SQUIRE PATTON BOGGS

New HIPAA Audit Process to Expose Many Healthcare Providers and Vendors to Enforcement

Overview

The Office for Civil Rights (OCR) of US Department of Health & Human Services is initiating an auditing process to evaluate compliance with provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is expected that the audits will expose many healthcare providers and their vendors to enforcement actions.

The increasingly widespread use of electronic protected health information poses a risk to the privacy and security of such information. The HITECH Act requires HHS to perform periodic audits of covered entity and business associate compliance with the HIPAA Privacy and Security Rules. In 2011, OCR, as the agency responsible for the enforcement of these rules, established a pilot audit program to assess the compliance controls and processes implemented by covered entities. Based on the results of the pilot program, OCR developed a protocol to measure the efforts of 115 covered entities – the Phase 1 audit program.

Phase 1 Audits

OCR's audit protocol contains the elements for assessment during the audits. The protocol is organized around modules, representing separate elements of privacy, security and breach notification. It is anticipated that the combination of these elements will vary depending on the type of covered entity or business associate selected for review. First, the protocol covers the following Privacy Rule elements: (1) notice of privacy practices for protected health information, (2) rights to request privacy protection for protected health information, (3) access of individuals to protected health information, (4) administrative requirements, (5) uses and disclosures of protected health information, (6) amendment of protected health information and (7) accounting of disclosures. Next, the protocol covers Security Rule elements for administrative, physical and technical safeguards. Finally, the protocol covers elements for the Breach Notification Rule. The protocol sets forth for each element of the protocol the specific section of the HIPAA Rules, established performance criteria, key activity associated with the performance criteria, audit procedures, nature of any implementation specifications and which area of the HIPAA Rules the element implicates (Privacy, Security or Breach Notification).

Phase 2 Audits

Based on the results of the Phase 1 audit, in March 2016, OCR announced Phase 2 of the HIPAA audit program as a part of its continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules.

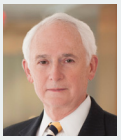
This next phase of the audit program will review the HIPAA policies and procedures adopted and used by both business associates and covered entities to meet certain standards and implementation specifications of the Privacy, Security and Breach Notification Rules. OCR intends to identify best practices learned through the audit process and provide industry guidance for addressing compliance challenges.

Currently underway, the first step of Phase 2 is to identify a pool of potential auditees by reaching out to covered entities and business associates of all sizes and functions. Sampling criteria for the randomly selected auditees will include: (1) size of the entity, (2) affiliation with other healthcare organizations, (3) the type of entity and its relationship to individuals, (4) whether an organization is public or private, (5) geographic factors and (6) present enforcement activity with OCR. Any entity with an open complaint investigation or that are currently undergoing a compliance review will be excluded from the pool of potential auditees.

The Phase 2 audit process will include desk and onsite audits for both covered entities and business associates. The initial set of audits will be desk audits of covered entities followed by a second round of desk audits of business associates. OCR intends to complete all desk audits by the end of December 2016. Next, a third set of audits will be conducted onsite and will examine a broader scope of HIPAA requirements. Some desk auditees may be subject to a subsequent onsite audit. The auditors prepare and share draft findings with the auditees who will have an opportunity to respond to the draft findings. Such comments will be included in the final audit report.

Upon completion of the final Phase 2 audit reports, OCR will analyze the information and develop aggregated results to better understand compliance efforts with particular aspects of the HIPAA Rules. It is OCR's general intent to use the audit reports to determine the types of technical assistance and corrective actions that should be made available to covered entities and business associates. However, where an audit report reveals a serious compliance issue, OCR may initiate a compliance review to further investigate. While OCR plans to make the audit results transparent, it will not post a listing of audited entities or the findings of an individual audit. Under the Freedom of Information Act (FOIA), however, OCR may be required to release audit notification letters and other information about these audits.

Contact



John E. Wyand
Principal, Washington DC
T +1 202 626 6676
E john.wyand@squirepb.com