akerman

Practice Update

Compliance with HIPAA—Help for Small and Mid-Sized Providers

April 30, 2018
By Elizabeth F. Hodge

Based on the results of the Office for Civil Rights (OCR) Health Insurance Portability and Accountability Act of 1996 (HIPAA) Phase 2 desk audits for covered entities, small and mid-sized providers (Smaller Providers) are on the OCR's radar when it comes to complying with HIPAA's risk assessment and risk management requirements. Unfortunately, Smaller Providers have also piqued the interest of cyber criminals. A recent report concluded that 69% of Smaller Providers participating in the HITRUST CyberAid Program experienced intrusion attempts and 65% detected malicious URL and command-and-control events.[1] This news comes as Smaller Providers continue to struggle with HIPAA compliance. While large providers typically have a dedicated compliance staff, Smaller Providers often lack such resources and must rely on employees who wear multiple hats, including those unrelated to HIPAA and compliance. The OCR audit results show that Smaller Providers cannot merely hope that the OCR will focus on larger providers. This article offers cost-effective suggestions that Smaller Providers can implement to improve their HIPAA compliance.

Results of Phase 2 OCR HIPAA Audit Program

According to an OCR representative, of the 166 covered entities selected for a desk audit in Phase 2

Related People

Elizabeth F. Hodge

Related Work

Data Privacy and Security

Health Insurers and Managed Care Organizations

Healthcare

Related Offices

Chicago

West Palm Beach

of the audit program, 90% were health care providers, and while some hospitals and nursing homes were included in the audit pool, most of the providers were Smaller Providers.[2] Of the 63 covered entities audited on their compliance with the requirement to conduct a risk anal-ysis, 46 auditees (73%) demonstrated either “negligible efforts” or no evidence of a serious attempt to comply with: (1) the risk analysis requirement;[3] and (2) the risk management requirement (i.e. implement security measures sufficient to reduce risks and vulnerabilities identified in a risk analysis to a reasonable and appropriate level). While the audit pool is admittedly small, these findings are likely representative of Smaller Providers as a whole.

Don’t Forget Professional Standards and State Data Breach Laws

Smaller Providers need to remember that HIPAA is not the only law requiring the appropriate safeguarding of patient information. State practice acts also impose an obligation on practitioners to protect the confidentiality of such information. Thus, a violation of HIPAA can also be a violation of a practice act, potentially putting the provider’s license in jeopardy.

Additionally, the American Medical Association (AMA) Code of Ethics requires physicians to “safeguard patient confidences and privacy within the constraints of the law.”[4] The Code of Ethics also says that a physician using an electronic health records system is expected to conduct due diligence to select a system that “conforms to acceptable industry practices and standards” with respect to, among other things, measures to ensure data security and integrity and the capacity to routinely audit access to records.[5]

In addition to professional obligations to secure patient records, physicians may also be subject to state data breach laws. Smaller Providers must also determine if they may be subject to any other federal or state privacy laws such as 42 C.F.R. Part 2 (governing confidentiality of substance use disorder records).

Recognize the Challenges

Smaller Providers face unique challenges with HIPAA compli-ance. The technology driven language of the Security Rule can be overwhelming and requires some specific expertise to understand and implement. However, there are relatively inexpensive yet high impact steps that Smaller Providers can take to comply with the Security and Privacy Rules.

Know Where Data Resides and Flows

With the proliferation of devices, the internet of things, and health apps, Smaller Providers must thoroughly understand where their data is maintained, and how it is transmitted and accessed. Understanding the flow of electronic protected health informa-tion (e-PHI) is necessary to conduct a complete and accurate risk assessment. A provider and any consultant hired to assist with the risk assessment should consider all applications, electronic health record systems, billing systems, documents and spread-sheets, database systems, web servers, fax servers, backup servers, cloud based servers, medical device messaging apps, and other media. Many Smaller Providers use outside vendors to provide IT services and should include them in the risk assessment process.

The OCR and the Office of the National Coordinator for Health Information Technology have created a free risk assessment tool for Smaller Providers that is designed to help identify and implement the most cost effective and appropriate administrative, physical, and technical safeguards to protect e-PHI.[6] Whether the Smaller Provider is performing the risk assessment on its own (using a tool) or working with a consultant, it must take a broad view of the data landscape so as not to inadvertently omit a device or system.

Follow Through after the Risk Assessment

It is not enough to perform the risk assessment. Security Rule compliance involves not only identifying and documenting risks, but also mitigating and managing the identified risks by imple-menting security measures sufficient to reduce the risks and vulnerabilities to a reasonable level. OCR has noted a trend in enforcement cases where risks had been previously identified but there was no follow through in the implementation of security measures and as a result, breaches occurred. For instance, the OCR's investigation of CardioNet, a wireless health services provider, revealed that it had performed an insufficient risk analysis and had inadequate risk management processes in place when one of its laptops was stolen. The investigation revealed that although CardioNet had drafted HIPAA policies and procedures, it had not finalized or implemented them.[7]

Smaller Providers should develop and implement a risk manage-ment plan. This plan will provide structure for assessing, prior-itizing, and implementing security measures to reduce the risks identified in the risk assessment. As the CardioNet and other resolution agreements show, covered entities must actually implement security measures to reduce identified risks. Smaller Providers should also periodically evaluate and the monitor the effectiveness of measures that are in place as threats and vulner-abilities to e-PHI can change over time. Finally, OCR expects Smaller Providers to document the risk analysis and the resulting risk management activities.

Document, Document, Document

OCR expects covered entities, including Smaller Providers, to document the risk analysis and resulting risk management activities. According to the OCR representative, based on the documentation submitted by auditees, it appeared that many providers could not demonstrate that they had engaged in the risk analysis process in the prior six years. Further, based on OCR comments regarding the desk audit findings, Smaller Providers must document their risk analysis, including rating the potential harms or vulnerabilities to the PHI they create, receive, and maintain.

Awareness and Education

Awareness and education can have a big impact in preventing cybersecurity incidents. The insider threat of current and former workforce members can generally be managed through training and education, yet many providers fail to foster an environment of awareness and appropriately train staff. Consequently, insiders remain a source of breaches.

Smaller Providers can develop a culture of security and awareness by educating workforce members on security matters through annual training and regular communication on security trends and best practices. The OCR's cybersecurity newsletters are infor-mative and may be shared with workforce members to remind them of the importance of security and sensitize them to security issues. Providers may also sign up for OCR's free Security and Privacy Listservs to receive the latest information about resolution agreements and guidance from OCR on topics of concern and use these communications as part of their ongoing education efforts.[8]

Access Control

The Security Rule requires providers to implement policies and procedures to ensure that workforce members have appropriate access and to prevent those who do not need access from obtaining it. Smaller Providers should include screening procedures as part of their workforce clearance and onboarding process and termination procedures to revoke access privileges as part of the workforce separation or termination process. Identity and access management policies and controls are critical to reduce the risks posed by insider threats.

Know Your Vendors

A provider should also understand what its vendors do and how they do it—particularly those who access, maintain, or transmit protected health information (PHI) on its behalf. Covered entities must enter into business associate agreements (BAAs) with those businesses or individuals that create, receive, maintain, or transmit PHI on their behalf. This requirement applies whether the PHI is in paper or electronic format. For example, many Smaller Providers use cloud storage providers (CSPs) because of the economies of storing e-PHI in the cloud. The OCR views CSPs as business associates, even where the PHI is encrypted in the cloud and the CSP does not have the encryption key.[9] As part of the Phase 2 audit program, the OCR published a template to help audited covered entities track their business associates. This tool is also helpful for any covered entity trying to stay current with its business associates.[10]

Avoid Marketing Mishaps

Providers sometimes include patient testimonials on their websites as part of their marketing efforts. Before using iden-tifiable patient information as part of a marketing campaign, providers must obtain a signed authorization from the patient permitting the use and disclosure of the patient’s information for that purpose. The authorization is required whether the provider is using a testimonial from the patient or “before and after” photographs. Failure to obtain proper permission from the patient is an improper use or disclosure of PHI and can subject the provider to enforcement activity. For example, a physical therapy practice entered into a resolution agreement with the OCR after someone complained that the practice impermissibly disclosed individuals' PHI on its website when it posted patient testimonials without first obtaining HIPAA-compliant authorizations from the patients.[11] The testimonials included the patients' full names and full face photographs. The practice agreed to pay $25,000 and develop policies and procedures addressing obtaining authorizations before using patient PHI.

Have an Incident Response Plan Before You Need It

It is not a matter of if a covered entity will have a breach, but when. The Security Rule requires that covered entities estab-lish policies and procedures for responding to an emergency or other occurrence that damages systems containing e-PHI. Such situations can include malware attacks (including ransom-ware), system failure, power outages, fire, vandalism, and natural disasters. An incident response plan should be created before something happens. Smaller Providers should designate an individual to serve as the "incident commander," and depending on the size of the organization, have a backup in case the incident commander is unavailable and, where possible, a small team to assist. Providers who outsource their IT functions should include the IT vendor in the response team.

Because of the short timelines under federal and state law to provide notice of a breach to affected individuals, it is prudent to plan ahead. Negotiating contracts with professionals and consultants while dealing with a breach distracts from mitigation. Identifying vendors to assist with breach response, forensics, legal, and public relations in advance allows the practice to more efficiently and effectively respond when there is an incident. Smaller Providers should inquire whether their cyber liability insurer has a list of preferred vendors or coordinates with breach response vendors.

Conclusion

As resolution agreements and the Phase 2 audit program demon-strate, Smaller Providers cannot stick their heads in the sand when it comes to compliance with HIPAA. Fortunately, there are cost-effective, relatively easy steps that Smaller Providers can take to identify and safeguard the PHI they create, receive, maintain, and transmit to comply with HIPAA and their relevant licensing and ethical requirements.

The authors would like to thank Stacey Callaghan of Akerman LLP for her assistance with this article.

Footnotes

[1] HITRUST and Trend Micro November 2017 Healthcare IT Security Bulletin.

[2] Comments by Linda Sanches, at the NIST/OCR 10th Annual Conference, Safeguarding Health Information: Building Awareness through HIPAA Security, September 6, 2017.

[3] According to the OCR, no auditee demonstrated that it had current and prior risk analysis results, policies, and procedures of the risk analysis process, or documentation of the implementation of its risk analysis process.

[4] American Medical Association, Principles of Medical Ethics, https://www.ama-assn.org/delivering-are/ama-principles-medical-ethics (last visited site Dec. 5, 2017).

[5] AMA Code of Medical Ethics Opinion 3.3.2.

[6] The tool is available at https://www.healthit.gov/providers-professionals/securi-ty-risk-assessment-tool.

[7] The press release is available at https://www.hhs.gov/about/news/2017/04/24/2-5-million-settlement-shows-not-understanding-hipaa-requirements-creates-risk.html. The Resolution Agreement and Corrective Action Plan is available at https://www.hhs.gov/sites/default/files/cardionet-ra-cap.pdf (last accessed on 12/20/17).

[8] See https://www.hhs.gov/ocr/list-serve/index.html.

[9] https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html (Site last visited January 8, 2018).

[10] The BAA tracking template is available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html.

[11] The Resolution Agreement is available at https://www.hhs.gov/sites/default/files/cpt-res-agreement.pdf (last accessed on 12/20/17).