Ensuring Due Dilligence with Business Partners

How Healthcare Organizations Can Assess the Risk of the Exchange and Use of Protected Health Information

Executive Overview

The regulatory landscape in healthcare has become increasingly complex, and the culture has shifted from one of compliance to one of enforcement. With the HIPAA Omnibus Final Rule and OCR enforcement, hospitals face new obligations regarding business associate agreements and Protected Health Information (PHI). Hospitals, business associates, and their subcontractors face severe penalties for breaches, including financial, criminal, and reputational. Thus it is essential that organizations have the proper technology and procedures in place to ensure that sharing information with Business Associates doesn't put PHI at risk. However, many healthcare organizations have yet to comply.

This paper describes the steps that healthcare providers can take to demonstrate due diligence with third party relationships and ensure they and their business associates are in compliance with the Omnibus Final Rule. Fortunately, technology is available to automate the process and to make it easier to assess the risk when exchanging and using PHI.

The Omnibus Final Rule: Who Has to Comply?

Covered entities: Any healthcare provider, health plan, or healthcare clearinghouse that transmits any information in an electronic form in connection with transactions for which HHS has adopted a standard. For example, hospitals, academic medical centers, physicians, pharmacies, and other healthcare providers who electronically transmit claims transaction information directly or through an intermediary to a health plan are covered entities. Covered entities can be institutions, organizations, or individuals.

Business Associates: Any vendor that creates, receives, maintains, or transmits PHI on behalf of a covered entity.

Subcontractors: An entity to which a business associate delegates a function, activity, or service, other than as a member of the business associate's workforce. There is no limit to the number of subcontractors that may be liable, because a subcontractor might delegate functions to other subcontractors, creating a chain of business associate entities.

The Omnibus Final Rule: What's it all about?

To better protect patient privacy, the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule made substantial changes to the obligations and liabilities between hospitals and their business associates. Every covered entity, business associate, or subcontractor needs to comply with HIPAA whenever they create, receive, maintain, or transmit PHI data. The Final Rule also includes a requirement to comply with patient requests to restrict disclosure of PHI to a health plan if they pay for a health service in full.

Many of the rule's stipulations dramatically affect how all of these organizations handle risk management and breach notification. If a hospital or other covered entity fails to conduct an adequate risk assessment and assure it can monitor business associates, it puts the organization at risk of a breach — and ultimately a charge of "willful-neglect," with a maximum penalty of $1.5 million per violation.

The basic principle behind the HIPAA Omnibus Rule is about doing everything possible to protect patient privacy while building a trusted relationship with business associates. In a perfect world, you could depend on business associates to understand and follow the HIPAA regulations when handling PHI. You could trust them to comply with the regulations and perform risk assessments to understand their shortfalls. Unfortunately, the real world is quite different.

Thus it becomes the covered entity's responsibility to educate and put in place the proper policies and procedures to make sure that business associates are doing everything to protect patient privacy, and that they take HIPAA and the Omnibus Rule very seriously. The challenge, when putting these tighter controls in place, is how to keep the processes and workflow between the covered entity and its business associates smooth and productive while managing the risks associated with access to PHI.

...Omnibus Rule is about doing everything possible to protect patient privacy.

IATRIC systems

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 business associate to include any downstream subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate, even if they only have an indirect relationship with a covered entity. Hospitals and other covered entities also need to consider whether any current vendors have become business associates in light of the expanded definition, thus requiring execution of a business associate agreement.

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.

What Healthcare Organizations Need to Do to Comply with the Omnibus Rule

Healthcare organizations need to take a closer look at how they manage their relationship with business partners in order to understand the risk involved and how to reduce it. Most hospitals don't know the specifics of how their third-party vendors operate or what information they are accessing. Administrative personnel are often responsible for managing business associate agreements, and they usually don't have an understanding of HIPAA or the potential impact of a violation to their organization's reputation. That needs to change.

If a covered entity engages a business associate to help carry out its healthcare activities and functions, the covered entity must have a written contract or other written agreement with the business associate that establishes specifically what the business associate has been engaged to do. The agreement also has to require the business associate to comply with the Omnibus Rule's requirements to protect the privacy and security of PHI.

Fundamentally, healthcare organizations need to change how they manage their relationships with business partners. They need to understand how their 3rd party vendors are accessing PHI, what systems they are accessing, and who within the associate organization is accessing them. They also need to know when (or if) to conduct a risk assessment, whether their business associate agreement (BAA) is in compliance with the Omnibus Rule, and if the business partner has had a data breach in the past. Gathering this information will allow the healthcare organization to take a risk-based approach as a way to manage those vendors appropriately.

Fundamentally, healthcare organizations need to change how they manage their relationships with their vendors.

IATRIC systems

Seven-Step Plan to Ensure Due Diligence

Follow these seven steps to understand and manage your overall risk with your 3rd party vendors relationships and agreements.

1. Assign risk that characterizes vendors 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 business associates destroy data; encryption requirements, risk management process, etc.
   c) Agreement Terms describes the status of the business associate agreement including PHI safeguards, notification of disclosures, terminations after breach clause, and right to audit clause.
2. Prioritize your vendors in terms of assignment of risk. High-risk business associates could be those that don't have a HIPAA training policy or proof of employee training, do not have a HIPAA breach policy, or lack clear policies and procedures regarding the protection of PHI.
3. Determine which vendors require additional evaluation.
   a) Send questionnaires to specific vendors when you need clarification or additional information about their security controls.
   b) Spot check the security controls defined on the questionnaire. (These could include facility access controls, device and media controls, access controls, audit controls, etc.)
   c) Conduct a risk assessment with vendors identified as high risk to make sure you have identified all PHI systems that the business associate is accessing and any vulnerabilities they might have. Next, perform a gap analysis of the delta between your policies and procedures and the business associates' to protect patient privacy.
   d) Using the results of the risk assessment and gap analysis, determine which vendors you should audit. From the results of the audit, create an action plan. This documentation, along with the information about the PHI they are accessing should be attached to the business associate agreement and can be used as proof if needed. We recommend using an automated tool for these like Iatric Systems Partner Risk Manager™ solution.
4. Have the ability to monitor progress, and report findings and deficiencies for further investigation.
5. Deny access for users associated with an out-of-date business associate agreement. We suggest an automated tool to manage this, like Iatric Systems SecureRamp solution.
6. Be able to perform an immediate risk assessment if a breach or suspicious activity occurs (which is required by the Omnibus Rule). To determine whether there is a low probability that PHI has been compromised, the covered entity or business associate must conduct a risk assessment that considers, at a minimum, each of the following factors:
   a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
   b) The unauthorized person who used the PHI or to whom the disclosure was made
   c) Whether the PHI was actually acquired or viewed
   d) The extent to which the risk to the PHI has been mitigated
7. Identify technology that can assist you with Steps 1 – 6.

Protected Health Information is not just data — it's the personal history of an individual, and represents a bond of trust between the patient and the covered entity entrusted with their data. A hospital's ability to maintain that trust is vital to its image, reputation, financial success, and longevity. It is not only the 'hard' costs associated with a breach that you need to consider, but also the cost when intangible assets such as trust are compromised.

Healthcare organizations can head off the consequences of a data breach by investing in technology that automates the process, and that makes enforcement of the policies possible.

The New Norm

How do you ensure compliance with the Omnibus Final Rule? You need to understand the risk of your various business partners. You need to define policies that specify who can access PHI and under what circumstances. You need to understand who, when, and how your business associates are accessing PHI. Finally, you need to make sure that those access policies are enforced — and be able to prove it.

Iatric Systems provides a technology solution that automates and simplifies this entire process. It combines two unique Iatric Systems products to provide a unified approach for managing business associate relationships, and protecting patient privacy, recognizing that they are closely intertwined.

Partner Risk Manager™

This easy-to-use application helps hospitals and other healthcare organizations manage their vendors and associated risk. By assessing, monitoring, and documenting the risk of all vendor questionnaires and contracts, and providing alerts whenvendors need updating, Partner Risk Manager helps organizations protect patient privacy and build trust.

Monitor the risk of third-party vendors and agreements, understand those that need to be updated

- Keep you informed of the status of your third-party vendors through risk determination
- Accomplish screening, tracking and cross-department collaboration related to vendors and agreements
- Prepare for OCR audit with complete reporting to document BA oversight
- Simplify vendors' compliance tasks to build better partnerships and a culture of compliance
- Customized pre-contract questionnaires with automated workflow logic
- Customized to evaluate the use of PHI, volume and frequency of data, how data is stored, processed, transmitted, and destroyed and much more

Iatric Systems provides a technology solution that automates and simplifies this entire process.

SecureRamp™

The remote access security solution, SecureRamp™ simplifies vendor and employee remote connectivity by using highly-advanced security measures to ensure secure access to your network and ePHI, while easing the burden on your staff.

Key Capabilities:

- Deny access for partners with out-of-date BAAs
- Multi-factor authentication with each access
- Automated security checks of the remote system (anti-virus up-to-date, activated firewall, encryption etc.)
- All vendors access the network through one managed tunnel
- Automates the management of remote access

The Integrated Solution that Protects PHI
Together, Partner Risk Manager and SecureRamp provide comprehensive, automated partner risk management and PHI protection. When utilizing these solutions together, they share information about associated risk and manage access to ePHI to prevent breaches before they occur.

Here's how it works:

- Partner Risk Manager identifies and manages the risk of your partners. By having all of your partners managed in one solution, SecureRamp is able to check each remote access attempt for an up-to-date BAA.
- SecureRamp is fully capable of being a stand-alone solution, as well.
- Not only will SecureRamp know if the user attempting to access your network is valid, it can block that access if they are no longer authorized with a current BAA

This workflow is just one example of how the Iatric Systems integrated solution helps ensure due diligence with your 3rd party vendors. It's the new streamlined model for risk management, remote access and PHI protection, making vendor relationships easier to manage, improving the security of your remote users, and ensuring compliance with the Omnibus Final Rule.

Ph: 978-805-4100 Fax: 978-805-4101 info@iatric.com