p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

OCR Begins HIPAA Audits Under the Watchful Eye of Congress

What to Expect and How to Prepare

01.19.2012

Elizabeth H. Johnson

Jessica M. Lewis

In November 2011, as required by the HITECH Act, the Office for Civil Rights (OCR) began auditing selected covered entities' compliance with the privacy and security provisions of HIPAA and its implementing regulations. In the near future, business associates will be eligible for audit selection as well. This article describes the current enforcement climate and provides practical steps on preparing for and responding to a HIPAA compliance audit.

Is it Getting Hot in Here? HIPAA Heats Up

The commencement of these audits is one of a series of changes that are transforming the HIPAA compliance landscape. The last two years have seen the implementation of breach notification requirements, a 60-fold increase in OCR's fining authority, increased enforcement activity with more serious repercussions for enforcement targets and, as noted, the start of OCR's compliance audits. Omnibus regulations implementing the majority of the agency's outstanding HITECH rules is anticipated shortly.

Breach notification has highlighted significant failures to secure health records, with the number of breaches reported increasing by 32% from 2010 to 2011 at an estimated cost to the health care industry of $6.5 billion. The severity of the problem has not gone unnoticed. On November 9, 2011, the Senate Judiciary Committee's Subcommittee on Privacy, Technology, and the Law convened a hearing in which its members chastised OCR for its delay in issuing final rules to implement the HITECH Act and challenged the agency to step up HIPAA enforcement activities.

Despite what appears to the regulated community as substantial enhancement of HIPAA enforcement, the Subcommittee made clear that the agency's efforts fell far short of its expectations, pointing out that, of tens of thousands of HIPAA complaints received by OCR since 2003, the agency has levied only one formal civil monetary penalty and has settled only six other cases for monetary amounts. (Of course, several of these actions reached penalties in the millions, a fact that did not assuage the Subcommittee.)

The Director of OCR, Leon Rodriguez, responded to the criticism by confirming that the agency is no longer required to provide enforcement targets with an opportunity to achieve voluntary compliance, as had been the case prior to the HITECH Act. Rodriguez stated that the agency intends to put its fining authority to good use, stating "the real frontier is in our leveraging these new, stiff penalties that we have under the HITECH statute and expanding our utilization of those penalties" to promote compliance.

The Audit Process

It is in this climate that OCR commences its first compliance audits to assess target

organizations' compliance with the HIPAA Privacy, Breach Notice, and Security Rules. Of the 150 targets to be assessed in 2012, the first 20 have been notified of their selection. The audits will be conducted by OCR's contractor, KPMG LLP, which has assisted the agency in developing an audit protocol to streamline the process. In this pilot phase, the audit program functions as follows:

- OCR will inform the covered entity that it has been selected as an audit target and will request documentation of its privacy and security compliance efforts. The response is due within 10 business days.

- OCR will conduct a site visit over a 3 to 10 day period, interviewing personnel and observing operations. Covered entities are expected to receive 30 to 90 days' notice of the site visit.

- OCR will draft an audit report, describing the audit procedures, the findings, and the actions to be taken by the audit target in response to the findings.

- OCR gives the audit target approximately 10 business days to review the draft audit report and to provide written comments to OCR regarding concerns and corrective actions in response to the draft audit report.

- OCR finalizes the audit report within 30 business days after receipt of the audit target's response.

- If “serious compliance issues” are identified, OCR may initiate a formal compliance review. Compliance reviews can result in a formal corrective action plan and/or monetary penalties.

Preparing for and Responding to an Audit

Preparing for an audit is critical to success given the short time frame, particularly the 10-day period in which to respond to the document request. The following considerations should be evaluated immediately:

- **Documentation:** At minimum, covered entities and business associates must have all policies and procedures required by the HIPAA Privacy, Breach Notice, and Security Rules finalized and regulator-ready. If your privacy function “owns” privacy policies and your IT function owns security policies, bring those groups together now to develop a comprehensive list of all relevant policies so they can be produced quickly. Consider other documentation that supports your compliance efforts. Are your logs of disclosures and security breaches in good order? Can you readily produce documentation supporting role based access, systems activity review, business associate contracting, training and other matters covered by the HIPAA rules?

- **Subject Matter Experts:** OCR will expect you to know which individuals in your organization can speak to each aspect of HIPAA implementation. Do you know who handles access requests? Who reviews access rights periodically to ensure they are correct? Who

monitors system activity? What activities are logged in your systems? Who is responsible for getting appropriate contracts in place with your business associates? Who handles privacy complaints? Find these people now and ask them the kinds of questions OCR might pose.

- **Site Visits:** If you are selected for an audit, assume there will be a site visit. OCR has determined that all 150 audits in this pilot phase will result in an onsite audit. Do not wait for the agency's notice of its visit to prepare.

- **Risk Analysis**: The Security Rule requires that covered entities periodically conduct a comprehensive, formal risk analysis. OCR recently released guidance on conducting such an analysis. The results of that analysis will be among the documents the agency can (and is very likely to) request for review. If you have not conducted a risk analysis in the last 12 months, do so now. Upon completion, evaluate the results and determine how best to mitigate or manage each risk identified (an activity also required by the Security Rule). Document the entire process.

- **Breach Notice and Incident Response:** By now your organization should have implemented a written incident response plan that reflects the requirements of both the Breach Notice Rule and the Security Rule. Ideally, your organization will also conduct a trial run of its response plan and adjust the procedure as needed in light of results.

- **Evaluate Compliance:** Your organization is required to periodically evaluate the effectiveness of its compliance program, including to accommodate the recent legal changes brought about by the HITECH Act and implementing regulations.

- **Training:** If you have not consistently or recently trained employees, now is a good time for a refresher. Maintain documentation evidencing that every relevant employee has been trained.

- **Business Associates:** If you have not identified all of your vendors that handle protected health information, now is an excellent time to do so. Negotiate business associate agreements with all such vendors.

- **Timely Response:** Make sure that the appropriate people will timely receive OCR's written notice of its intent to audit. Do not let it sit in someone's inbox while they are on vacation for a week, cutting your response time in half.

- **Influencing the Audit Report:** The agency provides covered entities with an opportunity to respond to the draft audit report. In our experience working with HIPAA assessors, they will be very responsive to constructive feedback, including presentation of new facts, legal arguments regarding the scope and application of the rules, and justification of your approach to implementation based on the unique

position of your organization. When you receive the draft audit report, formulate a response to any findings that you believe were unfair or inaccurate.

- **Next Steps:** Once the audit is over, be sure to take any compliance steps the agency has mandated, and seriously consider taking any it has suggested. Failure to demonstrate reasonable progress on the audit findings, particularly if brought to light by a reportable security breach, will almost certainly result in swift enforcement action by the agency.

Whether or not your organization is ever selected for an audit, the preparatory steps described above will enhance your organization's compliance posture. In a time when fines surpass the million dollar mark and a security breach lurks around every corner, undertaking that work will pay dividends even if your organization avoids an audit. Of course if you do find yourself among the lucky first 150 audit targets, you'll certainly be glad you took the time to prepare in advance.