HIPAA: It's Different for Manufacturers

by Heather L. Humphrey

A few years ago, the Y2K crisis refocused the data world. Suddenly medical device manufacturers saw the inherent risks data brought to the business industry. What began with answering a simple question about date functionality quickly moved to conversations about personal information, its appropriate uses, and potential risks.

Manufacturers experience HIPAA regulations differently than covered entities. They conduct assessments to see whether HIPAA applies, define HIPAA terms to fit within the manufacturer domain, and try to anticipate changing customer requirements. Manufacturers must identify how to communicate best with covered entities and negotiate for the best working relationship, whereas covered entities identify how to communicate HIPAA requirements to their patients, employees, and business associates.

Does HIPAA Even Apply?

Initially manufacturers were unsure how to address HIPAA. There was industry-wide confusion about the final regulations and little guidance from the Department of Health and Human Services. Those manufacturers aware that they received personal health information (PHI) from customers didn't wait for customers to ask, "Are you HIPAA compliant?" Instead, they developed HIPAA programs to:

- Comply with laws and regulations
- Allow manufacturers to continue to receive and process PHI from US customers
- Enable customers to give PHI to manufacturers with the assurance that it would be kept private and secure
- Respect the privacy of any personal information manufacturers come in contact with
- Manage risks associated with a manufacturer collecting and communicating PHI

However, unlike covered entities, manufacturers needed to assess whether HIPAA was even relevant to their businesses. After performing a HIPAA assessment (see "Sample Manufacturer HIPAA Assessment" below), manufacturers could move ahead, implementing a customized HIPAA program.

Sample Manufacturer HIPAA Assessment

- Identify covered entity and business associate components.
- Conduct HIPAA code set vulnerability assessment. Review HIPAA code set document and identify if a waiver is required for a respective business unit.
- Compile training inventory. Compile a list of team members who should take HIPAA training and include anyone from the business unit that interacts with PHI.
- Document data flows. Business units identified as covered components should document how PHI flows in and out.
- Conduct marketing vulnerability assessment. Meet with the marketing department and determine if it uses PHI and track the source of its information (covered components, through a business associate arrangement, or through the Internet).
- Prepare inventory of customers where the manufacturer is the business associate. Identify categories of covered entity customers, locate any existing business associate agreements, and prepare a list of these specific entities.
- Identify entities to which manufacturer discloses PHI. Identify entities that perform services that obtain access to PHI.
- Perform accounting vulnerability assessment and implementation planning. Identify systems that will be affected, and develop a first draft of an implementation plan.

- Perform authorization vulnerability assessment and implementation planning. Develop a plan for administering and tracking authorizations.

Many manufacturers struggled with the term "HIPAA compliant." IT vendors advertised HIPAA-compliant solutions, and covered entities asked manufacturers how and when they would become HIPAA compliant. But for most manufacturers whose objectives were to manufacture and sell products, the term didn't apply. Manufacturers identified as business associates were essentially "enabling" or "supporting" customers' HIPAA compliance. Manufacturers started educating covered entities on what it meant to be a business associate and the responsibility of enabling compliance.

Some manufacturers are called hybrid entities and are defined within the HIPAA regulation as "a single legal entity that is a covered entity whose business activities include both covered and non-covered functions that designates healthcare components." Manufacturers that bill to Medicaid or Medicare would be considered a covered component, where the sales organization would not.

Differentiating Privacy Agreements

Privacy officers at global manufacturers are concerned when covered entities implement the same business associate agreement (BAA) process for all entities—for organizations with large-scale exposure to PHI as well as organizations where employees will have incidental exposure to PHI. Individuals representing manufacturers such as field sales, clinical managers, and product technicians have limited frequency, access, and exposure to PHI.

Difficulties exist with having all organizations and individuals sign the same BAA, which drives inefficiencies in healthcare. If a company doesn't need to have exposure to PHI in order to provide the covered entity a service, then using a confidentiality agreement recognizing requirements for incidental use is a better option.

Another issue arises when a nonhealthcare manufacturer is asked to sign a hospital's BAA, which essentially binds the manufacturer to many of the same HIPAA requirements as the hospital when its sales representative is in and out of the hospital in 15 minutes. A confidentiality agreement recognizing requirements for incidental use is appropriate for these manufacturers.

Some privacy officers recommend covered entities differentiate the agreement process between organizations where employees will have incidental exposure to PHI. Another suggestion is to continue to drive a BAA with specific provisions for accounting and authorizations with organizations where access to PHI is based upon the business associate providing ongoing services on behalf of a covered entity.

Customer Response Plans

Manufacturers dream of a HIPAA czar who will help covered entities create standardized communications that can be used with their business associates. The cause for this dream is that in their pursuit of HIPAA compliance, covered entities send thousands of varied inquiries with various deadlines, inundating manufacturers with HIPAA requests.

Manufacturers want to support customers' HIPAA compliance but don't want to take their eyes off their main purpose of delivering products to customers so covered entities can treat their patients. One manufacturer received more than 300 inquiries from US hospitals, all with different requests, deadlines, and information needs. To respond to these inquiries by the April 2003 deadline, train staff, and notify the organization, the manufacturer had to dedicate many resources, which in turn created more inefficiency.

Business Associates' Business Associates

There could be a never-ending cycle of covered entities and business associates signing BAAs. As business associates, manufacturers share this commonality with covered entities. To a manufacturer, a business associate could be a temporary placement firm, distributor, third-party parts distributor, or product maintenance organization that provides a service on behalf of the business associate.

Clearly, the most important issue is to ensure that downstream business associates agree to the same terms outlined in the agreements with covered entities. Manufacturers can ensure this occurs by using standardized agreements with both covered entities and downstream business associates. For example, if a manufacturer is required to respond to an accounting of disclosures in 10 days, then the downstream business associate should respond in seven days, allowing the manufacturer to meet its deadline.

Super-sized Privacy

Manufacturers have had to create policies and procedures that consider the many requirements of customers and the patchwork of privacy legislation around the world (see "Manufacturer Privacy Programs" below). Although many programs started with HIPAA requirements, if a manufacturer operates around the world, it realistically has had to expand privacy programs to address requirements in the economy of global data.

Some manufacturers created a set of global privacy principles, which offer requirements of the key tenets to privacy such as notice, choice, disclosure, security, enforcement, and dispute resolution. These principles are generic enough to be adopted within the business units operating in foreign countries.

Those manufacturers who built general privacy programs modeled by the principles of the EU-US Safe Harbor Framework had a bit more work to do if they were identified as a business associate under HIPAA. A manufacturer would need to develop new program requirements that include accounting, authorization, marketing practices, business associate agreements, minimum necessary standard, notice, access, and amendment rights for patients.

Manufacturer Privacy Programs

All Manufacturers

- General "privacy of personal information practices"
- Human resources data privacy

Manufacturers Operating Globally

- Human resources data privacy
- EU-US Safe Harbor Framework
- Country-specific data protection directives

Manufacturers Operating in the US

- HIPAA privacy practices—if an identified business associate
- HIPAA product security—if products manage personally identifiable health information within US hospitals
- Graham-Leach-Bliley Act—if providing financial services to consumers
- US state privacy legislation

The Endgame

The bottom line is that manufacturers exist to develop, sell, and distribute products. They know a lot about the healthcare supply chain, operations, and driving efficiencies to get products where they need to be in order for covered entities to treat patients. In order to drive efficiencies with covered entities, manufacturers should:

- Identify the inherent risks and requirements for the types of data classifications (private, secret).
- Develop broad privacy programs if they operate globally (including use of product Web sites) and encompass other requirements than those in the HIPAA regulations.

- Determine if they are a hybrid entity according to HIPAA regulation and identify business associates (distributors, temporary resource firms) to ensure they have the same requirements in place as those required by the covered entity.
- Help customers achieve HIPAA compliance and educate covered entities on what it is like to be a business associate.
- Understand that not all business associates are created equal. Dialogue with a manufacturer's sales and clinical managers for a detailed process flow of hospital visits to clearly understand the PHI touching points before signing a BAA. If an organization will have incidental exposure to PHI, pursue a confidentiality agreement that includes PHI protections.
- If a covered entity is within a larger purchasing organization, recommend that standardized communication be initiated with manufacturers to minimize inefficiencies.
- Ask covered entities how you can work best together in the beginning of a compliance program. Together you will find efficiencies and reduce redundancy across the healthcare system.

Heather L. Humphrey *(heather_l_humphrey@Baxter.com) is the director of compliance for Baxter Healthcare Corporation in Deerfield, IL.*

Article citation:
Humphrey, Heather L. "HIPAA: It's Different for Manufacturers." *Journal of AHIMA* 76, no.2 (Feb 2005): 56-57,64.