CARLTON FIELDS

The HIPAA Audits are Coming, The HIPAA Audits are Coming!

April 04, 2016

Five Steps to Prepare for a HIPAA Audit

The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) recently announced the long-awaited launch of phase 2 of HIPAA's audit program. The program will target all types of covered entities, such as large organizational and individual health care providers, health insurance plans of all sizes, and health care clearinghouses—*and* their business associates. The OCR intends to include a broad spectrum of candidates so that it can better assess industry-wide compliance. Only those entities currently under investigation or undergoing compliance review by the agency are exempt from this phase. The OCR plans to complete the phase 2 audits by December 2016. Step one of the audit, verifying contact information of covered entities and business associates, is underway. The OCR is sending emails requesting this verification and warns that entities must check their junk mail and spam accounts for them. Contacted entities will have 14 days to respond to the email. But, the OCR says that even an entity that fails to respond to the initial email may be selected for an audit, or subject to a compliance review. Step two is the desk audit. The OCR will send requests for documents to selected entities and do a review based on the entity's response. Once contacted, those covered entities will have 10 days to submit the requested data and documents via a new audit electronic portal. At a minimum, entities should expect to be asked to produce copies of their policies and procedures along with documentation showing the results of the company's risk assessment and existing business associate agreements. The first round of desk audits will be limited to covered entities. The second round of desk audits will be of business associates and relate to their HIPAA compliance. Be aware that the OCR says site visits are optional during the desk audit phase. Step three will be onsite audits. Onsite audits of selected entities will begin with an entrance conference and last from three to five days, depending on the entity's size. Following the completion of each audit, desk, and onsite, the OCR will provide the entity with a draft of its findings. The audited entity will have 10 business days to review and return written comments to the OCR. The OCR will review any comments and provide the entity with its final report within 30 business days after the entity's response. The OCR says it intends these audits

as compliance improvement activities, but admits it will investigate serious compliance issues discovered during an audit. It is worrisome that the OCR has not defined what constitutes a "serious incident." A September 2015 OIG report said the OCR was not investigating enough incidents, and reports of recent enforcement actions suggest the OCR is at its "wit's end" with continued non-compliance of HIPAA regulations. As a result, there is speculation that almost any violation could be deemed a serious incident. A review of recent enforcement actions punctuated with large fines, likely provides some insight into the OCR's current hot-button issues. For example, the OCR recently settled with Triple-S Management Corp., an insurance holding company, for $3.5 million for failing to perform a risk assessment, failing to have business associate agreements in place, and failing to implement appropriate safeguards. The OCR settled with Feinstein Institute for Medical Research for $3.9 million stemming from a breach that resulted when a laptop computer holding the information of 13,000 patients was stolen from an employee's car. And, North Memorial Health Care of Minnesota reached a $1.55 million settlement with the OCR after a business associate's unencrypted laptop holding the information of 9,497 individuals was stolen. The OCR identified the failure to have a business associate agreement in place as a specific area of concern. Considering the most recent settlements and the fact that most audits will be paper based (desk audits), we offer the following recommendations to prepare for the upcoming HIPAA Audits. 1. Review and update HIPAA policies and procedures. Privacy and security policies are mandatory. If the OCR investigates a business and determines it has no policies, the business will be fined. Policies have been required for more than a decade and it is clear that the OCR has no patience for facilities that have yet to address this requirement. Each entity should review current policies and revise or update them as necessary. In addition, entities should ensure they have a policy that addresses the use of laptop computers and other mobile devices, and a policy about removing protected health information (PHI) from the physical business. If a policy permits PHI to be transported on mobile devices, entities should seriously consider a mandatory encryption policy. Encryption is a de facto requirement. 2. Review business associate agreements. Entities must identify all business associates and review existing business associate agreements. If the entity doesn't already have one, it would be wise to create an inventory of business associates and existing agreements. The entity must ensure that there is a valid business associate agreement in place for all business associates. If the entity discovers that it is disclosing PHI to a business associate without an agreement in place, it should get one signed as soon as possible. Also, if any business associate agreement was signed before January 2013, the entity must ensure the agreement complies with the revised rules, or must update the agreement. 3. Review your existing risk assessment or perform an updated risk assessment. A risk assessment is another key requirement. During phase one of the HIPAA audits, the OCR discovered that two-thirds of entities did not have a complete and accurate risk assessment in place. During phase two, entities should expect scrutiny of their risk assessments. The OCR says that the risk assessment should be ongoing and recommends an annual analysis. As part of a risk assessment the entity must review its current security measures including the administrative, physical and technical safeguards that protect the security of PHI, the threats and vulnerabilities to PHI, including the likelihood and impact of those events, and a list of corrective actions in case a

threatened event occurs. The risk assessment must be documented and retained for a minimum of six years. 4. Review other HIPAA required documentation. Entities are required to provide HIPAA training to all employees and maintain a record of that training. Each entity should review its current logs and provide any additional training as needed. New hires require training and must be listed in the training logs. Entities are also required to maintain logs of disclosures of PHI and responses to breaches. Each entity should determine if it has any such logs, create logs if required, and review existing logs for completeness. Health care providers and health plans are required to have Notice of Privacy Practices. Those entities should review their notice for compliance. 5. Consider how your business will respond to an audit Entities should consider appointing an audit team or lead responder so the business can respond within the limited time frame allowed for responding to the audit requests. That appointee should be able to quickly access the necessary documents, and should also monitor email inboxes for messages from the OCR. Emails from the OCR will be sent from OSOCRAudit@hhs.gov.

Authored By

Patricia S. Calhoun

Related Practices

Cybersecurity and Privacy
Health Care

Related Industries

Health Care
Life, Annuity, and Retirement Solutions
Property & Casualty Insurance

accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.