Health Law Alert: HIPAA Business Associates Take Note - Recent Enforcement Actions, HIPAA Audits Urge Compliance

September 29, 2016

Two recent enforcement actions of the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") emphasize the importance of proactive HIPAA compliance—both for health care providers and their business associates. With a $650,000 settlement agreement from earlier this summer, OCR stresses that covered entities and business associates must train workforce members and continually reevaluate policies and procedures addressing topics such as the security of mobile devices and encryption. And with a $400,000 settlement announced at the end of September, OCR underscores the need for covered entities to make sure that their business associate agreements have been updated to address Privacy and Security Rule requirements mandated under the Health Information Technology for Economic and Clinical Health ("HITECH") Act. As is often the case, both of these settlements arose after a covered entity reported a breach of protected health information ("PHI") to OCR.

I. Recent HIPAA Enforcement Actions Focus on Business Associates

In June 2016, OCR announced an important $650,000 settlement agreement with Catholic Health Care Services of the Archdiocese of Philadelphia ("CHCS"). CHCS was a business associate to six nursing homes. OCR learned of trouble in 2014 when each of CHCS's nursing homes was required to report a breach of unsecured PHI under HIPAA's breach notification rules. The breach involved theft of an iPhone from a CHCS workforce member. The iPhone was unencrypted and was not password protected. The iPhone contained extensive information including names, addresses, social security numbers, and information regarding medical treatment of patients and residents. OCR concluded that 412 individuals were affected.

At the time of the incident, CHCS did not have a policy regarding removal of mobile devices containing PHI from its facility. According to OCR, CHCS failed to comply with the HIPAA Security Rule by neglecting to conduct an accurate and thorough assessment of the risks to the confidentiality of PHI. In addition, CHCS failed to implement appropriate security measures to reduce risks and vulnerabilities and failed to have a security-incident-response plan.

In addition to the $650,000 settlement, OCR obtained CHCS's agreement to a Corrective Action Plan ("CAP") that keeps CHCS squarely under OCR's eye. The CAP requires CHCS to provide its HIPAA policies and a host of other information to OCR. If OCR determines CHCS to be in breach of the CAP, OCR can revoke the settlement agreement and pursue further enforcement action, including civil monetary penalties.

The CAP provides helpful guidance for all business associates and covered entities. The HIPAA Security Rule requires covered entities and business associates to develop and maintain written policies and procedures. Consistent with that requirement, the CAP directs CHCS to implement policies related to the following:

- Encryption of ePHI;
- Password management;
- Security incident response;
- Mobile device controls;
- Information system review, security reminders, log-in monitoring and automatic log off;
- Data backup, disaster recovery and emergency mode operation plans;
- Applications and data criticality analysis; and
- Audit and integrity controls.

In addition, the CAP directs CHCS to train its workforce members on its HIPAA policies as required by HIPAA. CHCS must train all of its workforce members that have access to PHI within 60 days of signing the CAP. The CAP requires CHCS to document this training and provide the documentation to OCR.

II. Covered Entity's Failure to Update Business Associate Agreements Leads to $450,000 Settlement

Another recent enforcement action highlights the need for covered entities to make sure that their business associate agreements have been updated to comply with HITECH requirements. In late 2012, Woman & Infants Hospital of Rhode Island ("WIH") reported a breach of PHI to OCR. The breach involved the loss of unencrypted software backups that included PHI of over 14,000 patients. During the course of its investigation into the breach, OCR learned that WIH had permitted a business associate to create and maintain PHI on its behalf under a business associate agreement that had not been updated to address the 2009 HITECH and the subsequent HIPAA "omnibus" regulations that were released in January 2013. For example, the business associate agreement at issue did not require the business associate to comply with the requirements of the HIPAA Security Rule. In addition to the $450,000 payment, the hospital was required to enter into a CAP with OCR (and to pay another $150,000 to the Massachusetts Attorney General to address the underlying breach of PHI that brought the whole matter to OCR's attention).

III. HIPAA Audits Now Include Business Associates

The latest round of HIPAA audits further heightens the need for business associates to focus on compliance. HITECH requires OCR to perform periodic audits to ensure that covered entities and business associates are in compliance with HIPAA. OCR performed a pilot audit program in 2011 and 2012, which at the time only extended to covered entities.

OCR recently launched another round of audits, this time extending to both covered entities and business associates. OCR has explained that it will select a range of organizations—large and small—for audit.

If selected, auditees must provide OCR with their HIPAA privacy, security, and breach policies within *10 days*. OCR uses a helpfully detailed audit protocol (which is available on OCR's website) to determine if the auditees are in compliance.

IV. Key Implications for Covered Entities and Business Associates

a. Ain't No Breach (or Business Associate) Small Enough

OCR's settlement with CHCS is significant because it holds a business associate—as opposed to the covered entity—directly liable. In addition, it indicates the government's willingness to punish HIPAA breaches that directly affect a relatively small number of persons (the CHCS breach affected 412 individuals). The takeaway is that *all* business associates—regardless of their size and the amount of PHI they receive—must take steps to comply with HIPAA.

b. Analyze Risks and Vulnerabilities

In part, OCR faulted CHCS for failing to conduct a thorough risk analysis. Likewise, WIH was penalized because it had not updated its business associate agreements to reflect the 2013 omnibus rule. Covered entities and business associates should consult OCR guidance (including the audit protocol mentioned above) and conduct a meaningful risk assessment. Although each organization is unique, organizations should consider common issues such as theft or loss of laptops and mobile devices. Malicious software and unauthorized access or disclosure may also be risk areas.

c. Implement and Reevaluate Policies

As noted above, OCR directed CHCS and WIH to implement certain policies and revise them as necessary. Covered entities and business associates would be well served to dust off existing policies to make sure they are current. Organizations should not wait until they are stuck with a breach or notice of a HIPAA audit to update these materials.

d. Train Workforce Members

OCR will continue to monitor CHCS's and WIH's obligation to train its workforce members. Lack of training among an organization's workforce creates a significant amount of risk. Covered entities and business associates should document training that meets the standards of the HIPAA Security and Privacy rules. There appears to be little sympathy by regulators for organizations that fail to train their workforce on current standards.

e. Review Business Associate Agreements

Although business associates have been directly subject to many HIPAA requirements since 2013, it is the covered entity's obligation to ensure a business associate agreement is in place. Given the volume of these agreements that exist for most covered entities, it is easy for noncompliant arrangements to slip through the cracks. As demonstrated by the WIH settlement, OCR will penalize covered entities that do not have updated business associate agreements.

Contact Us

If you would like additional information about anything discussed in this Alert, please contact Jesse Berg (612-632-3374 or jesse.berg@lathropgpm.com) or Catie Bitzan Amundsen (612-632-3277 or catherine.amundsen@lathropgpm.com).