Health Law Alert: HIPAA Enforcement on the Rise, As OCR Audit Program Moves Forward

May 20, 2014

A recent settlement from New York—involving the largest fine levied to date in the history of HIPAA enforcement, a staggering $4.8 million imposed on two public hospitals—should remind health care providers, health plans and the many business associates that work with these covered entities that the Office for Civil Rights ("OCR") is continuing to aggressively police HIPAA violations. At the same time, OCR is moving forward with its HIPAA audit program, mandated by the 2009 HITECH law, and will be proactively reviewing compliance by both covered entities and business associates.

Lessons from New York

The New York matter arose when two hospitals (separate covered entities that share a data network that is linked to their respective systems) reported a breach to OCR involving the electronic protected health information ("PHI") of 6,800 patients. Apparently, the breach arose when a physician at one of the hospitals tried to deactivate his own personal computer. This computer was linked to the shared electronic health records system used by the two hospitals. According to OCR, deficiencies in the steps taken by the hospitals to address their HIPAA Security Rule compliance—specifically concerning the technical safeguards used by the hospitals—resulted in the PHI being available on the Internet. Because of this lapse, a simple search through Google or another online search engine would lead the searcher to uncover PHI. The PHI appears to have been fairly detailed and included things like lists of the medications taken by patients; clinical lab results; and information related to patient vital signs and status at the hospital.

In the fall of 2010, the hospitals received a complaint from the partner of a deceased patient whose PHI was found on the web. After learning of this problem, the hospitals reported a breach to OCR in accordance with HIPAA's breach notification regulations. The hospitals also notified the affected individuals as well as media outlets.

OCR looked into the matter and uncovered a number of issues at the hospitals. Among the conduct OCR determined to have occurred:

- The hospitals failed to conduct an accurate and through risk analysis that incorporated all information technology equipment, applications and data systems;
- The hospitals failed to establish and maintain processes for assessing and monitoring IT equipment, applications and data systems and further failed to implement security measures to reduce risks and vulnerabilities to a reasonable level;
- The hospitals did not have in place appropriate policies and procedures for authorizing access to patient data bases; and
- The hospitals failed to comply with their own policies on information access management.

In addition to the $4.8 million fine, the covered entities were required to enter into a detailed corrective action plan that included undertaking a new risk analysis, developing a new risk management plan, revising policies and procedures (on a number of specific topics, such as mobile devices and information access management), training staff and providing ongoing progress reports to OCR.

HIPAA Audits: Ready or Not, Here they Come.

One of the major changes to HIPAA that resulted from HITECH was the creation of a new "HIPAA audit" program at OCR. Readers may remember that "pilot" audits—conducted by KPMG under contract with HHS—already took place in 2012. Those audits involved reviews of HIPAA compliance at 115 covered entities.

The new program is intended to be permanent. The audits will focus on specific areas of HIPAA compliance and will be conducted by OCR personnel (as opposed to KPMG as in the pilot program). OCR is currently in the process of determining which covered entities and business associates it will audit. 1200 organizations (800 covered entities and 400 business associates) have, or soon will, receive "pre-audit surveys" from OCR. These surveys are intended to gather information about recipients so that OCR can assess the size, complexity and fitness of the recipient for an audit. It appears that the business associates who are candidates for auditing will be chosen based on the lists of vendors that the surveyed covered entities produce to OCR. Of the total number of organizations surveyed, it appears that about 350 covered entities and 50 business associates will go through the full audit.

The audits themselves will be divided up into "desk" audits (where OCR personnel review materials provided by the covered entity or business associate) as well as "on-site" audits. After being notified that they are the subject of an audit, it appears that organizations will have about two weeks to produce the materials requested to OCR. Audit results can of course lead to enforcement actions against the covered entity or business associate, if OCR determines that to be an appropriate step.

Next Steps

So what can organizations to do address to their own potential exposure under HIPAA? Here are a few simple steps that covered entities and business associates alike should consider:

- OCR has repeatedly stressed the importance of complying with HIPAA Security Rule. The agency recently issued an extremely comprehensive "Security Risk Assessment Tool" that allows covered entities and business associates to evaluate their own compliance with the Security Rule in light of HIPAA standards. While a bit lengthy, the Risk Assessment Tool offers valuable insight into how OCR might view an organization's compliance and is a handy way to walk through the highly detailed and technical administrative, technical and physical safeguards required under the Security Rule. You can find the Tool here: http://www.healthit.gov/providers-professionals/security-risk-assessment
- As noted above, audit recipients will have a very short time frame (2 weeks) to produce materials to OCR. An organization that has not updated its internal policies, procedures and other compliance materials may need to scramble to get things in the proper shape before producing to OCR. Much stress and anxiety can be avoided by making sure things are up-to-date ahead of time, particularly in light of the numerous changes to HIPAA under the 2013 "omnibus" rule.
- OCR has also created a very helpful "audit program protocol" that organizations can use to understand what an audit might look like. This documents helps parties understand, for example, the kinds of things that might OCR consider in evaluating compliance with HIPAA's "minimum necessary" rule. The audit protocol sheds light on this and many other important questions. The protocol can be found here: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
- If you are a business associate, a lot of this may still be new or a bit overwhelming. While covered entities have been directly regulated by HIPAA since 2003, business associates have only found themselves recently directly subject to HIPAA requirements. If you have not yet done so, it would be a very good time to review what your organization is doing to comply with the Security Rule and the portions of the Privacy Rule that apply to business associates.

Need More Information?

Please contact Jesse Berg at jesse.berg@lathropgpm.com or Tim Johnson at timothy.johnson@lathropgpm.com if you would like to discuss any of this in more detail. In addition, please join Gray Plant Mooty's Health Law team at our annual Health Law Conference on July 17 at The Depot in Minneapolis.