New HIPAA Business Associate Requirements – Get Prepared

Changes were made to the HITECH Act effective March 23, 2013 to greatly improve security of electronic protected health information (ePHI) by reducing the risk of data breaches. A study by Office for Civil Rights (OCR) concluded that 45 percent\(^1\) of healthcare providers and other covered entities had an average of five HIPAA data breaches in a single year and two-thirds of data breaches involved a business associate\(^2\).

OCR audits will begin September 23, 2013 for both providers and vendors designated as business associates. HIPAA data breach fines will increase to $1.5M for second offence.

Overall impact of HITECH Act revisions concerning business associates

- Universe of vendors defined as business associates will be greatly expanded
  - Upwards to over 1,000 business associates for average health system
- Level of oversight and work required of both business associate-vendor and healthcare providers significantly increases:
  - Determining who qualifies under the new provision
  - Revising of contract terms
  - Establishing business associate agreements
  - Ongoing oversight with audits of business associate-vendors’ processes and documents

To be in compliance with the HITECH Act revisions of 2013, business associate management must be done at the entity level and will require more documentation and oversight.

Vendormate Can Help

Vendormate’s focus is to help healthcare providers and vendors solve their relationship challenges when it comes to regulatory and policy compliance. We provide a procurement cycle management platform to facilitate sourcing, contract workflow and archiving, vendor credentialing and onboarding, vendor entity performance management, and overall risk management.

In tackling new BA requirements, it will be important to employ a partner – like Vendormate – with experience capturing and managing vendor entity-level data for 1,900 healthcare providers via our Credential Manager application, which is integrated with our Contract Manager solution.

Utilizing Vendormate Contract Manager, healthcare organizations can:
- Easily centralize, exchange, track and report on BAAs and other HIPAA-required documentation.
- Conduct oversight of BAs and satisfactory assurances – using data filtering and reporting features to ensure audit readiness.

Vendormate will continue to expand its solutions to enable healthcare providers and business associate-vendors solve the challenges of HITECH Act requirements as part of hospital-vendor relationship management.
More Information on the Changes and Impacts\(^3\)

**Impacted entities:** Healthcare providers and healthcare plans, clearing houses and business associates and their subcontractors.

**Compliance date:** September 23, 2013, unless the business associate agreement and agreement between business associate and subcontractor was established prior to January 25, 2013. In these cases, compliance is delayed until September 22, 2014 or the date the contract is renewed or modified, whichever occurs first.

**Critical changes with the new rule include:**
- Tighter controls on Authorization to Releases of Patient Information and Notice of Privacy Rights
- More limits on the use of patient information for marketing and fundraising
- Broadened definition for Breach of Patient Information and enhanced penalties
- Updated and modified business associate agreements
- Mandate that subcontractors of business associates must be brought into compliance with HIPAA

**Definition of business associate expanded to include:**
1. **Subcontractors:** Create, receive, maintain or transmit protected health information (PHI) on behalf of business associates.
2. **Entities Providing Data Transmission Services:** Requiring access to PHI on a routine basis.
3. **Document and Data Storage Organizations:** Maintain PHI regardless of whether the entity actually accesses it.
4. **Personal Health Record Vendors:** Provide and manage personal health records on behalf of covered entities.
5. **Financial Institutions Lending to the Health Care Industry:** Perform functions above and beyond the mere processing of remittance advice.

**Impacts to business associates:**
- Subject to the HIPAA penalties and must comply with the Security Rule and sections of the Privacy Rule, including having a risk assessment and a plan for safeguarding patient information.
- Must ensure subcontractors comply with HIPAA requirements; all requirements and obligations that apply to direct business associates apply to all downstream service providers.
- Must keep documentation on their compliance plan and divulge any breaches with patient information.

**New requirements and liabilities for business associates under the Final Rule:**
The HITECH Act statutorily imposed direct liability on business associates for failure to comply with HIPAA. Business associates may face civil monetary penalties, and in some cases criminal penalties, for failure of them and their agents, including subcontractors, to comply with the following obligations:
- Meet all requirements of the security rule, including administering administrative, physical and technical safeguards, such as:
  - Conducting risk analyses
  - Designating a security official
  - Implementing required security policies and procedures
  - Implementing technical security measures and facility access controls
  - Conducting security awareness and training programs for all staff and management
  - Adopting a contingency plan
• Adhering to the following privacy rule obligations:
  o Limiting uses or disclosures of PHI to only those (i) provided for within their business associate agreement or (ii) permitted or required under HIPAA
  o Limiting permissible disclosures or requests for disclosures to the minimum necessary
  o Providing an accounting of disclosures
  o Providing access to its covered entity or the individual who is the subject of the PHI to the PHI kept in a designated record set
  o Providing PHI to the U.S. Department of Health and Human Services (HHS) to demonstrate compliance during investigations
  o Entering into business associate agreements with subcontractors that comply with the provisions governing business associate agreements between covered entities and business associates.
• Maintain compliance records and submitting reports to HHS required to determine whether a covered entity or business associate is complying with HIPAA.
• Providing a breach notification to its covered entity upon discovering a privacy or security “breach,” as defined under HIPAA, and performing a risk assessment, in accordance with the final rule, when determining whether a breach has occurred.

Appendix

HIPAA: Health and Insurance Portability and Accountability Act definition: The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. (HHS.gov – Health Information Privacy)

The HIPAA Omnibus Rule and why was it created?
• In February 2009, the American Recovery and Reinvestment Act (Stimulus Act) provided incentives for healthcare providers to adopt and implement electronic health records.
• Out of concern for privacy of patient’s electronic health records, the Health Information Technology for Education and Clinical Health Act (HITECH) was created to:
  o Improve the privacy and security requirements for patient information/records and protected health information (PHI)
  o Modify HIPAA to a more stringent level with greater protection and prevention of PHI breach.
  Fine for breach increased from $25K to $1.5M for repeat breach

Business Associate definition: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity’s workforce is not a business associate. (HHS.gov – Health Information Privacy)

Sources:
1. Ponemon Institute: Third Annual Benchmark Study on Patient Privacy & Data Security
2. OCR Breach Statistics