OBER | KALER
Attorneys at Law

November 9, 2011

Ober|Kaler Healthcare Information Privacy, Security and Technology Bulletin

James B. Wieland | jbwieland@ober.com

Joshua J. Freemire | jjfreemire@ober.com

OCR Publishes its HIPAA Audit Protocol: Focus to be on Data Gathering and Best Practices

On November 8th, the Office of Civil Rights made public, on a dedicated webpage, details of its HIPAA Audit Program. Section 13411 of the HITECH Act mandated that HHS implement periodic audits to ensure that covered entities are complying with the HIPAA Privacy and Security rules. Earlier this year, HHS made public the fact that KPMG had been selected by HHS to create and implement an Audit Protocol. An initial batch of 20 audits (of the eventual 150 to be completed by December 2012) will begin this month. The audits will cover both HIPAA privacy and HIPAA security compliance.

The announced protocol calls for audits of a wide range of covered entities, but does not identify any specific entities (or specific entity types) that will be identified for audit. As OCR explains,

> Every covered entity and business associate is eligible for an audit. Selections in the initial round will be designed to provide a broad assessment of a complex and diverse health care industry. OCR is responsible for selection of the entities that will be audited. OCR will audit as wide a range of types and sizes of covered entities as possible; covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses may all be considered for an audit.

Although the above notes that “every…business associate is eligible for an audit…” a later statement notes that “business associates will be included in future audits” indicating that OCR will be including only covered entities in this initial group of audits. OCR’s selections will remain private. Audit selections will not be announced, and OCR makes clear that audit findings that could identify the audited entity will not be made public.

As originally announced, OCR intends to complete a total of 150 audits before the end of 2012. Beginning this month, however, OCR will begin its audit program with an initial set of 20 audits. Following these initial audits (which OCR expects to complete by early 2012) OCR intends to revisit, and, as necessary, revise its audit protocol before beginning the remaining 130 audits during 2012.

Entities that have been selected for these initial audits will be notified by letter this month. A sample letter [PDF] is provided on OCR’s website. In this initial letter, OCR will introduce the auditor, explain the audit process, and provide the covered entity with a set of initial document requests relating to the entity’s HIPAA compliance. OCR expects that entities will provide all requested documents and information within ten business days.

At least during these initial 20 audits, every audit will entail a site visit by the audit contractor. Following an initial review of the documents and information provided in response to the audit letter, OCR’s audit contractors will contact the entity being audited to arrange for a site visit. OCR expects that the entity being audited will receive between 30 and 90 days notice before the site visit.

Site visit durations will vary depending on the size and complexity of the entity, but OCR expects that most will take between 3 and 10 days. During the site visit, OCR explains that “auditors will interview key personnel and observe processes and operations to help determine compliance.” OCR’s explanation of the audit process does not provide any further detail what site visits will entail, it is worth noting that interviews of “key personnel” are not specifically limited to personnel who are directly involved in the creation or maintenance of compliance strategies and materials. OCR’s guidance also includes a link to the GAO “yellowbook” containing government auditing standards.

Following the site visit, the OCR’s audit contractor will prepare, and make available to the audited provider, a draft audit report. Final audit reports will generally, according to OCR, “describe how the audit was conducted, what the findings were and what actions the covered entity is taking in response to those findings.” The covered entities “actions” will be added to the report after the entity has had the opportunity to discuss “concerns” identified in the report, and to describe to the auditor corrective actions taken to address those

"concerns." The covered entities response, however, will, like the response to the auditor's initial document request, be expected within ten business days. The final audit report, which will be submitted to OCR, will then contain an explanation of the steps the entity took to resolve any identified problems and identify the entities "best practices." OCR implies that some, but not necessarily all, final audit report findings will be made public; as OCR explains, it will "broadly share best practices gleaned through the audit process and guidance targeted to observed compliance challenges."

OCR's explanation of the protocol takes pains to make clear that the audit process is not intended, at least primarily, as an enforcement tool. As OCR explained,

> Audits are primarily a compliance improvement activity…The aggregated results of the audits will enable OCR to better understand compliance efforts with particular aspects of the HIPAA Rules. Generally, OCR will use the audit reports to determine what types of technical assistance should be developed, and what types of corrective action are most effective.

OCR's explanation also makes clear, however, that OCR will take steps to follow up where "serious compliance issues" are identified. In those instances, OCR explains that it "OCR may initiate a compliance review to address the problem." OCR's explanation also makes it clear that it "expect[s] covered entities to provide the auditors their full cooperation and support and remind[s] them of their cooperation obligations under the HIPAA Enforcement Rule."

Ober|Kaler's Comments

OCR's description of the protocol makes clear that, at least for now, that HIPAA audits will be conducted primarily as a means to identify vulnerabilities common to many provider types and to identify best practices to address those vulnerabilities. Covered entities, however, should do what they can now to ensure that they are prepared to respond in a timely fashion to both the auditor's initial document requests and the auditor's draft findings. In both cases, entities will have only ten days to respond. Early preparation will also ensure that entities are prepared to provide auditors their "full cooperation and support" in a manner that will make any required audit processes proceed as smoothly as possible.

Business associates, which will apparently be targeted at a later stage of the audit process, should take note. Business Associates are "newer to the game" and may not have as robust a HIPAA compliance infrastructure as providers. It is clear that the OCR will pursue clear violations of HIPAA, such as a lack of a comprehensive risk assessment and policies and procedures for physical, administrative and electronic security of ePHI.

About Ober|Kaler

Ober|Kaler is a national law firm that provides integrated regulatory, transaction and litigation services to financial, health care, construction and other business organizations. The firm has more than 130 attorneys in offices in Baltimore, MD, Washington, DC and Falls Church, VA. For more information, visit www.ober.com.