No more flying under the radar

HIPAA security risk assessments and security rule compliance

BY DANIEL F. SHAY, ESQ.

Every month, Dermatology World *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.*

It has been 12 years since the HIPAA Security Rule became effective, yet compliance remains a problem for many physician practices. Many physicians remain unaware of the full scope of their obligations under the Security Rule. They may lack required policies and procedures, may have never conducted a security risk assessment (SRA), or may not have updated either in many years. While you may be confident of your compliance with the Privacy Rule, and you may know exactly what to do in the case of a breach, if you cannot ensure the security of your electronic protected health information (ePHI), your compliance efforts are incomplete. Without conducting an SRA, you cannot secure your ePHI because you do not know where your risks lie.

Background

The Department of Health and Human Services' Office for Civil Rights (OCR) undertook its first Security Rule enforcement action in 2009 — four years after the Rule's compliance date of April 20, 2005. However, most enforcement was focused on larger institutions and health systems. This changed in 2012, with the first enforcement action taken against Phoenix Cardiac Surgery, P.C., in a case involving the improper posting of ePHI online. From that point forward, physician practices were on notice: assuming that you could fly under the radar due to the OCR having bigger fish to fry was no longer an option.

With the passage of the Health Information for Economic and Clinical Health Act of 2009 (HITECH), the OCR is also required to conduct periodic audits of HIPAA covered entities, including physician practices. This has led to an audit program, where the OCR proactively audits covered entities to determine their compliance with HIPAA. The current audit program developed after several initial efforts, including an audit pilot program. The audit pilot program targeted a broad range of covered entity types, including hospitals, health systems, and physician and dental practices. It uncovered significant concerns with physician practices.

Based on analysis of the audit pilot program, the OCR determined that small providers had the largest number of problematic findings, with 60 percent of the findings relating to failure to effectively comply with the Security Rule. Nearly every small provider surveyed had at least one problem relating to Security Rule compliance. Most failed to conduct a SRA. Many also had ineffective policies and procedures relating to access management, contingency planning and backups, encryption, and other aspects of the Security Rule, or simply lacked such policies and procedures altogether. In response, the OCR announced that its audit program would focus particularly on Security Rule compliance. These audits continue to the present. Physician practices therefore have even more incentive to review their HIPAA compliance policies, and ensure that they are meeting their requirements, especially with regard to Security Rule compliance.

The Security Risk Assessment

One key factor in ensuring Security Rule compliance is the performance of an SRA. The OCR has described SRAs as "foundational" to Security Rule compliance. Without an SRA, any policies or proce-

Looking for more help?

Looking for more help running your practice? Visit the American Academy of Dermatology's new Practice Management Center at **www.aad.org/practicecenter**.

dures developed by a physician practice to address Security Rule requirements are likely to be deemed ineffective. This is because the purpose of an SRA is to identify (1) whether the covered entity is in compliance currently, (2) what risks the covered entity faces, and (3) what steps should be taken to address the existing risks.

A practice that has drafted policies and procedures without first having conducted an SRA is effectively flying blind; because it does not know the risks it faces, it has no idea whether the policies and procedures even address those risks and, if they do, whether they are effectively crafted. Many of the requirements of the Security Rule are described as "addressable" in the regulations. This, however, does not mean "can be ignored if you don't want to deal with it." If a practice decides, for example, that it does not need to encrypt its ePHI, it must document why and how it arrived at that decision, all of which should be done as part of the SRA.

The good news is that the Security Rule does not mandate the format for an SRA. Instead, the OCR has published guidance regarding the minimum elements that must appear in the SRA, available at **www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf**. For example, the scope of the analysis must be appropriate. It should examine all places and methods by which ePHI is stored, transmitted, or used. This should take into account all manner of ePHI storage, from the physical PCs, laptops, or tablets used at the office, to the cloud-based storage provided by an EHR vendor, to the portal software offered to practice physicians that allows them to access patient records remotely. The SRA should also document how the above information was collected. This could be done through a variety of methods, including interviews with practice personnel, written statements from IT vendors, practice IT staff producing a documented review of systems, etc.

Of course, the SRA must identify and document the potential threats and vulnerabilities to the practice's ePHI, as well as taking into account the likelihood and potential impact of such threats and vulnerabilities occurring. The results of such a review are entirely dependent upon your practice's own IT infrastructure; each practice has its own unique concerns. For example, the use of thumb drives, laptops, or tablets presents a risk due to the potential for such devices to be lost or stolen. However, if your practice does not use such devices in the first place, their usage hardly represents a threat to your practice's ePHI. Similarly, the SRA should also assess the security measures currently in place. These, too, will differ from practice to practice.

The SRA should be updated periodically, whenever your practice's IT infrastructure changes. If you buy new hardware, switch

Key elements of a Security Risk Assessment

A Security Risk Assessment should:

- **Examine all places and methods by which ePHI is stored, transmitted, or used.**
- **Identify and document the potential threats and vulnerabilities to the practice's ePHI.**
- **Assess the security measures currently in place.**
- **Be updated periodically, whenever a practice's IT infrastructure changes.**

or modify your EHR, change the duties for your staff in a way that impacts their use of or access to ePHI, etc., the SRA should be updated. This does not necessarily require you to perform a complete SRA every time a minor change occurs. Rather, you can update the SRA to reflect the recent changes. For example, if you switch from using a server room and onsite storage of ePHI to a cloud-based option, you will not need to revisit many issues relating to the physical layout of your office (except insofar as they might have related to your server room).

While there is no mandatory format for documenting an SRA, the SRA must still be documented. If the OCR conducts an audit, there must be something to show for having conducted an SRA. Ideally, this document should address the minimum elements described above in a thorough manner, with the goal being to prove beyond a doubt that your practice has actually met its requirements.

It will likely help to use an outside consultant in the performance of an SRA. Consultants are usually very experienced in determining security risks, and may consider risks you would never have imagined. For example, a consultant might recommend against using wifi printers, citing them as a potential entry point for hackers that is less protected than other points in your office network. Consultants can also be engaged by attorneys, to ensure that the results of their investigation remain "under the privilege."

Policies and procedures

After having conducted an SRA, your practice must develop policies and procedures to address the requirements of the Security Rule. In general, the Security Rule requires that practices implement certain administrative, physical, and technical safeguards.

Administrative safeguards require that policies and procedures address issues such as who has responsibility for maintaining the security of your practice's ePHI, as well as who among the workforce has access to ePHI. For example, not every member of your practice's staff necessarily requires the same level of access to or authority to modify ePHI. Practice billing staff would have no reason to be able to modify clinical records, although they might need to view them. By contrast, practice clinical staff would need to be able to both view and modify clinical records, but should have no access to patient financial records.

Administrative safeguards also include having policies and procedures in place regarding security awareness and training. This should include both general awareness of what constitutes ePHI, as well as training regarding how to protect against malware, report discrepancies in records, manage passwords, etc. One particular area of concern is ePHI in a social media context. Workforce should be trained to recognize that even seemingly benign information (e.g. a "selfie" taken at the office) could include ePHI (e.g. patient records or a patient's face in the background of the selfie).

Security incident procedures and contingency plans to respond to hacks (or attempted hacks), emergencies, fire, vandalism, or system failures are also required as part of the administrative safeguards. Your practice will need to address issues such as disaster recovery, operating in "emergency mode," etc.

The Security Rule also requires that covered entities address establishing physical safeguards. These address four standards regarding facility access controls, workstation use, workstation security, and device and media controls. Facility access controls include issues such as physical access to different parts of the building (e.g. establishing policies and procedures granting different levels of access to different parts of your office, based on job duties). Workstation use and security requires that your practice implement policies and procedures regarding the use of workstations, including how workstations are themselves used, and the physical attributes of the surroundings of this or that workstation. For example, if your workstations are visible to the public, policies and procedures might require the use of a screen dimming device to permit only someone sitting close by to see the

Key questions security policies should answer

- Who's responsible for ePHI security?
- Who needs what access to ePHI?
- Do staff understand what shouldn't be posted on social media?
- How would we recover after a disaster?

screen, or might require that blinds be drawn so that pedestrians could not simply look in the window to view ePHI. Device and media controls address issues regarding the receipt and removal of hardware and electronic media containing ePHI or movement of those items both within and outside of your offices. This includes how records are backed up, what authorizations you require workforce to obtain to remove such devices, etc.

Technical safeguards are likely the one area that most physician practices have considered with respect to Security Rule compliance. Technical safeguards require that the practice have policies and procedures in place to address issues such as access control, audit controls, record integrity, authentication, and transmission security. Access control relates to issues such as assigning unique usernames and logins to identify and track individual users within the practice's system. For example, your practice should probably assign a unique login ID to each person who uses your systems containing ePHI, rather than simply having a "master login" through which everyone signs in. Audit controls relates to methods by which the practice monitors activity within the system, which relates back to access controls. With proper access controls in place, and assuming the software you are using is capable of doing so, you can monitor who accesses the different aspects of the software and when. For example, you could see that one of your staff logged in at 3 pm, viewed several clinical records, and modified one.

Record integrity requires ensuring that ePHI has not been improperly altered or destroyed. Your practice's ability to meet this requirement will depend on whether the software permits you to see when an individual record has been modified or deleted. Authentication addresses procedures to verify that the individual seeking access to ePHI is actually who they claim to be. Just because a user ID has logged in does not mean that the individual to whom that ID is assigned is the one using the ID. Authentication measures help determine that the correct person is logging in, such as by using a secret question or a fingerprint scanner. Finally, transmission security relates to taking technical measures to protect against unauthorized access to ePHI transmitted over an electronic communications network. Typically, this involves encrypting records for transmission purposes.

Even aside from Security Rule compliance requirements, adopting a HIPAA compliance plan incorporating the policies and procedures discussed above is simply a good idea. Just as you might develop a compliance plan to address fraud and abuse issues, you should do the same for HIPAA compliance. However, drafting policies in such a complex area may seem daunting for physician practices and their administrative staff. The good news is that you need not do so alone. Health care legal counsel can assist in the development of such policies.

Conclusion

The OCR has made it clear that it will be targeting smaller physician practices in the future. With the implementation of the OCR's HIPAA auditing program, physician practices should adopt a "when, not if" attitude regarding audits. This necessarily means that physician practices must review their current HIPAA compliance position, and take whatever steps are necessary to become compliant. Given the focus on the Security Rule, and the difficulties that small physician practices have had in this area, ensuring Security Rule compliance will likely prove a significant hurdle for many groups. Toward that end, conducting an SRA will help ensure that your practice has a clear understanding of its risks, which can serve as the basis for the development of policies and procedures to address and attempt to mitigate those risks.

Given the range of issues that a physician practice must address, and the necessary variation between practices in terms of their IT infrastructure, technical capabilities, practice size, physical facilities, and resources, it should be clear that no single set of policies and procedures will be effective for all practices. There is no "one size fits all" solution. Instead, physician practices should work with knowledgeable health care counsel and consultants to guide them through the SRA process and the development of effective policies and procedures regarding Security Rule requirements. ***dw***