HIPAA Phase 2 Audits

The U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) began a pilot program in 2012 to assess the procedures implemented by covered entities to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA). OCR evaluated the effectiveness of the pilot program and then announced Phase 2 of the program on March 21, 2016. Phase 2 Audits focus on the policies and procedures adopted by both covered entities and business associates to ensure they meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. Covered entities include health plans, health care clearinghouses, and health care providers; whereas, business associates include anyone handling health information on behalf of a covered entity.

Phase 2 Audits of business associates focus on risk analysis, risk management, and reporting of HIPAA breaches to covered entities. OCR emphasizes the importance of audits as a compliance improvement activity in order to identify best practices and proactively uncover and address risks and vulnerabilities to protect health information (PHI).

OCR chose entities to audit through random sampling of the audit pool. Communications from OCR were sent via email, so it is important to check spam filters and junk emails for communications from OSOCRAudit@hhs.gov. OCR emailed a notice to verify contact information. Once the contact information was verified, OCR emailed a pre-audit questionnaire to gather data about size, type, and operations of the entity. This data was used with other information to develop pools of potential covered entities for making audit selections.

Phase 2 Audits consist of three sets of audits. The first set of audits will be desk audits of covered entities and the second set of audits will be desk audits of business associates. These audits will examine compliance with specific requirements of the Privacy, Security, or Breach Notification Rules and covered entities will be notified of their audit in a document request letter. All desk audits in this phase will be completed by the end of December 2016. OCR will select entities and request they electronically submit documentation within 10 days. The third set of audits will be onsite and examine a broader scope of requirements from HIPAA Rules.

On July 11, 2016, 167 covered entities were notified that they were selected for a desk audit. Entities selected for the audit received two communications from OCR: (1) an email notification of their selection with instructions on how to respond to the desk audit document request, a timeline for response, and a link to submit documents online; and (2) a request to provide a listing of the covered entity's business

associates and providers information about an upcoming webinar. The selected entities had 10 business days (until July 22, 2016) to respond to the desk audit document request. Desk audits of business associates will begin in the fall of 2016.

If you are a covered entity and were not selected for a desk audit, you may still be chosen for a field audit in 2017. Best practice is to have a list prepared of business associates and their contact information because OCR will ask for this information.

There will be fewer in-person visits during these Phase 2 audits than in Phase 1, but covered entities should be prepared for a site visit when OCR deems it appropriate. Auditors will review documentation and then develop and share draft findings with the entity, which will then have the opportunity to respond to the draft findings. Audit reports generally describe the way the audit was conducted, discuss any findings, and contain entity responses to the draft findings.

As a best practice, the covered entity should conduct a self-audit using the audit protocols chart and the compliance review checklist to ensure that the covered entity has addressed all required areas and has a binder of up-to-date documents that the checklist recommends.

Under HIPAA, covered entities are required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, availability, and integrity of electronic protected health information (PHI). In recent compliance reviews, the Centers for Medicare and Medicaid Services (CMS) has identified risk analysis to be a continuing weak area for covered entities.

In March 2014, the HHS and the Office of the National Coordinator for Health Information Technology (ONC) released a Security Risk Assessment Tool (SRA Tool) to assist small- to medium-sized heath care providers in conducting their risk assessments by walking them through yes/no questions, including fields where supplemental information can be provided, that mirror the security sections of the OCR audit protocol chart referenced above. Based on the covered entity's answers, the SRA Tool explains whether corrective action should be taken and provides additional resources. The answers and risk remediation plan can be saved directly on the SRA Tool to generate a report. The information and report do not go to HHS or OCR; the SRA Tool is downloaded to the covered entity's computer and the answers are saved on the user's computer, not online.

Based on the recently released Ransomware and HIPAA Fact Sheet, during an audit, OCR may be particularly interested in whether the covered entity experienced any ransomware incidents and if so, how the covered entity has addressed those incidents. Ransomware is a type of malware that attempts to deny access to a user's data by encrypting data with a key known only to the hacker who deployed the malware, until a ransom is paid. If the covered entity has not experienced any ransomware incidents, then the covered entity should have a written process in place to detect, guard against, and report any ransomware incidents.

7/28/2016