advance healthcare NETWORK | ExecutiveInsight

The Omnibus Rule

It's all about relationships and trust

By Rob Rhodes, CPHIMS, CHCIO, CISSP, HCISPP
Posted on: July 28, 2014

Implementing a successful patient privacy program requires a significant commitment. Covered Entities, Business Associates, and subcontractors face severe penalties for breaches, including financial, criminal, and reputational. Covered Entities can maintain compliance by implementing a comprehensive seven-step program to ensure due diligence with their third-party relationships.

To better protect patient privacy, the HIPAA Omnibus Final Rule has changed the obligations and liabilities between Covered Entities and their Business Associates. In the years since HIPAA was passed, many organizations began to look at the Business Associate Agreement process as an exercise in paperwork or an item on their contract checklist that must merely be checked off. The Rule has once again reminded us that the focus and intent of the privacy rule and Business Associate Agreements specifically, is to protect patient privacy, not generate paperwork.

The Omnibus Rule has focused us again on the relationship between Covered Entities and Business Associates and the risk associated with the access or exchange of Protected Health Information (PHI) between them.

To effectively protect the PHI involved in Covered Entity/Business Associate relationships, it is essential to keep the processes and workflow between the two smooth and productive.

A key component to this process is for Covered Entities to have a good understanding of the amount and types of PHI exchanged or accessed and the Business Associates overall privacy and security practices and level of compliance with HIPAA.

In a perfect world, it would be the responsibility of the Business Associate to understand and follow the HIPAA regulations when handling PHI. Business Associates would comply with the regulations and perform risk assessments to understand their shortfalls. Unfortunately, the real world is often quite different.

Today, both the Business Associates and the Covered Entities vary in their understanding and compliance of the HIPAA regulations. Many organizations don't know the maturity level of their Business Associate Agreements, privacy and security programs, specifics of how their third-party vendors operate, or even what information they are accessing. Because of this, Covered Entities often have an inaccurate understanding of the risk to PHI associated with the relationship.

In many cases, administrative personnel in the Covered Entity's organization are managing the Business Associate Agreements and don't often have an understanding of HIPAA or the potential impact of a violation on their organization's reputation.

In my opinion, Covered Entities need to take a closer look at how they manage their relationships with Business Associates. Covered Entities need to understand their Business Associates' compliance with HIPAA, privacy and security maturity levels, exactly how much and what types of PHI is being accessed/exchanged, and ultimately the risk to PHI associated with the existing or proposed relationship.

In the end, it is the responsibility of the Covered Entities to ensure their third-party vendors are conforming to HIPAA standards and effectively protecting the PHI that their patients have entrusted to them.

Key Obligations of the Omnibus Final Rule
Highlights of the Omnibus Final Rule include the expanded definition of Business Associate, a revised breach notification standard, and expanded liability and obligations.

1. Expanded Definition. The Omnibus Rule expands the definition of the Business Associate to include any downstream subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate, even if they have an indirect relationship with a Covered Entity.
2. Revised Breach Notification. The Omnibus Rule eliminates the "significant risk of harm" standard as the threshold for breach notification. Under the previous rule, breaches were not required to be reported unless they posed a "significant risk of reputational, financial, or other harm" to individuals. The new standard presumes that a reportable breach has occurred unless the Covered Entity or Business Associate, through the use of a multi-factor risk assessment, determines that there is a low probability that the PHI has been compromised by the unauthorized use or disclosure.
3. Expanded Liability and Obligation. The Omnibus Rule expands the liability and obligations of Business Associates, such that Business Associates and their subcontractors who have access to PHI are directly liable for compliance with the HIPAA Privacy and Security Rules, and thus may be assessed civil monetary penalties and criminal penalties for violations. Business Associates and their direct subcontractors that access PHI must enter compliant Business Associate Agreements all the way "down the chain" of the information flow. HHS may impose civil monetary penalties up to $1.5 million for all violations of an identical HIPAA requirement in a calendar year.

How Healthcare Organizations Deliver on These Obligations
Fundamentally, healthcare organizations need to change how they manage their relationships with Business Associates. Covered Entities need to understand:

- How their business associates are accessing PHI
- What systems they are accessing
- Who within the associate organization is accessing them
- When the associate conducted a risk assessment
- Whether their Business Associate Agreement is in compliance with the Omnibus Rule
- If a data breach has occurred in the past

Gathering all this information will allow the healthcare organization to take a risk-based approach as a way to manage those Business Associates appropriately.

Seven-Step Plan to Ensure Due Diligence

1. Create a risk matrix that characterizes the Business Associates in terms of data classification, history, and agreement terms.

    - a). Data Classification defines attributes associated with the data the Business Associate has access to, such as sensitivity of the data, repositories, and breach history.

- b). History indicates the level of compliance with the HIPAA Security and Privacy Rules, how they destroy data, encryption, risk management process, breach history, etc.
- c). Terms describe the document status of the agreement including PHI safeguards, notification of disclosures, termination after breach clause, and right to audit clause.

2. Prioritize your Business Associates in terms of risk

3. Determine which vendors require additional evaluation based on the risk matrix.

- a). Send questionnaires to specific vendors.
- b). Spot check the security controls defined on the questionnaire.
- c). Conduct a security assessment with vendors that have high risk.

4. Have the ability to monitor progress, and report findings and deficiencies for further investigation.

5. Make sure you are alerted when users associated with a terminated Business Associate Agreement are identified as accessing PHI.

6. Move away from the harm-based approach that was introduced by the HITECH Act. The Omnibus Rule is risk-based and requires organizations to perform an immediate risk assessment if a breach or suspicious activity occurs.

7. Automate the risk information about your Business Associates using technology.

It's All About Relationships and Trust

Protecting patient trust goes hand-in-hand with delivering high-quality, cost-effective healthcare. Implementing a comprehensive patient privacy program is not just about preventing fines. It is about maintaining the trust and confidence of the patients you serve.

Trust is hard to earn and even harder to rebuild when it is lost. The Omnibus Rule has instituted regulations and obligations to ensure that patient privacy is protected, but it is up to each healthcare provider to embrace and implement change across their organization.

Your patients are depending on you.

Rob Rhodes is the Senior Director of Patient Privacy Solutions at Iatric Systems.