Legal Insight

K&L GATES

www.klgates.com

March 2013

Practice Group:

Health Care

HIPAA'S FINAL RULE: Putting Things in Perspective – Comments from OCR

By Patricia Shea

On March 22, 2013, Health and Human Services ("HHS") Office for Civil Rights ("OCR") Director Leon Rodriguez presented the keynote address to attendees of the American Health Lawyers' Association HIPAA/HITECH Conference in Baltimore, Maryland. His presentation focused on the long-awaited regulations officially published on January 25, 2013, that implement the majority of the remaining aspects of the Health Information Technology for Economic and Clinical Health Act passed in 2009 ("HITECH"). These regulations, known as the "Final Rule," modify numerous provisions of HIPAA's existing regulations governing the privacy and security of health information protected by HIPAA (called the "Privacy Rule" and "Security Rule," respectively) as well as finalize the interim regulations governing breaches of unsecured protected health information (the "Breach Notification Rule").

The presentation by Director Rodriguez tempered the vigorous legal commentary that followed the publication of the rules on January 25. While the new rules certainly deserve detailed attention by covered entities and their business associates and subcontractors, Director Rodriguez provided a useful perspective on the value of compliance.

The HIPAA/HITECH Landscape

The Final Rule made several substantial changes to the HIPAA landscape. Perhaps most significantly, the Final Rule expanded the definition of business associate. Previously, a business associate was a person or entity engaged by a covered entity (i.e., health care provider, health plan, or health care clearinghouse) that performed a function on behalf of a covered entity requiring the use or disclosure of protected health information or "PHI". Under the Final Rule, these persons and entities remain business associates, but any subcontractors to which they delegate any of their business associate tasks involving the use or disclosure of protected health information are also business associates even though these subcontractors do not have any direct relationship with the covered entity. Because HITECH made **all** business associates directly subject to and liable for violations of HIPAA's requirements, the expanded definition put a whole new group of vendors and individuals in OCR's enforcement crosshairs.

The Final Rule also changed the standard for reporting certain breaches of protected health information not secured in a manner specified by the Secretary of HHS (called "unsecured" PHI). Under the interim Breach Notification Rule, notification of a breach was not required if there was no significant threat of reputational, financial, or other harm to the individuals whose information had been breached. The Final Rule eliminates the "harm threshold" analysis and replaces it with a presumption that a breach occurred. As a result, now a breach need not be reported only if it can be shown that there is a low probability that the PHI has been compromised. The Final Rule does not define "compromised" but does include specific factors that must be considered when evaluating whether a low probability of compromised PHI exists. This new standard amounts to essentially

proving a negative and conceivably could make a covered entity or business associate a target for enforcement action because virtually every breach of unsecured PHI would be reportable to OCR.

The combination of the expanded definition of "business associate" and the elimination of the "harm threshold" for breaches of unsecured PHI drew strong reaction from lawyers and privacy and security officers, who feared that the new rules are the precursor to heavy-handed enforcement of an impossible standard. Director Rodriguez did not discount the importance of compliance, but he dispelled to some degree the notion of unfettered administrative action.

The "Show Your Work Method" to Mitigating Fines and Penalties

Don't interpret this potentially good news as suggesting there is nothing more to do or that covered entities and business associates should not be concerned about compliance. It isn't. Compliance with the standards and requirements in the Privacy, Security, and Breach Notification Rules is mandatory. Even a quick look at the cases and resolution agreements posted on OCR's website highlights the potential ramifications for failure to comply. But what it does mean is that OCR takes a straightforward, simple, common-sense approach to investigating, auditing, and enforcing potential noncompliance: **"Show Us Your Work."**

The "Show Us Your Work" method works like this.

OCR recognizes that even in a perfect world (i.e., one where the covered entity or business associate is totally and completely compliant with all of the applicable HIPAA obligations), breaches of unsecured PHI happen and will continue to happen largely because the weak link in the compliance chain is the human element. To put this into perspective, Director Rodriguez stated that only about 7% of the security breaches to date were the result of hacking by sophisticated individuals. In contrast, the vast majority of the security breaches were the result of theft, loss, unauthorized access or disclosure of protected health information **by employees or other workforce members** even though these individuals were trained and knowledgeable about the policies and procedures designed to safeguard that information. He referred to these workforce vulnerabilities as "low tech" and acknowledged that even if an entity meets all standards and best practices for HIPAA compliance, it is impossible to completely eliminate this low tech vulnerability.

What does this mean? Breaches will continue to happen and OCR knows it. The **key** to avoiding costly fines and penalties is to be able to show OCR what was in place to prevent the breach in the first instance, to investigate and mitigate the effects of the breach when it occurred, and to review the HIPAA compliance program generally as a result of the breach to prevent it from recurring. The only way to be able to establish this is to **document everything.** "Everything" includes the policies and procedures that were in place at the time of the breach and that were designed to prevent it from occurring in the first instance; documentation that workforce members received training on the policies and procedures; the report and subsequent investigation of the breach; mitigating measures taken as well as notifications made; and any re-evaluation and modification to policies and procedures made as a result of the breach and its investigation. If these actions are not documented, they are viewed as not happening. Period. End of discussion.

Suggestions for Implementing the "Show Your Work" Method

The Final Rule became effective March 26, 2013 but with a six-month implementation window. Use this six-month time frame to work the compliance problem and critically re-evaluate your compliance program generally. At the same time, make necessary modifications to existing policies and procedures to comply with the Final Rule's new requirements.

Here are some practical suggestions for making HIPAA life simpler:

1. *Take the Privacy and Security Policies and Procedures off the shelf.* Many entities put these policies and procedures in place as far back as 2003 and have never looked back. This is probably a violation in and of itself because the environment changes constantly and covered entities (and now business associates) should be reviewing these policies and procedures and updating them appropriately. Document the review even in the unlikely event no changes are made.

2. *Reassess your risk assessment.* This is the starting point for risk mitigation plans and strategies. It may also be the starting point for OCR's investigation and the basis for enforcement action if (a) there is no risk assessment, or (b) there is a risk assessment, but it has not been maintained so that it is current with the constantly changing environment. Risk assessments must be ongoing. And document everything.

3. *Don't be a "teachable moment."* Director Rodriguez stated that to date, OCR's enforcement actions have been strategic and selected based on the instruction they might offer others regarding the necessity for compliance; OCR has not been "cherry picking" the easy cases. Here are two of the teachable moments Director Rodriguez cited:

    - OCR took enforcement action against a health insurer when 57 unencrypted hard drives containing PHI for over 1 million individuals were stolen from a facility the health insurer had leased. OCR's investigation indicated that the health insurer failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operations changes. The investigation also showed a failure to implement the appropriate physical safeguards by not having adequate facility access controls. The health insurer was fined $1.5 million and was required to enter into a corrective action plan to address the cited deficiencies.
    - OCR took enforcement action against a state agency overseeing health programs based on the results of an investigation which began as a result of a breach report of a stolen electronic storage device containing PHI from an employee's car. The subsequent investigation revealed that the agency did not have required policies and procedures in place to safeguard the information and had not completed a risk analysis. Additionally, the agency failed to implement sufficient risk management measures, complete security training for its workforce members, implement device or media controls, or address device and media encryption as required by the Security Rule. The agency was fined $1.7 million and was required to enter into a corrective action plan to address the cited deficiencies.

    Had the above entities made a good faith effort to comply with HIPAA's requirements and still suffered the breach, the enforcement action might not have been so severe. Regardless, the goal should be to avoid being a teachable moment, and the best way to avoid that is to make a good

faith effort to comply with HIPAA's requirements. And, of course, document these good faith efforts.

4. *Take decisive action when a breach occurs.* According to Director Rodriguez, doing nothing "drives enforcement." So when breaches occur, be prepared. Have a plan to respond and specify the time frames associated with that response. And fix the piece of the HIPAA puzzle that failed – whether that is retraining employees or implementing a new protocol. And document everything.

Putting It All Together

It is important to remember that HIPAA compliance is not once-and-done. It has a life cycle that does not end unless and until a covered entity or business associate no longer creates, receives, maintains or transmits protected health information. Compliance is a mindset and method of operation. Each time a violation of a policy or procedure or a breach occurs, the compliance program should be reviewed and strengthened to address the vulnerability. Nothing is perfect so this constant monitoring and evaluation will be ongoing. But the good news is that if a good faith effort to comply has been made and the entity can "Show Its Work," when bad things like breaches happen, the enforcement consequences should be less onerous.

Author:

Patricia C. Shea
patricia.shea@klgates.com
+1.503.226.5726