CME

Daniel F. Shay, JD

THE HIPAA SECURITY RULE: ARE YOU IN COMPLIANCE?

Taking steps to protect your patient information and prepare for a possible breach can avoid costly audit violations.

© JOHN UELAND

Physician practices have lived with HIPAA for more than 20 years. By now, most probably know how to deliver a proper Notice of Privacy Practices, when it is permissible to leave voicemail messages for patients, and who their business associates are (e.g., the billing company is, but the janitor is not). Most of these issues fall under the HIPAA Privacy Rule, a set of regulations updated periodically since being introduced in 2000 that most physician practices view as a part of daily life.

However, there is another HIPAA rule that is – or should be – an integral part of practice: the Security Rule. The requirement for HIPAA-compliant electronic health record (EHR) software barely scratches the surface of the obligations of the Security Rule. Unfamiliarity with the requirements has led to multiple costly settlements between HIPAA-covered entities (including small physician practices) and the Department of Health and Human Services' Office for Civil Rights (OCR).

This article explores the government's recent HIPAA enforcement efforts and 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).

The pitfalls of HIPAA enforcement

The OCR was given the authority to enforce HIPAA in 2003. The compliance date for the Security Rule was in 2005, but no enforcement actions were taken until July

About the Author

Daniel Shay is an associate at the law firm of Alice G. Gosfield & Associates in Philadelphia. Author disclosure: no relevant financial affiliations disclosed.

Physician practices can no longer count on being too small to draw the attention of the HIPAA auditors.

The Security Rule is an integral, and often misunderstood, part of complying with HIPAA.

Auditors are increasingly looking at small practices to check for HIPAA enforcement.

Security violations can result in settlements costing hundreds of thousands of dollars in addition to the price of improved compliance.

2009. Even then, most enforcement actions involved larger institutions and health systems. In April 2012, Phoenix Cardiac Surgery P.C. in Arizona became the first physician practice to face Security Rule enforcement. The group had mistakenly made its appointment calendar publicly viewable online. The OCR's investigation then discovered several other HIPAA problems, including a lack of effective training for the practice's workforce, ineffective administrative and technical protection for its electronic protected health information (ePHI), and failure to conduct an SRA. The group was required to pay $100,000 and engage in remedial efforts to correct its HIPAA deficiencies.

The case is fairly typical of OCR settlements, which usually involve the OCR responding to a report of a breach or improper disclosure. When the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 directed the OCR to perform "periodic audits" of HIPAA-covered entities, the agency shifted from having a primarily reactive role to also having proactive enforcement duties. The OCR conducted a year-long Audit Pilot Program in 2011 that examined the Privacy and Security Rule compliance of 115 covered entities, from hospitals and group health plans to physician and dental practices. This eventually led in October 2014 to the second phase of the Audit Program, which continues to this day.

In the Audit Pilot Program, the OCR found that 58 out of 59 small practices audited had at least one problem relating to Security Rule compliance. In particular, almost 80 percent of the small practices audited had not conducted a complete SRA. Other problem areas included access management, security incident procedures, encryption, and integrity controls. These results led the OCR to focus the second phase audits specifically on smaller practices and Security Rule compliance. 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:

- Nonexistent or incomplete SRAs,
- Lost or stolen media storage devices containing unencrypted ePHI – including laptops and thumb drives,
- Improperly configured appointment calendars, which are 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 $100,000 and up, with several larger covered entities paying $1.5 million. The OCR has also imposed remedial efforts such as requiring the covered entity to conduct or update an SRA, develop risk management plans, or review and revise existing policies and procedures. These efforts, too, can be costly and time consuming.

The importance of safeguards

The Security Rule is about more than just using encryption and obtaining "HIPAA-compliant" software. The Security Rule also requires that physician practices take proactive efforts to establish administrative, physical, and technical safeguards.

Administrative safeguards are primarily concerned with 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 of the Security Rule to effectively communicate with information

technology professionals, practice employees, and management, and to effectively help craft policies and procedures to meet and respond to security risks.

Under the administrative safeguards, covered entities must also develop policies and procedures to prevent, detect, correct, and contain security violations. In addition, they must address workforce security, such as ensuring that staff members have appropriate levels of access to ePHI, and establish policies and procedures to address incidents of inappropriate access. They also must train staff members on their obligations under the Security Rule, establish incident procedures to address security violations, and develop

SECURITY RULE SAFEGUARDS

The HIPAA Security Rule requires physician practices to take steps such as the following to safeguard their patients' electronic protected health information (ePHI).

	Example action(s)
Administrative safeguards	
Security management	Establish policies and procedures to prevent, detect, correct, and contain security violations. Conduct a Security Risk Assessment.
Assigned security responsibilities	Identify a security officer for the practice.
Workforce security	Establish policies and procedures ensuring only appropriate members of staff can access ePHI.
Information access management	Establish policies and procedures to authorize access to ePHI, including workstation, program, and process access.
Security awareness training	Provide training for staff.
Security incident procedures	Establish procedures to be followed in the event of a security incident.
Contingency plan	Provide for disaster recovery.
Evaluation	Conduct technical and non-technical evaluations of safeguards periodically.
Business associate assurances	Seek assurances that business associates conform to these safeguards.
Physical safeguards	
Facility access controls	Establish policies and procedures limiting access to areas that house systems containing ePHI, such as the server room.
Workstation use	Establish policies and procedures governing how staff may use workstations.
Workstation security	Restrict access to workstations by unauthorized users.
Device and media controls	Restrict removal from office of hardware containing ePHI.
Technical safeguards	
Access control	Assign unique user IDs/logins for different system users.
Audit control	Track use of systems and software containing ePHI.
Integrity	Ensure that ePHI has not been improperly modified or deleted.
Person/entity authentication	Verify the identity of individuals logging in by using passwords or two-factor authentication.
Transmission security	Use encryption or other methods to protect the security of transmitted ePHI.

Administrative safeguards deal with how office staff and management protect electronic patient health information.

Physical safeguards dictate the use of office design and devices to comply with HIPAA.

Technical safeguards address the use of technology in the medical office.

The security risk assessment is the key to an effective Security Rule compliance program.

contingency plans to protect the security and integrity of ePHI in case of fire, power outage, natural disaster, and other emergencies.

Physical safeguards relate to the practice's physical site, such as facility access. If the practice has a server room onsite, for example, it must decide who can enter that room and how to keep out unauthorized individuals. Office layout must also be considered. If unauthorized individuals could see ePHI on a monitor through an office window, the practice must consider how to prevent that from happening. The practice must also establish workstation use policies, such as requiring staff members to log off after a specific amount of time to prevent ePHI being left unattended. In addition, the practice must consider device and media controls, such as policies and procedures for the removal or transfer of devices (e.g., thumb drives, laptops, or tablets) that contain ePHI.

Technical safeguards are the most straightforward requirements of the Security Rule. They address such matters 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., how to modify or destroy ePHI), and transmission security (e.g., protecting against unauthorized access to ePHI when the information is transmitted through the Internet). (See "Security Rule safeguards," page 7.)

Completing a security risk assessment (SRA) is necessary to identify your practice's risks and whether your HIPAA compliance efforts are actually effective.

Your SRA must measure both the vulnerabilities of your electronic data and the security measures already in place.

Practices must measure the impact that a breach of its patient information would have.

Conducting a security risk assessment

Before a physician practice can address those safeguards, however, it must conduct an SRA, which the OCR calls "foundational."[1] The SRA is the key to an effective Security Rule compliance program. Without one, the practice is essentially "flying blind," with no idea what its risks are or whether its compliance efforts are effective.

The OCR has published guidance on the seven elements that all SRAs should cover:

1. Potential risks and vulnerabilities to all of the ePHI that the practice creates, including all forms of electronic media, such as hard drives, personal digital assistants, tablets, workstations, and laptops.

2. How the practice collected data about the storage, use, maintenance, and transmission of ePHI. This could be based on interviews with staff or business associates, reviews of current systems where ePHI is stored, reviews of documentation, and the like.

3. 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, you do not need to consider the risk of passers-by viewing ePHI on unattended workstation screens. Likewise, if the practice uses a remote website to allow physicians to access patient records from home and never uses thumb drives or laptops with ePHI stored on them, there is likely little risk posed if a laptop is lost or stolen.

4. Security measures currently in place. This, too, will vary from one practice to another. The ultimate goal is to determine whether the existing security measures are sufficient in light of the identified potential risks and vulnerabilities.

5. The impact of potential threats, if they occur. This assessment may be qualitative, quantitative, or both. This is separate from determining the likelihood of a threat's occurrence. For example, the practice might determine that because it uses a remote website for physicians' 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, if the remote website was hacked, the impact could be catastrophic.

6. The level of risk involved in each identified threat and vulnerability. After considering the likelihood of the threat occurring and the severity of its impact, the practice

would assign a risk level. So, the unlikely but catastrophic threat might still receive a low or medium risk level.

7. Documentation of all of the above. The OCR does not specify the format, giving physician practices a degree of flexibility in how to actually document the SRA.

A practice needs to update its SRA whenever the practice's electronic infrastructure or any other 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 risks inherent in the new site, as well as any policies and procedures dealing with physical safeguards. Likewise, if a practice purchases a new EHR, it must update its SRA to address the change.

Next steps

Compliance with the HIPAA Security Rule is not easy. It requires understanding complex regulations and being familiar with the technical aspects of your practice's ePHI infrastructure. Smaller physician practices may struggle to conduct an effective SRA independently because of a lack of technical knowledge and resources.

With this in mind, it may be helpful to engage a consultant who specializes in performing SRAs. In addition, if the practice's attorney directly engages the consultant, much of the material gathered for the SRA may be cloaked under the attorney work-product privilege so that public disclosure of the SRA need not include the full information on which it is based. The attorney can also help the practice develop all of the policies and procedures used to address its HIPAA obligations, which should be unique to each physician practice. This compliance protocol is required under the Security Rule, but it also represents a "best practice" in ensuring ongoing HIPAA compliance. FPM

Send comments to **fpmedit@aafp.org**, or add your comments to the article at **http://www.aafp.org/fpm/2017/0300/p5.html**.

- You should update the SRA whenever you change the electronic infrastructure or other integral aspects of your practice.
- An attorney can help perform the SRA and keep certain material protected from disclosure.