WINSTEAD

No HIPAA Hall Pass for Business Associates and Small Breaches

09.01.16

Phase 2 Audits of Business Associates:

The Department of Health and Human Services, Office for Civil Rights (OCR) is in the process of conducting its phase 2 audits of Covered Entities and Business Associates. "Covered Entities" include health plans, healthcare clearinghouses, and healthcare providers who transmit any health information in electronic form. Vendors of these Covered Entities are referred to as "Business Associates." These Business Associates create, receive, maintain, or transmit protected health information on behalf of a Covered Entity.[1]

Covered Entities have already been notified if they were selected for a HIPAA desk audit conducted by OCR. The audits cover compliance with the HIPAA privacy, security, and breach notification rule.

Guess who's next? That's right, Business Associates will be audited this fall. Whether you are a Business Associate or Covered Entity, you can learn from the experiences of others.

For the phase 2 audit, OCR is identifying Covered Entities and Business Associates that represent a wide range of health care providers, health plans, health care clearinghouses, and Business Associates. The auditees will be selected based on the following criteria:

- The size of the entity,
- Affiliation with other healthcare organizations,
- The type of entity and its relationship to individuals,
- Whether an organization is public or private,
- Geographical factors, and
- Present enforcement activity with OCR.

Entities with an open complaint investigation or that are undergoing a compliance review will not be audited.

The OCR's audit of Covered Entities required them to submit documentation supporting their compliance with the HIPAA notice of privacy practices, access, breach notification, risk analysis, and risk management requirements. OCR developed three guidance documents to assist audited entities. These documents are available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.[2]

Small Breach Investigations:

In addition, in August of 2016, OCR begun to more widely investigate HIPAA breaches impacting fewer than 500 individuals. This initiative is through the OCR Regional Offices. The Regional Offices will have discretion to determine which smaller breaches to investigate. However, each office will increase its efforts to identify and obtain corrective action with respect to systematic noncompliance and breaches. These Regional Offices will consider:

- The size of the breach,
- If there was theft or improper disposal of unencrypted protected health information,
- If there was hacking or unwanted intrusions of protected health information,
- The amount, nature and sensitivity of the protected health information, and/or
- If there were numerous breach reports from the particular Covered Entity or Business Associate.

Likewise, the Regional Offices may consider a lack of reporting for breaches impacting fewer than 500 individuals.[3]

Contact

Cheryl Camin Murray
Shareholder
214.745.5142
cmurray@winstead.com

[1] *See* 45 C.F.R. § 160.103.
[2] *See* HHS, Office for Civil Rights, HIPAA Privacy, Security, and Breach Notification Audit Program at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/.
[3] *See* HHS, Office for Civil Rights, HIPAA Privacy Rule Information Distribution, OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals, August 18, 2016.