Reinhart

HIPAA Harvest? Be Prepared to Be Picked by OCR for Round 2 HIPAA "Enforcement" Audits

Citing widespread noncompliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, the Department of Health and Human Services (HHS), Office of Civil Rights (OCR) indicates that the next phase of HIPAA audits will focus on electronic protected health information (e-PHI) security. Although this emphasis is consistent with industry predictions, recent commentary by OCR representatives suggests that the agency expects these audits to result in increased enforcement action for Security Rule violations. Health care providers and their business associates, who are also subject to the Security Rule, are advised to review the status of their HIPAA Security Rule compliance in preparation for this upcoming wave of HIPAA enforcement.

POSTED:

Oct 8, 2014

RELATED PRACTICES:

Health Care

https://www.reinhartlaw.com/practices/health-care

RELATED PEOPLE:

Heather L. Fields

https://www.reinhartlaw.com/people/heather-fields

Pre-Audit Surveys and Updated Audit Protocol

OCR will conduct a pre-audit survey of approximately 550 to 800 entities to gather information to enable OCR to assess the size, complexity and "fitness" of the entity for an audit.[1] Entities that may be surveyed include health care providers, health plans, health care clearing houses and business associates. OCR will collect information such as recent data about the number of patient visits or insured lives, use of e-PHI, revenue and an entity's location. Originally planned for the summer of 2014, the pre-audit surveys have been delayed until OCR is able to implement a new web portal through which OCR will conduct the surveys.

OCR will use the results of these pre-audit surveys to select entities to audit. Entities selected for an audit will receive notification and data requests electronically. Originally, OCR planned for most audits to consist of desk audits focused on selected HIPAA provisions that were the source of a high number of compliance failures in the pilot audits, with an undisclosed number of comprehensive on-site audits if resources allowed. However, OCR recently stated that it now intends to do a larger number of comprehensive on-site audits and "fewer than 200 desk audits," down from the originally planned 400 desk audits, citing additional funding and the availability of a web portal to conduct audits.

OCR intends to assess entity compliance efforts using an updated audit protocol that reflects changes included in the HIPAA Omnibus Final Rule issued January 25, 2013.[2] In addition to the audit data requests, selected entities will also be asked to

identify and provide current contact information for their business associates. In 2015, OCR plans to audit business associates selected from this pool of identified business associates.

Phase II Audit Preparation Needed

OCR's 2012 HIPAA pilot audit program was an "assess and inform" audit. These audits revealed widespread HIPAA noncompliance regarding both the Privacy Rule and the Security Rule. Indeed, two thirds of the entities audited did not have complete and accurate risk assessments of threats to or vulnerabilities of e-PHI held by the entity.[3] Thankfully for those audited, OCR used the results to provide education and training to entities regarding HIPAA requirements. In contrast, OCR officials have made it clear OCR intends to use this round of audits as "an enforcement tool."

Given the prevalent failures identified during the last round of audits, OCR's next audit phase will likely target risk assessments, and may focus on whether and how entities have employed data encryption. Accordingly, health care entities and their business associates should pay particular attention to the current status of their Security Rule compliance program. Among the action steps that should be considered to prepare for a possible audit are the following:

- **Update Security Rule Risk Analysis, and Related Security Policies and Procedures.** Ensure your risk assessment, risk management plan, and accompanying policies and procedures are current and compliant. Responsive materials provided during the Phase II audits must be current *as of the date of the request*, not the submission. Health care providers would be well advised to use the OCR audit protocol once released on OCR's website. Until that time, the current protocol is available.
- **Watch Your E-mail.** OCR will be sending pre-audit surveys, audit notifications and document requests through e-mail or other electronic media (e.g., CDs). Selected entities will have only two weeks to respond to data requests, so prompt awareness of a data request is imperative. Failure to submit a response to a request may lead to a referral for regional compliance review.

The Health Care team at Reinhart Boerner Van Deuren s.c. is available to assist you in developing and implementing a HIPAA compliance plan, including developing a risk assessment and risk management plan.

Please feel free to contact Heather L. Fields or any other member of Reinhart's Health Care team, or your Reinhart attorney, to discuss any questions or concerns related to your health care entity.

---

[1] 79 Fed. Reg. 10158 (Feb. 24, 2014); *See* Linda Sanches, OCR Senior Advisor, OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2 (March 31, 2014).

[2] 78 Fed. Reg. 5566 (Jan. 25, 2013).