 years since the effective date of the HIPAA Security Rule and most health care providers, including pharmacies, appreciate that the requirements of HIPAA must be incorporated into day-to-day operations. Nevertheless, there has been enormous changes in legislation, enforcement and technology in those 20 years, and HIPAA simply does not look the same as when it was original enacted. Where once pharmacists worried about handing patients the wrong paper instruction or ensuring that patients did not stand too close as to overhear another patient's information, the concerns are now ensuring patient access to information and preventing hackers from encrypting entire IT systems for bitcoin. The following are some of the most important HIPAA and HIPAA-related topics in 2023.

PATIENT ACCESS

The United States Department of Health and Human Services, Office of Civil Rights ("OCR"), which is responsible for enforcement of HIPAA, has announced 45 enforcement actions related to failure of providers or health plans to provide patients with timely access to their information (referred to in HIPAA as "Protected Health Information" or "PHI"). Each of these cases involved only one or two patient complaints and settlements or penalties ranged from $1500 to $240,000. Here is what we have learned from these enforcement actions.

- Take Patient Access Seriously. In many of these cases, staff simply did not prioritize a patient requests for copies of their PHI or did not understand their obligations to respond to such requests. HIPAA requires that patients have a right to request copies of their PHI and to receive such copies within 30 days. Other Federal and state laws may require that PHI be provided even more quickly. There are some exceptions to this requirement, but such exceptions are very narrow and often require that patients be offered the opportunity to appeal. A simple way to avoid running afoul of patient access requirements is to have policies that address patient right to access, educate staff regarding their obligations, and have clearly assigned staff responsible for responding to such requests .
- Do Not Require a Specific Form to Be Completed. When HIPAA was originally implemented, most providers decided that in order to release PHI, a patient authorization form needed to be completed, regardless of where the PHI was sent or for what purpose. The OCR now maintains that asking for patients to complete authorization forms in order to access their own PHI is unduly burdensome and cannot be required. Although providers can require that patient access requests be in writing, there **cannot be a requirement** that a specific form be used.
- Understand Who Can Access PHI. HIPAA recognizes that in some instances, particularly when a patient lacks capacity, a personal representative can "step into the shoes" of the patient to assume the rights of the patient, including the right to access PHI. HIPAA defers to state law in determining who qualifies as a personal representative, but it is essentially anyone who has the right to make health care decisions on behalf of the patient (including deceased patients). For example, in New York, the public health law specifically states that family members in a specific order (e.g., spouse, child, parent, sibling) are considered to be personal representative of a deceased patient. In order to ensure that the right people have access to PHI, pharmacies should be familiar with state laws regarding individuals who are authorized to make health care decisions on behalf of a patient.
- Do Not Overcharge. Both HIPAA and most state laws allow providers to charge a fee to provide copies of PHI. Such charge must be a reasonable cost based fee for preparing and sending the PHI. Many states have long-established charges for providing paper records, and to date there have not been enforcement actions based upon reliance on such state-mandated fees for paper records, although the OCR could arguably pursue enforcement if the fees are not cost-based. HIPAA also requires providers to produce records in electronic format (e.g., on an encrypted CD or by email) if requested by the patient. The OCR has stated that it estimates the cost for producing electronic PHI to be around $6.50 unless the provider can document evidence that the cost was higher.

PHISHING/RANSOMWARE ATTACKS

Phishing attacks occur when a third party (often referred to as a hacker) exploits and manipulates human behavior in order to access IT systems and information. The hacker generally pretends to be an individual or organization that the victim trusts, like a package delivery services or the IRS, and creates a sense of urgency to rush the victim into taking a particular action, such as

continued on page 19

HIPAA Risks

From page 18

clicking on a link embedded in an email or disclosing a user name and password. This then results in the hacker introducing a virus into the individual's IT system. Although there are various dangerous viruses that can be introduced, ransomware attacks have become the virus of choice.

A ransomware attack is a type of malicious software designed to block access to a computer system until a sum of money is paid. Typically the malicious software encrypts an entire server or even an entire IT system and the hacker demands a payment in bitcoin in order to turn over the de-cryption key or refrain from posting PHI that has been exfiltrated. There are strategies, other than paying the ransom, that can be used to address a ransomware attack (e.g., using data backups). However, the OCR has stated that victims of a ransomware attack must treat the incident as a potential breach of unsecured PHI, unless it can be demonstrated through forensic analysis that PHI was not accessed. Just as a reminder, breach of unsecured PHI, particularly those breaches involving more than 500 individuals, require numerous notifications to be made including to the affected individuals, the OCR, and in some instances, the media. Furthermore, we are increasingly seeing that large breaches result in class action suits that are even more costly than potential HIPAA penalties

The most important step in preventing phishing and ransomware attacks is to educate staff that they should not be clicking on links from people or entities that they do not know. In addition, installation of anti-virus software, review of system activity and a strong incident response plan can go a long way in reducing the likelihood or costs of such attacks.

TRACKING TECHNOLOGIES

The OCR has been increasingly focused on concerns surrounding tracking technologies. Online tracking technologies, like Google Analytics or Meta Pixel, collect and analyze information about how internet users are interacting with a websites. The HIPAA Rules apply when the information that providers collect through tracking technologies or disclose to tracking technology vendors includes PHI.

The OCR views webpages as either authenticated or unauthenticated. Authenticated websites require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. Authenticated websites pose the greatest risk of exposure and providers must take steps to ensure that any user-authenticated webpages that include tracking technologies are in compliance with the HIPAA. Most notably, providers must be sure to enter into a business associate agreement with third parties that receive PHI as a result of tracking technologies.

Unauthenticated webpages that contain tracking technologies pose less of a risk but must still be evaluated. The OCR provides the following example: "tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider." If the this information is disclosed to, or collected by, a tracking technology vendor, the HIPAA Rules apply.

For more information regarding the OCR's guidance on this topic, see *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.*

RISK ANALYSIS

Finally, performance of risk analyses continues to be the most important step for a provider to take towards compliance with the HIPAA Security Rule. Nearly all settlements, which do not involve patient access discussed above, rely on lack of a comprehensive up-to-date security risk analysis as a basis for the settlement. Security risk analyses can be performed by a vendor or internally using the security risk analysis tool developed for small to medium sized entities. The recently updated security risk analysis tool can be found at: *https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.*

CONCLUSION

There are obviously many more important facets of HIPAA compliance, but this highlights some of most significant, and perhaps unexpected, issues that must be addressed by pharmacists in their ongoing HIPAA compliance efforts. On a final note, if this article did its job and scared you just a little, make sure that your organization carries cyberliability insurance, especially as we expect more concerns to arise when artificial intelligence starts to attack HIPAA defenses.

~ By Stacey Gulick, Esq.

Stacey L. Gulick is Chair of the Garfunkel Wild's HIPAA, Privacy, and Risk Management Practice Group. Stacey's practice focuses on Federal and state regulatory, interoperability and technology related issues, including response to government inquiries, compliance initiatives and transactions. Stacey assists clients in implementation of cybersecurity and HIPAA compliance programs and investigations, information security breach response, medical staff hearings and bylaws, and healthcare diligence in large transactions such as mergers and acquisitions. Stacey also has extensive experience in the unique regulatory and business needs of various health care providers including pharmacies.