Bloomberg BNA

BNA's Health Law Reporter™

Health Information

The Security Risk Assessment: Keystone of Security Rule Compliance

By Daniel F. Shay

Daniel F. Shay is an attorney with Alice G. Gosfield and Associates PC in Philadelphia where he focuses on physician representation, fraud and abuse compliance, Medicare Part B reimbursement, and HIPAA compliance in the physician context. He can be reached at dshay@gosfield.com or 215-735-2384.

In 2003, the HIPAA Security Rule final regulations were published, with a compliance date of April 20, 2005. The Department of Health and Human Services Office for Civil Rights (OCR) also received the authority to enforce HIPAA regulations in 2003, with the first enforcement action under the Security Rule occurring in July 2009. For several years, enforcement actions primarily targeted larger covered entities, such as hospital systems. However, beginning in 2012, the OCR began to enforce the HIPAA Security Rule against smaller physician practices. Since that time, the OCR has reported multiple settlements with covered entities regarding Security Rule compliance failures, often arising out of breaches of patient protected health information (PHI). While many covered entities are aware of their duties under both the HIPAA Privacy Rule and the Breach Notification Rule, Security Rule compliance remains an area of concern.

OCR Enforcement Efforts

In 2012, Phoenix Cardiac Surgery PC entered into a settlement agreement with the OCR, marking the first enforcement action of the Security Rule against a physician practice. The group had improperly made its appointment calendar visible on a public internet site. This led to an investigation by the OCR, which discovered that the group failed to meet several of its obligations under HIPAA. For example, prior to the breach, the group had not conducted a security risk assessment (SRA). Other failures included not adequately training members of the group's workforce and having ineffective administrative and technical security safeguards to protect the group's electronic PHI (ePHI). As a result, the group was fined $100,000 and required to engage in efforts to remediate these failures.

Such a story is all too common in the current environment. A covered entity, be it a small physician practice like Phoenix Cardiac Surgery, or a larger institution like New York Presbyterian Hospital, faces a breach of PHI or unsecured ePHI, and reports the breach to the OCR as required under the Breach Notification Rule. The OCR then investigates, discovers that the covered entity has failed to meet its Security Rule compliance requirements and imposes fines and remedial actions on the covered entity. Settlements range from $100,000 to multiple millions of dollars, with several in the $1.5 million range.

Similarly, beginning in 2011, the OCR launched an audit program. This program, mandated by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) began with the OCR's Audit Pilot Program. This program ultimately determined that small providers had the greatest number of problems, especially with respect to Security Rule compliance. The vast majority had never conducted an SRA. The Audit Pilot Program eventually shifted to "Phase 2," beginning in 2014 and continuing to the present day. The Phase 2 audits target both smaller providers and business associates.

Requirements of the Security Risk Analysis

The HIPAA Security Rule imposes multiple requirements on covered entities. These include meeting various Administrative, Physical, and Technical Safeguards, discussed more fully below. However, one of the first and most important steps that a covered entity must take is to conduct an SRA. The OCR has described SRAs as "foundational." ("Guidance on Risk Analysis Requirements Under the HIPAA Security Rule," p. 1, July 14, 2010.) Conducting an SRA is one of the Administrative Safeguards required under the Security Rule. Without an effective SRA, whatever compliance efforts the covered entity engages in will be viewed as incomplete at best and at worst wholly ineffective. This is due to the nature of the SRA itself.

The ultimate purpose of the SRA is to: (1) compile and quantify the risks to the security and privacy of the covered entity's ePHI, (2) evaluate the covered entity's current ability to address those risks and (3) determine what steps must be taken for the covered entity to protect against, detect and remediate any such risks. Without an SRA, the covered entity's security efforts are little better than a shot in the dark.

The OCR has published documentation providing guidelines for the required elements of an SRA. First, the scope of the SRA must address the potential risks and vulnerabilities to all ePHI that the covered entity creates. This includes all forms of electronic media. If the covered entity stores ePHI on hard drives located on office desktop or laptop computers, this must be addressed. Likewise, if the covered entity uses a "cloud-based" electronic health records (EHR) software package, that too must be taken into account. Other forms of ePHI storage could include tablets, PDAs, cell phones, thumb drives, etc.

The SRA must document the method used to collect data regarding how ePHI was stored, used, maintained or transmitted by the covered entity. Towards this end, the covered entity could conduct a review of current systems housing ePHI, review documentation or conduct interviews with its own workforce or business associates.

The SRA must further identify and document potential threats and vulnerabilities to the covered entity's ePHI. This aspect of the SRA will vary greatly, depending on the covered entity's infrastructure, physical layout, and personnel. If, for example, computer screens are visible to patients entering a waiting area, that must be addressed. Likewise, if the covered entity uses a "bring your own device" policy that permits physicians to use their personal cell phones or tablets, that too must be addressed. By contrast, if the same covered entity explicitly prohibits the use of unencrypted thumb drives, that need not be addressed.

The SRA is also required to assess the current security measures that the covered entity employs. As with the potential threats and vulnerabilities, this too will vary widely depending on the covered entity in question. To effectively assess security measures, however, the covered entity must consider the threats and vulnerabilities already identified and determine whether its security measures are sufficient.

The SRA must further assess the potential impact of the threats identified. In other words, it must examine the degree of harm that a potential threat would cause, were it to occur. This is not the same as determining the likelihood of the threat's occurrence, however. By way of example, if the covered entity had identified that it faced risks because its clinicians used their own mobile devices to access and store ePHI, it would need to consider the impact of such a device being lost or stolen. Even if the devices themselves were secured with effective encryption, a failure of such encryption could prove catastrophic if the device was stolen and the thief managed to break the encryption, even if such an occurrence was highly unlikely.

Having determined the potential impact of identified threats, the SRA then must include a determination of the level of risk involved with the threat. In other words, it must consider the likelihood that the threat could occur. As discussed above, the catastrophic nature of a given threat occurring may be offset by its extreme unlikeliness. By contrast, a threat that might impact the covered entity only slightly could be much more likely. For example, if a covered entity's office space includes windows that look onto a computer monitor which only displays an appointment calendar, and the appointment calendar only shows the time of the appointment, a first initial, and the last name of the patient, then the potential impact might be relatively low (given

the limited ePHI visible), but the likelihood of it being improperly disclosed might be high (given the location of the computer and its visibility to people outside). Based on a consideration of both the potential impact and the likelihood of occurrence of each identified threat, the SRA should then assign each threat a risk level.

Lastly, the SRA must actually document all of the above required elements in a written form. It is not enough to merely say that one has conducted an SRA—there must exist written proof. However, the OCR does not mandate the use of any specific format, which offers covered entities flexibility in how they present the results of their SRAs.

Under the Security Rule, the SRA should be updated periodically, and whenever the covered entity's electronic infrastructure changes, or other aspects discussed within the SRA itself have changed (e.g., if the physical layout of the office changes, due to renovations). The purchase of a new EHR software suite, providing practitioners with new mobile devices, even the installation of a new wireless printer can all require that the covered entity revisit its SRA, at least with respect to the new circumstances.

Security Rule Requirements

Once a covered entity has conducted an SRA, it is in a much better position to establish Administrative, Physical, and Technical Safeguards. Conducting an SRA meets one of the requirements for Administrative Safeguards. The remainder mostly address safeguards relating to personnel and administrative activities. The first of these is appointing a Security Officer (who may also be the covered entity's Privacy Officer). This individual should be technologically savvy enough to understand the technical aspects of Security Rule compliance, but also capable of communicating both with technical and nontechnical workforce members. In addition, the Security Officer should be someone either familiar with or capable of learning about the Security Rule requirements; having an understanding of these will be critical to the Security Officer's tasks.

Other Administrative Safeguards include the need to develop policies and procedures to prevent, detect, correct and contain security violations. Other policies and procedures should address workforce security (e.g., ensuring that workforce members access ePHI only as authorized, and establishing policies and procedures to respond to unauthorized access incidents). Administrative Safeguards also include workforce training efforts, establishing incident procedures to respond to security violations and developing contingency plans to respond to disasters or emergencies that endanger the security and integrity of ePHI.

Physical Safeguards are those relating to the physical space in which the covered entity houses its ePHI. They include facility access controls, whereby a covered entity must address how to prevent unauthorized individuals from accessing the facilities housing ePHI. For example, the covered entity must decide how to physically secure a server room or a room with a firewall devices so that it is only accessible to authorized individuals. This could be by use of a simple key lock, the key to which is held only by such individuals, or it could involve something as elaborate as a biometric scanner (e.g., fingerprint scanner, retinal scanner, voice recognition software, etc.). Physical Safeguards also include establishing policies and procedures regarding workstation use, such as requiring employees to log off of a workstation if they will be away from it for more than a specific amount of time. In addition, it can include policies and procedures regarding removal and transportation of ePHI on mobile storage devices, such as thumb drives or laptops.

Technical Safeguards address a host of technically oriented issues. In most cases, they are what people will likely think of when they imagine the requirements of the Security Rule. For example, Technical Safeguards touch on issues such as whether to use encryption, policies and procedures addressing authentication of users of systems containing ePHI (e.g., passwords, how often those passwords are changed, how complicated they must be, etc.), policies and procedures addressing the integrity of ePHI (e.g., preventing unauthorized modification or destruction of ePHI), and transmission security (e.g., preventing unauthorized access to ePHI transmitted through electronic means).

Conclusions

The complexity and scope of the various safeguards further demonstrates the necessity of conducting an SRA. Many covered entities, however, are ill equipped to conduct the SRA on their own. They may lack the technological knowledge necessary to effectively anticipate threats and vulnerabilities, or to find effective solutions. Often, an outside security consultant may be better positioned to perform the SRA on the covered entity's behalf. This also can be done in coordination with legal counsel, using attorney-client privilege and attorney-work product privilege as the document goes through multiple drafts.

However, in the current HIPAA climate, covered entities can no longer afford to ignore their Security Rule obligations. Larger covered entities can face massive fines for Security Rule failures, given the scope and impact of data breaches compromising ePHI. Smaller covered entities can no longer assume that they are "small potatoes" and therefore of little concern to the OCR. The Phoenix Cardiac Surgery settlement, and the results of the OCR's HIPAA Audit Pilot Program and continued Phase 2 audits suggest otherwise.

Moreover, given how much of the practice of medicine involves ePHI, and given the rise in hacking incidents and ransomware attacks, covered entities should assume that they face a "when, not if" scenario. A breach will eventually occur. When it does, the question becomes whether the covered entity has met is requirements under the Security Rule. If it has not, the covered entity may find itself on the sharp end of the OCR's stick, paying large fines and engaging in costly and time-consuming remedial actions.