Health Law Alert: HITECH Breach Notification Rules, Business Associate Requirements and Increased Penalties for HIPAA Violations Present Challenges for Providers

November 18, 2009

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) made a number of significant changes to HIPAA. Many of the most important changes are already in effect or will become effective in early 2010. On November 5, 2009, Gray Plant Mooty's Health Law practice group held a roundtable focusing on recent developments in HITECH. If you would like a copy of the materials presented at our roundtable, please contact us via the information found at the end of this alert.

Breach Notification Rules

Prior to HITECH, the HIPAA Privacy Rule required a covered entity (CE) only to "mitigate"—without providing much detail as to what that meant—harmful effects known to the CE from an improper release of Protected Health Information (PHI.) HITECH has expanded what a CE must do in the event of the "breach" of the security or privacy of an individual's PHI, requiring both the patient involved, and media outlets in certain cases, to be notified of the breach. HITECH also created requirements that apply directly to a CE's business associates (BA) in the event of such a breach.

The Department of Health and Human Services (HHS) issued regulations explaining these breach notification obligations for CEs and BAs in late August. The regulations became effective on September 24, 2009, though HHS stated that it would not enforce them for an additional six months. In spite of this delay, the regulations are in effect and both CEs and BAs need to move quickly to ensure they have the infrastructure necessary for compliance.

How Do the New Breach Notification Regulations Apply?

The regulations only apply to "unsecured" PHI. PHI that is "secured" is not subject to the regulations, which means that the requirements discussed below do not apply to such secured PHI. For PHI to be secured, it must be either "encrypted" in accordance with standards specified under the HIPAA Security Rule or the media on which the PHI is stored must be destroyed in one of several ways.

PHI that does not meet these standards is "unsecured." The regulations are triggered in the event of a "breach," which means a use or disclosure of PHI that is not permitted under the Privacy Rule. CEs and BAs are thus required to decide whether a release of PHI constitutes a violation of the Privacy Rule. If so, the CE or BA then must decide whether the security or privacy of the patient's PHI has been compromised. To do this, they must engage in a "risk assessment," focusing on specific considerations outlined in the regulations, to decide whether there is a significant risk of harm to the patient. If this harm threshold has been met, and one of several narrow exceptions cannot be satisfied, the notification requirements discussed below must be met. If the risk assessment leads to the conclusion that no significant risk of harm is present, notification is not required. However, it is the CE's or BA's burden to justify their decision, which means that it will be important to ensure a paper trail exists documenting the appropriate analysis in case questions arise in the future.

What Must a Covered Entity or Business Associate Do if a Breach Occurs?

The CE must provide written notification to the affected individuals within a 60-day window of discovering the breach. If a BA learns of a breach, it is required to notify the CE so that the CE can notify the individuals involved. The clock on this 60-day period starts running when the CE, in the exercise of reasonable diligence, should have known of the breach. Notice is imputed to the CE from a variety of parties, such as its employees and its agents, including BAs in some cases. Part of the challenge for CEs will be ensuring that BAs provide timely notification, so that the CE can notify patients within the requisite time period. The manner in which this takes place will likely need to be addressed in BA contracts between the parties.

In addition to notifying affected individuals, if a breach affects more than 500 people, CEs must inform the media about the breach. They are also required to provide notice to HHS, which will publicize the breach on its Web site. For breaches affecting less than 500 people, CEs are required to keep an annual log of any breaches and provide that log to HHS within 60 days of the start of the next calendar year. In spite of the 6-month respite from enforcement, CEs are required to log any breaches that occur during the remainder of 2009 and they will have to provide that log to HHS in early 2010.

Business Associates Directly Regulated Under HIPAA

Business associates have historically had to comply with certain HIPAA requirements solely as a result of their agreements with CEs. If a BA breached its obligations, it would only be liable to the CE under that contract and it would not be subject to direct oversight or penalties by HHS. HITECH has increased the stakes for compliance, however, by directly regulating BAs beginning on February 17, 2010.

As a result of this change, BAs are subject to a host of new obligations. In addition to the breach notification obligations, they are directly subject to parts of the HIPAA Security Rule requiring the use of technical,

physical, and administrative safeguards to ensure the confidentiality of electronic PHI. Understanding the requirements of the Security Rule, what types of safeguards are acceptable and how the safeguards should be implemented, will be a challenge for many BAs. Also, BAs must directly comply with a host of standards found in the Privacy Rule, including using and disclosing PHI only as permitted under the Privacy Rule and blowing the whistle to HHS on a CE if the CE has a practice of violating its obligations under the BA agreement. Meeting these requirements is important because if a BA runs afoul of its new obligations under the Privacy or Security Rule, it can be penalized directly by HHS and other enforcement agencies.

Unfortunately, it is not altogether clear how the new HITECH obligations should be addressed in the contract between CEs and their BAs. The HITECH statute discusses these changes as things that "shall be incorporated" into the BA agreement. Some observers view this as meaning that all BA agreements dating back to 2003 need to be amended to include the new HITECH requirements. Others believe that the new requirements are incorporated as a matter of law into BA contracts. HHS has not clarified exactly what they have in mind. However, with BAs obligated to comply with provisions of the Privacy and Security Rules starting in February, it is worth monitoring any guidance HHS publishes over the next several months to see if this issue is addressed.

Enhanced Enforcement Options and Increased Penalties for Noncompliance

HITECH significantly expanded options for HIPAA enforcement. For example, State Attorneys General have been empowered, since February 2009, to bring civil actions against persons who violate HIPAA if the Attorney General believes the violation threatens state residents. In addition, over the next three years regulations will be issued permitting portions of financial recoveries for HIPAA violations to be paid by HHS directly to individuals harmed by the violation. HHS will also be conducting audits of CEs and BAs to ensure their compliance with the Privacy and Security Rules.

In addition, HITECH increased the penalties against CEs and BAs for violating HIPAA. This happened in several ways. First, HITECH expanded regulators' ability to impose criminal penalties for violating HIPAA. Second, the civil penalties that can be imposed were dramatically increased in amount. For example, while the maximum fine that could be imposed for identical violations in a one year period was $25,000 under the previous rule, HITECH permits fines of up to $1.5 million for identical violations within the same year. The enhanced civil penalties are now linked to the covered entity's level of culpability. Third, HITECH has eliminated certain defenses that could be raised in the past against HIPAA violations. No longer can parties avoid penalties by claiming that they did not have actual or constructive knowledge of the violation. Together with the new obligations discussed above, these enhanced penalties have increased the risks of noncompliance.

Other Notable Points about HITECH

- HITECH has expanded the disclosures for which CEs must maintain an accounting to include disclosures for treatment, payment, and health care operations, if the disclosures for those purposes are made through an electronic health record.
- Providers will be required to agree to an individual's restriction on disclosures of their PHI to a health plan if the disclosure is for payment or health care operations purposes and it pertains solely to services for which the provider involved was paid in full out-of-pocket.
- Significantly less leeway exists for CEs to engage in marketing or fundraising activities.

If you would like further information, or copies of the materials presented at our HITECH Roundtable on November 5, please contact Jesse Berg at 612.632.3374 or jesse.berg@lathropgpm.com, or Tim Johnson at 612.632.3208 or tim.johnson@lathropgpm.com.