The Office of Civil Rights (OCR) recently updated the audit protocol that it will be using to assess Covered Entities’ and Business Associate’s compliance with the Health Insurance Portability and Accountability Act (HIPAA) privacy, security, and breach notification rules. OCR also released a template that Covered Entities and Business Associates may use to keep track of their business associate relationships. The release of the updated audit protocol and Business Associate tracking template is part of the implementation of the Phase 2 HIPAA Compliance Audits.

What Changed?
One of the major changes to the audit protocol is that the OCR distinguished between the portions of the protocol that are applicable to both Covered Entities and Business Associates and the portions that are only applicable to Covered Entities. This should clarify the audit protocol requirements that Business Associates should review as part of their risk assessments and document as part of their policies and procedures.

In addition, the OCR made a number of changes to the types of audit inquiries that are associated with each HIPAA requirement. The audit protocol now contains specific questions that the Covered Entity or Business Associate should assess as part of its risk assessment. The revised protocol also provides more detail about the information that should be included in the Covered Entity's or Business Associate's policies and procedures. For example, 45 C.F.R. § 164.308(a)(3)(ii)(A) requires a Covered Entity or Business Associate to implement a workforce security authorization and/or supervision policy. The updated version of the audit protocol includes a list of elements that may be included in this policy, such as addressing how the entity process access to information systems, how requests for access to ePHI are submitted, and how the entity verifies authorization and/or supervisory approvals. This additional guidance provides concrete examples of issues to consider when drafting policies and procedures, and should help Covered Entities and Business Associates in assessing their current policies and procedures for compliance with HIPAA.

The OCR sample Business Associate tracker contains a list of the specific information the OCR will request from a Covered Entity or Business Associate as part of the Phase 2 HIPAA Compliance Audits. In response to a request from the OCR, Covered Entities and Business Associates should be able to quickly produce the following information for each business associate:

- name of business associate,
- type of service provided,
- contact information for two points of contact at the business associate,
- and the website URL for the business associate.

Covered Entities and Business Associates are not required to use the OCR tracking template. However, Covered Entities and Business Associates should review their Business Associate tracking documents to ensure that they have captured the information that will be requested by OCR as part of an audit.

**What You Should Do Next**

Covered Entities and Business Associates should conduct a risk assessment using the new audit protocol to identify compliance issues and gaps in documentation. In addition, Covered Entities and Business Associates should ensure that their Business Associate tracking system contains the information that OCR will request as part of an audit. Once the audit requests are initiated, entities that are selected for the OCR Phase 2 HIPAA Compliance Audit will only have ten business days to respond to request for documentation, so Covered Entities and Business Associates
will want to ensure that they have sufficient documentation to promptly respond to a request by OCR.

© 2020 Foley & Lardner LLP