Word Count: 2,268

How Secure Do You Feel About Your HIPAA Compliance Plan?

Daniel F. Shay, Esq.

Physician practices have lived with the reality of HIPAA for over twenty years. In that time, it has likely become second nature for most practices to navigate questions such as how to deliver a proper Notice of Privacy Practices, whether it is permissible to leave messages on patient answering machines or voicemails, and which entities are the practice's business associates (e.g., the billing company is, the janitor is not). Most of these issues are governed by the Privacy Rule, a set of regulations first published in 2000, and updated periodically since that time. Most physician practices are generally comfortable with the Privacy Rule's requirements; they are simply a part of daily life now.

However, there is another rule[1] that is – or should be – an integral part of the practice of medicine: the Security Rule. Physicians and practice managers might claim to be familiar with the requirements of the Security Rule, citing the need for HIPAA-compliant EHR software, or encryption. But these requirements barely scratch the surface of the obligations of a physician practice with respect to the Security Rule. Moreover, unfamiliarity with the requirements has led to multiple instances of costly HIPAA settlements between HIPAA covered entities (including small physician practices) and the Department of Health and Human Services' Office for Civil Rights (the "OCR") – the government office tasked with HIPAA enforcement.

This article explores the government's recent HIPAA enforcement efforts, including common errors made by HIPAA covered entities. It also examines the requirements of the HIPAA Security Rule, with a special focus on Security Risk Assessments ("SRAs").

Audits and Enforcement – The Pitfalls

The OCR was given the authority to enforce HIPAA in 2003. The Security Rule compliance date was April 20, 2005. However, no Security Rule enforcement actions were taken until July 27, 2009, and most enforcement actions after that were focused on larger institutions and health systems. In April, 2012, Phoenix Cardiac Surgery, P.C. became the first physician practice to face Security Rule enforcement when it entered into a settlement with the OCR. The group mistakenly posted its appointment calendar on a publicly viewable internet calendar, which led to the initial OCR investigation. The investigation discovered that the practice had failed several of its HIPAA obligations, including having not provided effective training to its workforce members, having ineffective administrative and technical security safeguards to protect its electronic protected health information ("ePHI"), and having failed to

[1] Actually, more than just one; there is also the Breach Notification Rule, which is not a focus of this article.

conduct a security risk assessment ("SRA"). The group was required to pay $100,000 and engage in remedial efforts to correct its HIPAA deficiencies.

The Phoenix Cardiac Surgery case is fairly typical of OCR settlements, which usually involve the OCR responding to a report of a breach or improper disclosure. With the passage of the Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act"), the OCR was tasked with the performance of "periodic audits" of HIPAA covered entities, shifting the agency from a primarily reactive role to one that also had proactive enforcement duties. In response, the OCR conducted a year-long Audit Pilot Program in 2011, examining the Privacy and Security Rule compliance of 115 covered entities, ranging from hospitals and group health plans, to physician and dental practices. This eventually led to "Phase 2" of the Audit Program, beginning in October, 2014, which continues to this day.

In the course of the Audit Pilot Program, the OCR found that out of 59 small providers audited, 58 had at least one problem relating to Security Rule compliance. In particular, almost 80% of the small providers audited had not conducted a complete SRA. Other problem areas included access management, security incident procedures, encryption, and integrity controls. These results convinced the OCR of the need to focus the Phase 2 audits both on smaller providers, and on Security Rule compliance specifically. In short, physician practices can no longer count on being too small to draw the attention of the OCR.

A survey of the OCR's resolution agreements also demonstrates common problem areas with respect to Security Rule compliance. As found during the Audit Pilot Program, many covered entities have either not conducted an SRA at all, or have conducted an incomplete SRA. Lost or stolen media storage devices containing unencrypted ePHI – including laptops and thumb drives – are also a major source of problems. As noted above, appointment calendars have also been configured improperly, making them publicly searchable online. In many cases, the covered entities that have made these errors also fail to implement effective policies and procedures to detect, prevent, contain, and correct security violations.

Settlement amounts have been from $100,000 up to multiple millions of dollars, with several larger covered entities paying $1.5 million. The OCR will also impose remedial efforts, usually requiring the covered entity to conduct or update an SRA, as well as to develop risk management plans, and to review and/or revise existing policies and procedures. These efforts, too, can be costly and time consuming.

Security Rule Requirements of HIPAA

The Security Rule, contrary to what many believe, is about more than simply encryption and obtaining "HIPAA-certified" software products. The Security Rule requires that physician practices take proactive efforts to establish Administrative, Physical, and Technical Safeguards, with each requiring the performance of specific tasks.

Administrative Safeguards are primarily concerned with those safeguards that relate to personnel and overall administrative activities. For example, the Administrative Safeguards require that a HIPAA covered entity appoint a HIPAA Security Officer, and conduct an SRA. The Security Officer should be someone who is familiar enough with both the requirements of HIPAA and the technical aspects that fall under the Security Rule to serve as an effective communicator between practice IT staff, other employees, and management, and to effectively help craft policies and procedures to meet and respond to the risks the practice faces.

To meet the requirements for Administrative Safeguards, covered entities must also develop policies and procedures regarding the prevention, detection, correction, and containment of security violations. They must also address issues relating to workforce security, such as ensuring that workforce members have appropriate levels of access to ePHI, and must establish policies and procedures to address incidents of inappropriate access. They also must train workforce with respect to their Security Rule obligations, establish incident procedures to address security violations, and develop contingency plans to ensure the security and integrity of ePHI in the event of an emergency (such as a fire, power outage, or natural disaster).

Physical Safeguards are chiefly focused on those requirements relating to the practice's physical site. The practice must address facility access controls. For example, if the practice has a server room onsite, it must decide who may have access to that room and what mechanisms are used to bar access to unauthorized individuals. Office layout must also be considered. If there are workstations facing windows through which ePHI would be visible, the practice must consider how to prevent unauthorized individuals from viewing ePHI on the monitors. The practice must also establish workstation use policies, such as requiring workforce members to log off after a specific amount of time. In addition, the practice must address device and media controls, such as developing policies and procedures governing the removal or transfer of devices (e.g., thumbdrives, laptops, tablets, etc.) containing ePHI.

Technical Safeguards are what most physicians think of when they consider the requirements of the Security Rule. Technical Safeguards address matters such as the practice's use of encryption, authentication (e.g., password policies), audit controls (e.g., tracking which individual user is viewing a given record at a given time), integrity policies and procedures (e.g., to address the modification or destruction of ePHI), and transmission security (e.g., protecting against unauthorized access to ePHI when transmitted through the internet).

The SRA – Elements and Requirements

Before a physician practice can address the Administrative, Physical, and Technical Safeguards, it must conduct an SRA. The OCR has described the performance of an SRA as "foundational."[2] The SRA, ultimately, is the key to any effective Security Rule compliance

[2] "Guidance on Risk Analysis Requirements Under the HIPAA Security Rule," p.1, July 14, 2010, at http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

program. Without conducting an SRA, a physician practice is effectively "flying blind," because it has no idea what its risks are, and therefore cannot know whether any compliance efforts it takes are effectively protecting the practice.

However, most smaller physician practices are not in a position where they themselves can conduct an effective SRA. There may well be issues that the practice will never consider, either because of a lack of knowledge about the regulatory requirements, a lack of technical understanding, or simply a lack of experience at confronting and addressing problems. With this in mind, it may be helpful to engage an outside consultant who specializes in performing SRAs. In addition, if the consultant is directly engaged by the practice's attorney, much of the material produced as part of the SRA may be cloaked under the attorney work-product privilege. Even if the practice intends to disclose the SRA itself, the full information from which the SRA is ultimately derived need not be disclosed and can be protected as privileged.

The OCR has published guidance on the seven elements that should appear in all SRAs.

1. The scope of the SRA must address potential risks and vulnerabilities to all of the ePHI that the practice creates. This should include all forms of electronic media, such as hard drives, PDAs, tablets, workstations, laptops, etc.

2. The SRA should document how data was collected relating to the storage, use, maintenance, and transmission of ePHI. This could be based on interviews with workforce or business associates, reviews of current systems where ePHI is stored, reviews of documentation, and the like.

3. The SRA should identify and document potential threats and vulnerabilities to the practice's ePHI. This will depend heavily on the practice's ePHI infrastructure, and even on its physical layout. For example, if there are no exterior windows in the building, there need be no consideration of the risk of passers-by viewing ePHI on unattended workstation screens. Likewise, if the practice uses a remote website to allow its practitioners to access patient records from home, and never uses thumbdrives or laptops with ePHI stored on them, there is likely little risk posed by a lost/stolen laptop scenario.

4. The SRA must assess current security measures that it has in place. This, too, will vary from one practice to another. However, the ultimate goal is to determine whether the existing security measures are sufficient in light of the identified potential risks and vulnerabilities.

5. The SRA must determine the impact of potential threats, if they occur. This is separate from determining the likelihood of a threat's occurrence. This assessment may be qualitative, quantitative, or both. For example, the practice might determine that, because it uses

a remote website for practitioner home access to ePHI, there is a low risk of threat to the ePHI, and that its passwords and website security are sufficient to keep its vulnerabilities low. However, were the website to somehow be hacked, it could have a catastrophic effect. Thus, even an unlikely threat could be extremely impactful.

6. The SRA must determine the level of risk involved in the identified threats and vulnerabilities. This determination should consider the likelihood of the threat occurring, and the severity of its impact, after which a risk level would be assigned. So, the unlikely, but catastrophically-impactful threat might still be assigned a low or medium risk level.

7. The SRA must document all of the above in some form of finalized documentation. The OCR, however, does not specify any required format for such documentation, giving physician practices a degree of flexibility in how to actually document the results of the SRA.

An SRA need only be updated periodically, but it must be updated whenever the practice's electronic infrastructure changes, or when any aspect addressed in the SRA changes. For example, if the practice were to move to a new physical location, it would need to update its consideration of any physical site aspects of the SRA (and likely would have to update its policies and procedures relating to Physical Safeguards). Likewise, if the practice purchases a new EHR, it must update its SRA to address the change.

Conclusion

Compliance with the HIPAA Security Rule is not an easy thing. It requires an understanding of complex regulations, as well as familiarity with technical issues relating to a given practice's ePHI infrastructure. Physician practices, however, need not go it alone in achieving compliance.

In conducting an SRA, it will likely be helpful to engage the services of an experienced, technically savvy consultant. Even if the practice has technically knowledgeable IT staff, that staff may not have encountered the range of problems that an experienced consultant has. These consultants can also be engaged by the practice's legal counsel, to help cloak the documentation gathered in the course of the SRA "under the privilege." While the final SRA document will likely need to be disclosed in the event of an audit or investigation, the practice can still attempt to assert the privilege over the material that formed the basis for the SRA.

Attorneys can also help work with the practice to develop its own compliance protocol, which should be unique to each physician practice. These policies and procedures are required under the Security Rule, but they also represent "best practices" in ensuring ongoing HIPAA compliance.