Published on *The National Law Review* https://natlawreview.com

HIPAA Auditors Are Coming!

Article By:

Ned Milenkovich

Paul Revere, a patriot in the American Revolution, is best known for his “midnight ride” during which he alerted the Colonial militias in and near Concord, Massachusetts of an impending attack by yelling “The British are coming!” While history has taught us that Revere did not utter these exact words, he did set out on horseback shortly before midnight on April 18, 1775, and orally delivered coded warnings that allowed the militias to confront the British troops and repel their advances all the way back to Boston. Today, health care attorneys have a warning of their own to deliver to organizations that are covered entities or business associates under the ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)***: “The HIPAA auditors are coming!”

Health care providers, health plans, health care clearinghouses and their business associates need to know that the ***U.S. Department of Health and Human Services***’ ***Office of Civil Rights (OCR)*** is starting to roll out the second phase of HIPAA audits (Phase II Audits). Now is the time to assess your organization’s compliance with HIPAA’s security rule (Security Rule). If your organization is selected for a Phase II Audit, are you ready?

Background

In February 2014, the OCR issued a notice that stated its intent to survey to up to 800 covered entities and 400 business associates through a second phase of HIPAA audits. After several delays, the OCR started the audit process in early 2015 by sending out pre-audit screening surveys to hundreds of health care organizations. Based on the timeline proposed by the OCR, Phase II Audits are anticipated to start in earnest in the fall of 2015.

The Phase II Audits will examine covered entities and business associates. In comparison, audits performed in 2011 and 2012 (Phase I Audits) only focused on covered entities. While Phase I Audits were a comprehensive review of a covered entity’s compliance with all aspects of the HIPAA Security Rule, Phase II Audits will only address specific areas of concern. The OCR’s auditors will zero in on areas of higher risk that are more likely to threaten the privacy and security of protected health information (PHI) and on organizations that have patterns suggesting repeated non-compliance with the Security Rule.

The OCR stated that most of the Phase II Audits will be conducted by desk review; however, comprehensive on-site reviews are also possible. According to a high-level official at the OCR,

organizations that are in noncompliance with HIPAA's Security Rule could face civil monetary penalties ranging from "$215,000 on the low end right up into the millions of dollars."

HIPAA Risk Assessment

Health care organizations that did not receive a pre-audit screening letter from the OCR this past spring should not assume that they are through the HIPAA-audit woods. With the rising number of data breaches, it is not unreasonable for health care organizations to anticipate increased scrutiny concerning compliance with the Security Rule. If your organization wants to avoid severe fines, it is imperative to determine if your organization is in compliance with all applicable standards and requirements in the Security Rule. If you are not sure that your organization is compliant, you should complete a risk assessment as soon as possible.

The risk assessment should examine your organization's compliance with HIPAA's administrative safeguards, physical requirements and technical standards. As a first step, health care organizations may want to download a free "***Security Risk Assessment (SRA)*** Tool" that is available at http://www.healthit.gov. The SRA Tool asks 156 yes-or-no questions that can help determine your organization's compliance with HIPAA. After you have completed the risk assessment, you may want to review your answers with a health care attorney who is experienced with the HIPAA Security Rule, especially if you have identified areas of concern.

Conclusion

The Colonial militias heeded the warnings from Paul Revere and prepared for attack. Because of their efforts, the militias were able to defeat the British Army. If you are a health care organization that is a covered entity or a business associate that must comply with the HIPAA Security Rule, are you confident that your organization is fully compliant with the rule's administrative, physical and technical standards? If you are wrong, can your organization cover the cost of a large monetary fine? If not, it is time to prepare for battle and conduct a HIPAA risk assessment.

National Law Review, Volume V, Number 259