



# HIPAA, HITECH and Business Associates

Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), called the Health Information Technology for Economic and Clinical Health (HITECH) Act, codifies and expands on many of the requirements promulgated by the Department of Health & Human Services (DHHS) pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to protect the privacy and security of protected health information (PHI).

For example, HITECH, for the first time, directly regulates business associates – defined to include persons who, on behalf of a covered entity (but other than as members of the covered entity’s workforce), perform or assist in performing a function or activity that involves the use or disclosure of individually identifiable health information, or that otherwise is regulated by HIPAA. Specifically, as of February 17, 2010, HITECH now will:

- Require business associates to comply directly with Security Rule provisions directing implementation of administrative, physical and technical safeguards for electronic protected health information (e- PHI); and development and enforcement of related policies, procedures, and documentation standards (including designation of a security official).
- Impose on business associates an obligation to directly comply with HIPAA’s business associate safeguards, including limiting use and disclosure of PHI as specified in the agreement or as required by law; facilitating access, amendment and accounting of disclosures; opening books and records to DHHS; and returning or destroying PHI, if feasible, upon contract termination.
- Deem a business associate to violate HIPAA if the business associate knows of a “*pattern of activity or practice*” by a covered entity that breaches their business associate agreement (BAA), but fails to cure the breach, terminate the BAA, or report the non-compliance to DHHS.
- Require DHHS to conduct compliance audits.

## Loricca, Inc.

1118 Nikki View Drive  
Brandon, FL 33511  
Phone: (813) 600-3005  
Fax: (813) 436-5533  
mwhitcomb@loricca.com  
www.loricca.com

## When should a BA (business associate) be compliant?

- 1.** The HITECH Act is effective **NOW** with regard to all the requirements that went into law February 2009. All BAs must be in compliance now with those various requirements, including breach response activities. If they are not in compliance now, then they are currently breaking the law and are at great risk.
- 2.** Additionally, all BAs must currently be in compliance with all their BA Agreement requirements. They should look at them now. Most BA Agreements require written policies, procedures and other safeguards that are explicitly required. Many are similar to the requirements of Covered Entities (CE) under HIPAA. They face sanctions, fines, and loss of their CE clients if they are not in compliance, as well as being vulnerable to civil actions. If they are not in compliance with all the BA Agreement specifications now, then they are breaking their legal obligations and are at great risk.
- 3.** State Attorneys General offices are holding BAs and subcontractors accountable for following the HIPAA requirements now. If they are not in compliance now, then they risk having actions brought by the state AGs in any of the states where they do business.
- 4.** The NPRM expands HIPAA to both BAs and their subcontractors, and the comments closed on September 15, 2010. The NPRM changes could go into effect any day with an announcement from HHS.  
  
HIPAA Covered Entities must comply with the HIPAA Security Rule. In addition, as of February 2010 the bulk of the Security Rule also applies **directly** to Business Associates of a Covered Entity, and will be enforceable against Business Associates by the Department of Health and Human Services (HHS).

## *Business Associates Agreements (BAA)*

The HIPAA Security Rule requires Business Associates Agreements to obligate Business Associates to implement administrative, physical and technical safeguards “that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information [EPHI] that it creates, receives, maintains, or transmits” on behalf of a Covered Entity.

Before the HITECH Act, Business Associates were not required to comply with the Security Rule itself, and most Business Associate Agreements did not specify what administrative, physical and technical safeguards Business Associates needed to have in place.

With the passage of the HITECH Act, Business Associates must comply with the Security Rule’s administrative, physical and technical safeguards regulations. The government will therefore have the authority to enforce these provisions of the Security Rule directly against Business Associates, and the same penalties that may be imposed on Covered Entities may be imposed on Business Associates, as well. Covered Entities still are required to obtain Business Associate agreements, even though the regulations are now directly enforceable by HHS.

The HITECH Act now applies certain HIPAA provisions directly to business associates. Formerly, privacy and security requirements were imposed on business associates via contractual agreements with covered entities. We suspect that many small providers do not have the requisite contracts in place. In some cases contracts exist but may not meet all the requirements of the rules.

The HIPAA Security Rule also requires Covered Entities to include a provision in their Business Associate Agreements requiring Business Associates to report any “Security Incidents” of which their Business Associates become aware. A Security Incident is defined as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”

This reporting requirement will include any Security Incident at the Business Associate or any of its downstream contracted entities that handle the Covered Entity’s EPHI. The definition of the term “Security Incident” includes not only actual but attempted unauthorized access to a system.

This Security Incident reporting requirement is broader than the breach reporting requirements introduced more recently in the HITECH Act. As a result, Business Associates are required to report Security Incidents that may not require the Covered Entity to report as a breach under the HITECH Act. Covered Entities and Business Associates should therefore carefully consider these distinctions when a release or other potential Security Incident occurs.

The HIPAA Security Rule requires the Business Associate Agreement to: (1) ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it; and (2) to authorize termination of the contract by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of the agreement. These exact provisions are required by the HIPAA Privacy Rule, as well.

Under the HITECH Act, business associates are now directly "on the compliance hook" since they are required to comply with the safeguards contained in the Security Rule. Most, if not all, software vendors providing EHR systems will clearly qualify as business associates. Requiring vendors to comply directly ensures that more provider/vendor dialog will occur regarding the necessary contracts, and regarding other compliance issues of mutual interest. The vendors themselves will insist on it.

The responsibility for business associates does not stop with Security Rule compliance and contractual agreements. The HITECH Act requires business associates to report security breaches to covered entities consistent with the notification requirements. Also, they are now subject to civil and criminal penalties under HIPAA if certain conditions exist. Business associate requirements need to be reviewed individually and imposed depending on how the relationship with the healthcare provider is defined.

The bottom line is that business associates and providers will share more joint responsibilities than they have previously. Large providers, with the help of counsel and other specialized staff, will not likely be surprised by these changes. However, for many small providers the HITECH Act may be the first real introduction to the business associate relationship concept as another regulatory requirement that requires serious attention.

Recent studies have shown that Business Associates cause 42% of HIPAA HITECH data breaches, and other improper disclosures of PHI are caused by sub-contractors. Proper management of BAs and Subs is something that healthcare providers need to do now.

Your organization may have sufficient information privacy and security measures implemented, but what about your vendors? From your payroll provider to your copy service, from your data hosting provider to your records disposal service, dozens of third parties handle personal information on your behalf, and your information security program is only as good as theirs.

Identifying these service providers and obligating them by contract to implement necessary security measures is mandatory in many states and thus necessary to comply with law. Forty-six state laws and several federal rules require your organization to notify affected individuals of any breach your providers may cause, making appropriate diligence and contracts necessary to avoid costly data breaches and related risks. The Ponemon Institute's 2009 study of data breach costs indicates that 42 percent of the breach incidents studied was caused by third-party mistakes, and the involvement of those third parties increased the cost of the breaches by 12 percent.

Examples of contractor missteps that have caused recent data breaches include:

- Tossing boxes filled with the personal information of tens of thousands of individuals into open dumpsters and recycling bins.
- Publishing login credentials in a brochure and on the Internet for a secure website that contained hundreds of thousands of individuals' personal information.
- Leaving an unencrypted laptop containing personal information of thousands of individuals in a car, from which it was stolen.
- Losing a shipment of computer backup files and unencrypted CDs containing personal information for tens of thousands of individuals.

In all cases, the organizations that hired these contractors were obligated to give notice of the breaches. These incidents typically result in bad press, government enforcement actions, lawsuits, and lost productivity while the organization responds to the breach. The average cost to respond? Over \$6.5 million.

So how do you comply with information security laws and avoid cleaning up a contractor's costly data breach? The most effective solution is to implement a comprehensive privacy and security compliance program that includes vendor management. The first step to vendor management is to actually identify all the contractors that access your data. The next step is to conduct appropriate diligence on their security programs, which can consist of a questionnaire, a conversation, an onsite review — any level of checking is better than doing nothing.

One of the most crucial steps in vendor management is executing a strong contract that is agreed to before the first piece of sensitive data reaches the contractor's hands. A number of states require contracts by law when a service provider will have access to or dispose of personal information. Contractual issues to consider include control of subcontractors a service provider may use; compliance with applicable information privacy and security laws; appropriate security measures such as encryption and system activity review; notice and cooperation in situations involving data breaches; the right to audit the contractor's compliance and security program; and appropriate allocation of responsibility and liability in the event of a breach.

Health law practitioners have developed no clear consensus on the implications of HITECH for BAAs, and many disagree on whether there is any actual mandate to amend existing agreements. Some argue that because HITECH now directly regulates business associates and directly imposes on them the new privacy and security obligations defined in Subtitle D, it is unnecessary to update existing BAAs. Others point out that Sections 13401 and 13404 explicitly mandate that HITECH's new security and privacy provisions be *"incorporated into the business associate agreement."*

In actuality, the need to amend may well depend on the specific language included in existing BAAs and its interpretation by the parties and, ultimately, DHHS. For example, sample BAA language developed by the Office for Civil Rights (OCR) provides: *“The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and [HIPAA].”* While some first-generation BAAs adopted this language wholesale, others provided for automatic amendment or amendment by notice from the covered entity to incorporate any revisions necessary to assure ongoing compliance without the need to re-contract.

Some attorneys argue that even the sample language (*particularly if previously updated to comply with the Security Rule*) adequately addresses any new mandates, as it defines regulatory references to mean those “in effect or as amended” and requires any ambiguity in interpretation of the BAA to be “resolved to permit the Covered Entity to comply” with HIPAA. Given the explicit mandate in HITECH to incorporate its new provisions, the safer approach may well be to amend the agreements.

Additional issues covered entities and business associates should consider in evaluating existing agreements and developing or negotiating new ones include:

- 1. Who is a Business Associate?** Because HITECH imposes direct obligations on business associates and provides for the imposition of civil and criminal penalties on non-compliant business associates, vendors may want to re-evaluate their position. In the past, some vendors who did not believe themselves to be “business associates” as defined in HIPAA willingly signed BAAs because their obligations under those agreements were not, practically speaking, particularly substantial. Others who thought they might be business associates but whose customers failed to ask them to sign BAAs did not press the issue, on the theory that failure to execute a BAA was a compliance problem only for the covered entity. Today, the stakes have changed: a vendor’s acknowledgement that it is a business associate when it is not can unnecessarily expose the vendor to substantial civil and criminal penalties under 42 U.S.C. §§ 1320d-5 and 1320d-6; yet its failure to enter a BAA when one is required would violate HITECH. One way to resolve this is to provide in a scope statement that the BAA applies only if and to the extent the vendor is a business associate to the covered entity (as defined in HIPAA), and that the vendor does not, by signing the BAA, concede it is one.
- 2. Security Guidance.** HITECH requires DHHS to issue annual guidance on *“the most effective and appropriate technical safeguards”* to facilitate compliance with the Security Rule. Also, the law’s breach notification provisions will apply only to breaches of “unsecured” PHI. PHI is deemed unsecured unless rendered *“unusable, unreadable, or indecipherable”* to unauthorized individuals by technologies or methodologies explicitly identified in separate guidance issued by DHHS (and currently limited to encryption or destruction). Covered entities who want their vendors to adopt and maintain what might be considered industry best practices may wish to require those vendors to commit to comply with all relevant security guidance. Business associates *may* be willing to

implement existing guidance, but many are unlikely to want to commit in advance to language that mandates adoption of unspecified standards at unknown cost.

- 3. Accounting for Disclosures.** HITECH permits a covered entity to comply with its accounting responsibilities with respect to electronic health records by providing a complete accounting or by providing an accounting of the covered entity's disclosures and a *"list of all business associates acting on behalf of the covered entity including contact information."* Parties to a BAA may or may not want to specify in advance how the covered entity will respond to future requests for accountings.
- 4. Responsibility for Noncompliance.** Covered entities are directly accountable under HIPAA only for their own conduct and the conduct of their workforces. Yet "workforce" is defined broadly to include *"employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."* This can include temporary employees, outsourced staff, and others who may under federal and state tax and employment laws and service contracts be considered employees of a business associate but nevertheless in some respects are the responsibility of the covered entity. Moreover, many HIPAA standards that apply to a covered entity's direct actions are implicated by a business associate's non-compliance. For example, a covered entity that fails to respond properly to its BA's non-compliance with the Privacy Rule thereby may be deemed to have violated HIPAA. For these reasons, HITECH's enhanced enforcement provisions may cause covered entities to seek broader assurances from BAs (*e.g.*, indemnification) than previously was the case. BAs, by contrast, are likely to seek protection for actions taken at the direction of a covered entity or its employees, and to impose other limits on potential liability to their customers (or third parties) in connection with the underlying arrangements.

Covered entities and business associates alike should work now to develop strategies for eventual compliance with HITECH.

***Michael Whitcomb, PMP, CISM***

Michael is the founder and President of **Loricca, Inc.** He has 25 years of experience building and supporting secure systems for government and commercial organizations of all sizes. Michael brings the technical knowledge and proven leadership ability for Loricca to provide world class security services. Since founding Loricca, Michael has established the company's presence providing security solutions to some of the country's largest companies.

Prior to Loricca, Michael served in technical leadership positions, leading and implementing solutions for various clients within both the government and commercial sectors including finance, healthcare, retail and federal government. Michael holds a Bachelor of Science in Management of Information Systems from the University of Phoenix in addition to the PMP and CISM professional certifications.