Five myths about HIPAA

By Daniel F. Shay, Esq.

DermWorld covers legal issues in "Legally Speaking." This month's author, Daniel F. Shay, Esq. is a health care attorney at Alice G. Gosfield and Associates, P.C.

In 1996, the Health Information Portability and Accountability Act (HIPAA) was signed into law. Four years later, the first major set of regulations, known as the Privacy Rule, were published. Since then, HIPAA has had additional regulations published, and the HHS Office for Civil Rights (the OCR — the government entity responsible for enforcing HIPAA) has published numerous FAQs and guidance documents. Yet, HIPAA continues to confuse health care professionals. This article examines and debunks five of the most common and persistent myths about HIPAA.

Inquiry = authorization

Physicians often struggle to understand when they may reply to a patient's email, social media post, or online review, often believing that such acts by patients mean the physician may respond substantively. But these kinds of communications may reveal protected health information (PHI) about the patient, and do so through unsecured electronic channels (e.g., a Facebook post, unsecure email like Outlook or Gmail, or an online review site). This, in turn, may be treated as an improper disclosure, unless the patient has provided an authorization to communicate through such channels. However, merely sending an email asking, "Does this skin condition look like [disease]?", posting the same question on social media, or posting a review is not an authorization. A HIPAA authorization requires a specific form that includes mandatory language. If the patient has not completed one, the physician cannot respond in any way that reveals PHI, including acknowledging that the patient is a patient! A better response is to suggest calling the physician's office or asking over the patient portal, without providing a substantive response.

Sharing photos

In the digital age, we can all send photographs effortlessly using text messaging, email, or social media. Dermatologists are no exception, sometimes sending each other photos of patient body parts or skin conditions to seek a colleague's advice, or merely to discuss the case casually. Some physicians also belong to online communities where they may discuss patient care. Many health care providers believe that if the picture does not show a patient's face, or include medical record information, then sharing the photo will not violate HIPAA.

Want more Legally Speaking?

Check out archives of the most popular Legally Speaking articles at **www.aad.org/dw/legally-speaking**.

But any information capable of individually identifying a patient is considered PHI. For example, a patient's distinctive tattoo or birthmark shown in a photo could be used to identify them. By contrast, a picture of a skin condition on the patient's otherwise indistinct forearm poses far less risk. The key question that should be asked before sharing the image is whether anything in the image could be used to identify the patient individually. If it could be, then it is best not to share the image outside of those reasons permitted under HIPAA.

"Our HIPAA-compliant EHR means we comply with the security rule."

Having a HIPAA-compliant electronic health record (EHR) system is an important aspect of compliance under the Security Rule (which governs electronic PHI or ePHI). However, compliance requires more than just appropriate software. Many physician practices, especially smaller ones, have taken very few steps to achieve Security Rule compliance beyond purchasing compliant EHR software. Actual compliance requires the development of policies and procedures to address risks to ePHI, as well as the implementation of administrative, physical, and technical safeguards to protect ePHI. Moreover, those policies and safeguards can only be developed after the practice has conducted a security risk assessment (SRA). The failure to conduct an SRA, and to take the required steps after that, most often is discovered only when it is too late because a breach of PHI has already occurred and the HHS OCR (the government entity tasked with enforcing HIPAA) is auditing the practice. We have represented dermatologists who have gone through such audits. They are time-consuming, intrusive, and can result in financial penalties and expensive remediation. So, remember: your HIPAA-compliant EHR alone will not protect you.

Business associates

Understanding which parties are business associates (BAs) under HIPAA is essential for compliance. The HIPAA regulations require entering into business associate agreements (BAAs) with BAs. But many physicians end up confused as to when someone is a BA at all. A party is a BA to a physician practice when they act on behalf of the practice in a way that requires access to or use of PHI. Typical BAs include billing companies, EHR suppliers, and

HIPAA eCompliance Module

Check out the Academy's e-compliance training at **https://shop.aad.org/collections/practice-management/products/2022-ecompliance-series-hipaa-training-for-medical-offices.**

attorneys who need PHI as part of their representation. They can also include third parties that sell or lease their clinical services to the practice, but which are not under the practice's direct control. When under the practice's direct control, they are considered "workforce" and no BAA is necessary. The key question is "on whose behalf is the service being performed?" Sometimes there is no service at all, and the arrangement involves two parties that still need access to PHI, such as when a private equity group is proposing to buy a practice. In those cases, a BAA is inappropriate because nobody in the arrangement is a BA. Different documents may be required to protect the practice's PHI. In other cases, two "covered entities" (e.g., a practice and a hospital) are simply sharing information with each other, and neither is providing services to the other, even if the patients originate with one of the parties. Just because they're "your" patient doesn't mean they aren't the other entity's patient. In such cases, neither is a BA, and no BAA is necessary.

Cash businesses and covered entities

One final question that can come up is whether HIPAA applies at all. This issue arises in the context of concierge practices, or practices where patients only pay out of pocket. HIPAA only applies to "covered entities" and BAs. A covered entity is one that transmits health information in connection with specific electronic transactions described in the HIPAA regulations. These transactions include health care claims, health care payment or remittance advice, coordination of benefits, health care claim status, and referral certification and authorization, and other similar transactions. If a practice does not send health information as part of the HIPAA transactions, then it is not a covered entity and HIPAA does not apply. Thus, for cash-based practices that never accept insurance, such as a practice that only provides cosmetic services not covered by insurance, they may not actually be subject to HIPAA.

Conclusion

The HIPAA regulations are complicated and can be confusing. There are many myths circulating about how and when it applies. Hopefully, this article has clarified at least a few common myths. When in doubt, it is best to seek the advice of legal counsel. **DW**

Academy practice management resources

Check out the Academy's compliance resources at **www.aad.org/member/practice/compliance**.