BCLP. Client Intelligent

BenefitsBCLP

HIPAA AUDITS ARE COMING (AGAIN) – ARE YOU READY?

Jul 03, 2014

The Office of Civil Rights ("OCR") of the U.S. Department of Health and Human Services ("HHS") is required to conduct periodic audits of compliance with the Privacy, Security and Breach Notification Rules under the Health Insurance Portability and Accountability Act ("HIPAA").

In Phase I, which closed on December 31, 2012, OCR conducted 115 performance audits. Now, OCR is preparing for Phase II.

To have a broad range of covered entities audited in Phase II, OCR is sending electronic pre-audit surveys to 550-800 eligible entities this summer. The pre-audit surveys are designed to ascertain the size, location, services and best contact information of the covered entities.

OCR is expected to select 350 covered entities for audit (232 health care providers, 109 health plans and 9 health care clearinghouses). Audit notifications and request letters will be mailed to selected covered entities in the fall of 2015.

The Phase II audits will differ from Phase I audits in many respects:

Desk Audits

The actual audits of covered entities will be conducted from October 2014 through June 2015 and for the most part will be internally staffed and involve desk audits. Requested documents must be submitted electronically via email or other electronic media. The data requests from OCR will specify content and file organization, file names and any other document submission requirements. Covered entities will have two weeks to respond. Only requested data submitted on time will be assessed.

Auditors will not contact the covered entity for clarifications or to ask for additional information so it is important that submitted documentation is complete and up-to-date. Failure to submit response to request may result in a referral for regional compliance review.

Narrower Focus

The Phase II audits will be more narrowly focused based on the deficiencies identified in the Phase I audits. The audit protocols for covered entities are projected to be distributed as follows:

- 100 covered entities will be audited on the Privacy Rule with the first round of audits in 2014 focusing on the notice of privacy practices and individuals' access to their own protected health information and shifting in the second round of audits in 2015 to implementation of safeguards and training.
- 100 covered entities will be audited on the Breach Notification Rule with the emphasis on content and timeliness of required notifications.
- 150 covered entities will be audited on the Security Rule with the audits conducted in 2014 focusing on the risk analysis and risk management and possibly shifting in the second round of audits in 2015 to device and media controls and transmission security.

Business Associates

Business Associates will also be audited. Audited covered entities will be asked to identify and provide contact information for their business associates. From this pool, OCR will identify at least 50 business associates (at least 35 IT-related business associates and 15 non-IT related business associates) for audit in 2015.

Steps to Take Now

Although we don't know the specifics of the final data requests, covered entities and business associates should take steps now to review their HIPAA documents so that any deficiencies can be addressed prior to an audit. Plan sponsors should pay particular attention to the targeted audit areas:

- Notice of Privacy Practices. Ensure that the notice has been updated for the 2013 final omnibus rule. Gather documentation evidencing the distribution (and posting on the health plan intranet site, if applicable) of the revised notice.
- Individual Access. Review written policies relating to an individual's right to access his or her own protected health information and ensure that it has been updated for the 2013 final omnibus rule. Gather copies of individual's requests for access and the responses to such requests.
- Safeguards and Training. Review existing safeguards and update as necessary to protect the privacy of protected health information. Gather training materials as well as documentation evidencing the training of workforce members.
- Breach Notification. Review written policies for identifying breaches and providing the required notification to affected individuals, the media and HHS. Ensure that such policies have been

updated for the 2013 final omnibus rule. Gather documentation of any breach assessments, and furnished notifications.

- Security Rule. Obtain copy of most recent risk assessment and corresponding risk management plan. Consider whether circumstances have changed so that conducting a new risk assessment is warranted. Gather copies of the policies relating to device and media controls for equipment and hardware that may contain protected health information and transmission securities (e.g., encryption).

In connection with Phase I, OCR established a comprehensive protocol containing the requirements to be assessed in its performance audits. At last check, the protocol had not yet been updated to reflect the 2013 final omnibus rule but it still offers helpful insight as to the type of documentation OCR is likely to seek in this upcoming round of audits.

While Phase I audits focused on bringing covered entities into compliance, Phase II and future audits are expected to be more focused on enforcement (i.e., imposition of civil monetary penalties or resolution agreements). Thus, the importance of getting your HIPAA documents in order sooner rather than later cannot be overemphasized.
