Adapting BA Practices to Meet the Omnibus Rule

By Thomas McSteen, JD, CIPP

The 2013 HIPAA Omnibus Rule marks a key milestone for implementation of the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH). One of the most far-reaching impacts of HITECH and the Omnibus Rule is that business associates (BA) and their subcontractors now must comply with HIPAA regulations promulgated by the US Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), including the HIPAA Security Rule and applicable portions of the HIPAA Privacy Rule.

While a BA's compliance obligations with regard to HIPAA were previously governed only by the contractual relationship between a covered entity and a BA, as well as the contractual relationship between a BA and its subcontractors, now the HIPAA regulations can be enforced by OCR directly against both BAs and their subcontractors, and subcontractors' subcontractors, effective September 23, 2013.

The Omnibus Rule is being implemented within a framework of increasing enforcement by OCR. Also, in 2012, OCR completed the first phase of its HITECH auditing program, which focused on covered entities. OCR will begin a new phase of auditing after October 1, 2013 that will likely include BAs. Given this context, BAs must understand what these changes mean to their business, and take steps to ensure they are compliant with the newly updated HIPAA regulations and other provisions of the Omnibus Rule. Medical device company Medtronic, a business associate of multiple healthcare facilities, took the following steps to reach compliance with the new rules.

BAs Now Covered Under HIPAA

HIPAA regulations apply directly to Medtronic only for patient data collected in Medtronic's role as a covered entity or a BA. Medtronic's diabetes management business is a covered entity under HIPAA, and four Medtronic businesses (cardiac rhythm disease management, neuromodulation, spinal and biologics, and surgical technologies) provide services that create BA relationships with healthcare facilities and practitioners. For clarity, these relationships do not make the entire business unit a BA—only the specific services that are performed on behalf of a covered entity.

There also are situations in which Medtronic receives patient information from a covered entity that do not give rise to a BA relationship. For example, Medtronic receives patient information via the HIPAA public health exception so that the company may track and report on its Food and Drug Administration (FDA)-regulated devices. Also, Medtronic field representatives have access to patient information when providing technical support to healthcare practitioners because they often are present during surgeries. For these and other scenarios, Medtronic is careful to not enter into a BA relationship with a covered entity.

While these legal distinctions are important, Medtronic's global privacy and security program is designed to safeguard all patient data. Practically, this means that Medtronic safeguards and protects all data on US patients that it collects, receives, accesses, uses, maintains, discloses, and destroys—consistent with corporate policies and standards—even when the HIPAA regulations do not directly govern certain patient data.

Other BA Role Changes

The Omnibus Rule changed several things for Medtronic as a BA. The following are areas of Medtronic's US privacy and security program that were adapted in 2013 to better comply with the new requirements—documentation, partnerships, and incident management and breach notification requirements.

Documentation

The fact that OCR can now knock on Medtronic's door and conduct an audit requires that the organization update its compliance documentation, even if it doesn't need to implement any specific changes in how it protects and safeguards patient data. For example, while Medtronic may have implemented certain security controls, the company will need an updated security risk assessment for each BA function, which will serve as the foundation for whether and how to implement a certain security control. Medtronic also is a covered entity for its employee health plan. Compliance documentation for Medtronic and all BAs must include:

- Security risk assessment—As OCR has shown through both enforcement actions and audit findings, security risk assessments are required. Lack of a documented risk assessment in each BA role would result in a finding, if audited.
- Permissible uses and disclosures, minimum necessary rule—While Medtronic is already required per its business associate agreements to meet these standards, these are two examples of HIPAA Privacy Rule requirements that will be re-evaluated to validate compliance at the same time a security risk assessment is completed.
- Security training—Medtronic's regular privacy and security training will be augmented by targeted training for BA functions.
- Policies and procedures—In addition to Medtronic's corporate privacy and security policies, additional policies and procedures may be implemented on a business unit level per the findings of a risk assessment.

For any BA, whether they have a developed compliance program or not, now is the time to conduct risk assessments, confirm one's compliance documentation, and prepare for the possibility of an OCR audit.

Partnerships

With over 5,000 BA relationships with covered entities, Medtronic has engaged in continued conversations with healthcare facilities about its data privacy and security program. Medtronic is experiencing more oversight from its covered entity customers—and in turn, Medtronic will be exercising more oversight over its vendors who are now also covered business associates per the Omnibus Rule. While BA oversight of vendors may already be required by the terms and conditions of BA agreements, it is now a necessary risk management function to ensure vendors are complying with all HIPAA/HITECH regulations.

Covered entities are responsible for executing compliant agreements with its BAs, and BAs must do the same with their subcontractors. Most BA agreements were amended previously to comply with the 2009 HITECH Act, so it may be that many current BA agreements will not need to be amended. In any event, the covered entity must initiate an amendment. Regardless of whether current BA agreements are amended or not, however, BAs must now comply with the HIPAA/HITECH rules. In turn, it's up to a BA to execute a similar BA agreement with its subcontractors that perform services and have access to patient data in support of the BA's services to the covered entity.

Incident Management and Breach Notification Requirements

Every covered entity and BA will likely, at some point, have a privacy or security incident that will constitute a breach under HIPAA/HITECH. So it's critical that every business associate be prepared to respond to such an incident. Further, every healthcare entity needs to integrate applicable state laws into its security incident management program, as these vary and can be stricter than the federal HIPAA laws. As Medtronic works in every state, Medtronic's incident management program must comply with all applicable laws across the United States.

For consistency as well as good customer relationships, Medtronic follows the HIPAA/HITECH standards for breach notification even in its non-HIPAA roles (i.e., field employees working in a technical support role). In these instances, Medtronic clarifies to its healthcare customers that it is reporting as a business partner, even though it is not legally obligated to do so.

The Omnibus Rule changes the standard for breach notification. First, it clarifies that the notification clock starts on the first day that any person, other than the individual committing the breach, knows or should have reasonably known of the compromise to the privacy or security of patient data, even when it is not clear that the incident will meet the definition of a breach.

Once the company becomes aware of the possible breach, the Omnibus Rule sets a new standard for notification. Currently, the regulations require notification when a compromise to the security or privacy of patient information presents significant risk of harm. The Omnibus Rule, effective September 23, presumes that notification is required whenever there is a compromise to the privacy or security of patient data, unless a documented risk assessment supports a conclusion that there is a "low probability" that the data was compromised.

A New BA Playing Field

The adage "nothing has changed, everything has changed" certainly applies to Medtronic's compliance as a BA. While the organization has been focused on compliance as a BA for several years, the stakes are now higher to ensure compliance. In addition to meeting the terms and conditions of BA agreements, Medtronic and its subcontractors that are now BAs must comply with the HIPAA/HITECH rules. All BAs can expect more oversight by covered entity customers as well as direct oversight by OCR. The playing field, and the stakes, have definitely changed.

Thomas McSteen (thomas.m.mcsteen@medtronic.com) is the US privacy and data security officer for Medtronic.

Article citation:
McSteen, Thomas. "Adapting BA Practices to Meet the Omnibus Rule" *Journal of AHIMA* 84, no.9 (September 2013): 56-57.