VIEWS & VISIONS

A publication of Bowles Rice LLP

Summer 2015

A New Round of Federal Audits to Review HIPAA Privacy and Security Compliance

Susan Saxe, R.N., J.D., Director
Corporate Compliance & Regulatory Affairs
West Virginia University Physicians of Charleston

Susan B. Saxe is both a registered nurse and practicing attorney. She is currently employed as the Director of Corporate Compliance & Regulatory Affairs for West Virginia University Physicians of Charleston, a large academic physician group practice in Charleston, West Virginia.

Ms. Saxe obtained her BSN degree from West Virginia University's School of Nursing in 1980 and practiced clinical nursing for several years before entering law school. In 1989, she graduated at the top of her law school class at West Virginia University, where she was a Manuscript Editor of the West Virginia Law Review, a member of the Order of the Coif and a recipient of the Patrick Duffy Koontz prize for scholarly excellence. After graduating from law school, she clerked for two years for the Honorable John T. Copenhaver, Jr., United States District Judge for the Southern District of West Virginia. She is a former partner of Bowles Rice.

Ms. Saxe has extensive expertise and experience with the defense of practitioners and hospitals in medical malpractice actions. Her current practice places an emphasis on issues relating to risk management, corporate compliance and state and federal administrative and regulatory law. She has lectured frequently on issues of interest to the medical and legal community, and is a former Chair of the Law & Medicine Committee for the West Virginia State Bar.

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) establish national standards for the privacy of protected health information, the security of electronic protected health information and notification to consumers whose protected health information has been breached. The United States Department of Health and Human Services (HHS), specifically its Office for Civil Rights (OCR), is charged with the enforcement of these standards and related rules.

While much of the first decade of the OCR's enforcement activity was complaint driven, HITECH's provisions now require the agency to perform periodic audits of compliance, by HIPAA-covered entities and their business associates, with the provisions of the Privacy, Security and Breach Notification Rules. The first phase of those audits began in 2011, through a pilot program designed to assess compliance-related controls, policies and processes implemented by HIPAA covered entities, in order to address and satisfy privacy, security and breach notification obligations.

During the 2011 and 2012 audit initiative (Phase 1), 115 HIPAA-covered entities, including health plans, health care clearinghouses and individual and organizational providers, were selected for review and compliance scrutiny. As part of the Phase 1 review, a comprehensive audit protocol was established by the OCR for use in assessing covered entities' compliance with each of the privacy, security and breach notification requirements.[1]

Of the three types of covered entities reviewed during the Phase 1 audits, health care providers were found to have had the most issues of non-compliance, and smaller health care providers were generally vulnerable and non-compliant in all three audit areas. Only 11 percent of the covered entities reviewed during the Phase 1 audits had no negative findings or observations.[2] Approximately 40 percent of the findings relating to non-compliance were attributed to a lack of awareness of the specific requirements of the rules. Covered entities were reportedly most "unaware" of privacy requirements relating to notices of privacy practices, authorizations for the release of information to third parties, individual access rights and the "minimum necessary" standard.

While negative findings related to Privacy Rule compliance were substantial during the Phase 1 audits, approximately 60 percent of the negative findings were related to non-compliance with the Security Rule standards. In fact, at least one Security Rule deficiency was noted in 58 of 59 audited providers, with such deficiencies primarily attributable to inadequate system user monitoring, absent or insufficient risk assessment, absent or insufficient contingency planning, and errors or omissions relating to user access controls and media reuse and destruction.[3]

Armed with the information gleaned from the Phase 1 audits, OCR is now preparing to launch Phase 2 of the HIPAA/HITECH compliance audits. As noted in a February 24, 2014 notice in the Federal Register, the first step in this new round of audits is the agency's planned issuance of a mandatory pre-audit screening survey of up to 1,200 covered entities and business associates.

According to the notice, not all of the surveyed organizations will be selected for audit. Instead, the survey will be used to "gather information about respondents to enable OCR to assess the size, complexity and fitness of a respondent for an audit."[4] The Phase 2 audit initiative, although initially expected to start between October 2014 and June 2015, was delayed due to federal budgetary constraints. Consensus within the industry is that the Phase 2 audit process may begin sometime in late 2015.

Once a covered entity is actually selected by OCR for a compliance audit, it must respond to a time-sensitive data request, including a disclosure of its business associates who, unlike Phase 1, are also subject to audit in Phase 2. According to OCR's representatives, once notified of selection for an audit, covered entities will have only two weeks to provide a comprehensive response to the OCR's data request. Extensions and supplemental filings will not be permitted.[5] *Although an exact commencement date for the Phase 2 audits has not yet been announced, covered entities and their business associates must prepare now to ensure that they are able to fully and quickly respond to an audit notice, and are able to demonstrate good faith compliance with the numerous and complex regulatory standards set by HIPAA and HITECH.*

As part of their specific pre-audit preparations, covered entities and their business associates must verify that they have a complete and accurate security risk analysis in place as required by the Security Rule, and that their HIPAA privacy and security policies and procedures are current and address all of the relevant regulatory standards. By downloading and utilizing OCR's Phase 1 HIPAA audit protocol as a guide, covered entities and business associates can begin their own assessment of policy and procedure gaps and areas of non-compliance, for which outside guidance and/or expertise may be needed to ensure audit readiness.[6]

[1] *The Phase 1 audit protocol is available for public review on the OCR website. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html*

[2] *Lessons Learned from OCR Privacy and Security Audits, Program Overview and Analysis, Linda Sanches and Verne Rinker, Presentation to IAPP Global Privacy Summit (Mar. 7, 2013).*

[3] *Id.*

[4] *79 Fed. Reg. 10158 (Feb. 24, 2014).*

[5] *Sanches/Verne Commentary, supra.*

[6] *For the Phase 2 audit initiative, OCR is in the process of revising its audit protocol to reflect the changes included in the HIPAA Omnibus Rule that became effective on September 23, 2013.*