Ongoing best practices for 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 2000, the Privacy Rule for the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was published, with the Security Rule following in 2003, and the Breach Notification Rule in 2013. In practical terms, HIPAA has been a fact of life for physician practices for almost a quarter century. While many practice owners and administrators feel comfortable with HIPAA, that confidence is sometimes misplaced. Familiarity with the general requirements of HIPAA is insufficient to protect a physician practice from eventual problems.

Prepare for failures

By now, stories of physician practices and their HIPAA mishaps are all too familiar. From a practice that used a publicly visible Google calendar for appointments, to tales of lost unencrypted thumb drives or laptops full of PHI, to stories of improper PHI disclosures on social media, tales of HIPAA woe abound. Other HIPAA mishaps can arise from actions outside a physician practice's control, such as ransomware attacks or hacking incidents, but these incidents can also expose longstanding noncompliance. Still others may not even seem like mistakes. For example, many physicians may not know that it is a HIPAA violation to withhold records from a patient who is delinquent in payment, which may account for why the Office for Civil Rights (OCR – the government's HIPAA enforcement agency) has enforced against such withholding multiple times. Even nonpaying patients are guaranteed the right to access their records.

Some physician practices may feel small enough to fly under the radar. However, since 2012, the OCR has enforced frequently against small physician practices. Moreover, while hackers may focus on larger institutions, small practices may have weaker defenses and yet still have data that hackers see as valuable.

The smartest move is to orient compliance efforts around being prepared for when something goes wrong, not whether something may go wrong. In other words, assume that your practice will eventually face some kind of HIPAA problem. The question then becomes how well you can respond, and how robust your compliance framework is when you do.

Policy review and renewal

Having a HIPAA compliance plan, policies, and procedures is good. However, we caution our clients that merely having these documents is not enough; one must actively live by them. To that end, these policies and procedures should be reviewed periodically and updated to account for changes in personnel and/or the workplace environment.

No set of policies or procedures will be seen by the OCR to be effective for purposes of Security Rule compliance unless they were devel-

Want more Legally Speaking?

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

oped in response to a Security Risk Assessment (SRA). In addition to being required by the Security Rule, the OCR has described the SRA as "foundational." Without one, the OCR will consider any security policies and procedures to be ineffective, because they are not grounded in any understanding of the risks the covered entity faces. The OCR's website includes a list of Resolution Agreements: settlement agreements into which covered entities enter with the OCR to resolve HIPAA violations and avoid Civil Money Penalties. It is rife with cases where the covered entity either had never performed an SRA or had one that was woefully out of date and no longer relevant.

The SRA requires covered entities to consider the nature of the risks they face, the severity of those risks, and the likelihood of their occurrence. Only after analyzing this information will policies be seen by the OCR as worthwhile. Moreover, the Security Rule requires the SRA to be updated in response to practice changes. For example, if the practice switches from a locally installed EHR to a cloud-based system, the SRA should be updated to account for these, with policies and procedures revised to consider the way the new EHR works.

Although the Privacy Rule does not require a "Privacy Risk Assessment," it is wise to consider similar questions under HIPAA, and to update the risk analysis and policies and procedures as circumstances change. Reviewing these documents periodically helps to ensure that policies and procedures stay up to date and can promote a culture of active compliance.

Staff training

Many staff go through mandatory HIPAA training when first hired and may do periodic re-training. Initial training is required by HIPAA, as is re-training when job functions are materially changed by HIPAA policies or procedures. The precise form of training is not mandated. One of the most important things to impart to staff and physicians alike is the instinct to "think twice." In any tale of HIPAA violations where you wonder, "What were they thinking?!" it is likely that they didn't think; they simply acted without considering the potential HIPAA ramifications. Had they thought twice, they might have recognized the HIPAA risk which seems obvious in hindsight. This is especially true with respect to workforce usage of social media.

Our legal practice represented a rural physician group that hired an enthusiastic front desk staff member. One day, a patient came in and gave the new employee an apple grown in the patient's orchard. The employee was so excited that they took a photo of the apple and posted it online, with a comment about how much the employee enjoyed their new job. Unfortunately, the apple was sitting atop a charge sheet when the picture was taken. Fortunately, no PHI was clearly visible in the picture (thanks to how

Compliance help

Learn more about HIPAA compliance at **www.aad.org/member/practice/compliance/hipaa**.

it was cropped and zoomed), but the risk was there. This is a prime example of a situation in which the employee needed to think twice. If they had, they might have at least put the apple on a blank desk or, better still, simply posted a description instead of a picture taken in an office setting where PHI could be almost anywhere in the background.

To get employees to think twice, it can be helpful to teach them to consider HIPAA in context. Most employees know that it's improper to post PHI online. But most are likely imagining posting information taken from a patient chart on purpose, rather than inadvertently including it in an offhanded comment. Moreover, they aren't considering that a patient walking through the background of a photo taken at work is PHI; nor that a photo of a patient's one-of-a-kind tattoo is PHI, when the image is circulated with a group of fellow physicians to ask for advice on a skin condition. It is insufficient for employees to merely understand that, legally speaking, PHI is any individually identifying information; they must understand what kind of information that might include and think broadly about how that information might be improperly disclosed or used. Periodic training to remind employees of how this works may help.

The impact of ongoing compliance

The OCR has publicly stated that its goal is to encourage and attain compliance with HIPAA-covered entities. Put another way, the OCR's goal is not, necessarily, to punish those who face HIPAA violations; rather it seeks to bring them back into compliance. In our own legal practice, we have represented clients who have faced HIPAA problems, and taken remedial action which helped them to avoid the imposition of penalties. One client was hacked, had an out-of-date SRA, as well as generic policies and procedures, and upon discovery took extensive efforts to document not just what had gone wrong, but also every step the client took to remediate the problem. The client fired the IT staff whose actions had made the hack more likely, switched EHRs, conducted a new SRA, and developed new policies and procedures, all of which was submitted to the OCR for review. The OCR determined that the client had attained compliance, and considered the matter closed.

If the client had, prior to the incident, engaged in more ongoing HIPAA compliance efforts, the experience of responding to the OCR's inquiry might have been less nerve-wracking and expensive. Certainly, the client would have had an easier time demonstrating the steps it took to respond to the problem, because presumably those steps would be outlined in the client's policies and procedures.

In general, when the OCR sees that a HIPAA-covered entity is actively engaged in compliance efforts, it has not often punished HIPAA failures. Penalties or entering into a resolution agreement is much more likely when the covered entity's policies and procedures are out of date, or otherwise demonstrate blind spots that ongoing compliance might have caught. One can think of these efforts as the proverbial "ounce of prevention." Knowledgeable legal counsel can help in this regard. **DW**