

Legislative Brief

HITECH Act: Compliance Steps



The deadline for compliance with the HITECH Act – **February 17, 2010** – is rapidly approaching. Brokers who are HIPAA Business Associates will now have additional responsibilities. This Legislative Brief summarizes the HITECH Act and provides steps that a broker, as a Business Associate, can take to comply with the HITECH Act.

What is the HITECH Act?

The HITECH Act is the Health Information Technology for Economic and Clinical Health Act. It was enacted on February 17, 2009, as part of the American Recovery and Reinvestment Act of 2009 (ARRA). The HITECH Act contains health information technology provisions and also makes significant changes to the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (the HIPAA Privacy and Security Rules).

Many of the HITECH Act provisions apply mainly to Covered Entities, such as health plans. However, under the HITECH Act, Business Associates must now comply with the same HIPAA Security Rule requirements that previously applied only to Covered Entities. Business Associates must also comply with some of the same HIPAA Privacy Rule requirements as well.

Compliance Steps to Take:

- Update Business Associate Agreements.** These agreements must be revised to include any new privacy and security requirements of the HITECH Act. Business Associates may also be responsible for making sure they enter into Business Associate Agreements with appropriate Covered Entities – that was previously up to each Covered Entity – so they should be aware of which relationships might cause them to be considered a Business Associate. Updated agreements should be updated and executed by **February 17, 2010**.
- Monitor Compliance with Business Associate Agreements.** The HITECH Act provides that Business Associates are directly regulated with respect to HIPAA Privacy, in addition to being bound by their Business Associate Agreements. Now, any breach of a Business Associate Agreement (and the related HIPAA Privacy Rules) could result in direct penalties being imposed on the Business Associate. The HITECH Act also requires a Business Associate to take action to cure breaches of its Business Associate Agreement by the applicable Covered Entity.
- Adopt a Breach Notification Policy.** The HITECH Act requires Covered Entities to notify individuals of security breaches involving “unsecured PHI.” If the breach is of unsecured PHI held by a Business Associate, the Business Associate must notify the Covered Entity. Unsecured PHI is PHI that is not encrypted or destroyed. Encryption or destruction is not mandatory, but if a breach occurs, notification is required. The Department of Health and Human Services released an interim rule in August 2009 and will begin enforcing the rule on **February 22, 2010**.

Legislative Brief

HITECH Act: Compliance Steps

- **Implement Safeguards as Required by the HIPAA Security Rule.** The HITECH Act states that Business Associates must implement administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of electronic PHI (ePHI). Previously, this requirement was imposed through the Business Associate Agreement. Now Business Associates must comply with these Security Rule requirements in the same manner as Covered Entities. See the last page of this Legislative Brief for a list of the required safeguards and implementation specifications. These safeguards should be implemented by **February 17, 2010**.

The HIPAA Security Rule requirements are scalable, with some implementation specifications being “required” and others being “addressable” (see additional information below). How each Business Associate implements the requirements may depend on a Business Associate’s size, complexity and capabilities; its technical infrastructure, hardware and software security capabilities; the costs of security measures; and the probability and criticality of potential risks to health information. Note however that they are **not** optional and cost alone is not a justification for failing to implement a procedure.

- **Implement Policies and Procedures to Comply with the HIPAA Security Rule.** As part of the safeguards mentioned above, Business Associates will most likely have to adopt and implement new policies and procedures about how they will protect ePHI.
- **Be Aware of New Limitations Under the Privacy Rule.** These new rules primarily affect Covered Entities, but may impact a Business Associate through the services it provides to Covered Entities:
 - Marketing Restrictions – Business Associates may not use PHI to inform an individual about products or services without the individual’s authorization if the Business Associate receives compensation for making the communication.
 - Minimum Necessary Standard – Covered Entities are required to use or disclose the “minimum necessary” amount of PHI. The HITECH Act requires new regulations to be issued updating the minimum necessary requirement in 2010. Until then, only a limited data set should be used, if possible.
 - Prohibition on Sale of Protected Health Information – Covered Entities and Business Associates may not sell PHI or ePHI unless they receive a valid authorization and statement from the subject of the PHI. There are exceptions to this rule for disclosures for public health, treatment, research purposes or payment to a Business Associate for activities covered by the Business Associate Agreement. New regulations are expected to be issued in 2010.
- **Train Employees on Privacy and Security Policies and Procedures.** This step is especially important if any new policies or procedures are adopted. If current policies and procedures are sufficient for compliance, employees should be given refresher training.

Legislative Brief

HITECH Act: Compliance Steps

What are “Required” Implementation Specifications?

When an implementation specification within the Security Rule is “required”, the Business Associate must meet the implementation specifications.

What are “Addressable” Implementation Specifications?

“Addressable” implementation specifications are **not** optional. Rather, a Business Associate is provided more flexibility in determining how it will comply with an “addressable” implementation specification. If an implementation specification is “addressable”, a Business Associate must do one of the following:

- If an “addressable” implementation specification **is** reasonable and appropriate, then the Business Associate must implement it.
- If an “addressable” implementation specification **is not** appropriate and/or reasonable, then the Business Associate must implement an alternate measure that accomplishes the same result, if reasonable and appropriate.
- If an “addressable” implementation specification **is not** applicable to the situation **and** that standard can be met without implementation of an alternate measure in place of the “addressable” implementation specification, the Business Associate can choose not to implement the “addressable” implementation specification.

In all cases, a Business Associate should document the reasons for each of its decisions and the procedures implemented to comply with the Security Rule.

This Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

(EAS 1/10)

Content copyright © 2009-10 Zywave, Inc. Images copyright © 2000 Getty Images, Inc. All rights reserved.

Legislative Brief

HITECH Act: Compliance Steps

HIPAA Security Rule Compliance Guide

Standards	Sections	Implementation Specifications R= Required A=Addressable
Administrative Safeguards		
Security Management Process – Implement policies and procedures to prevent, detect, contain and correct security violations.	164.308(a)(1)	Risk Analysis (R) - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI.
		Risk Management (R) - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Security Rule general requirements.
		Sanction Policy (R) - Apply appropriate sanctions against work force members who fail to comply with security policies and procedures.
		Information System Activity Review (R) - Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.
Assigned Security Responsibility	164.308(a)(2)	(R) - Identify the security official who is responsible for the development and implementation of security policies and procedures.
Work Force Security – Implement policies and procedures to ensure that all members of its work force have appropriate access to ePHI and to prevent those work force members who do not have access from obtaining access to ePHI.	164.308(a)(3)	Authorization and/or Supervision (A) - Implement procedures for the authorization and/or supervision of work force members who work with ePHI or in locations where it might be accessed.
		Work Force Clearance Procedure (A) - Implement procedures to determine that the access of a work force member to ePHI is appropriate.
		Termination Procedures (A) - Implement procedures for terminating access to ePHI when the employment of a work force member ends.
Information Access Management - Implement policies and procedures for authorizing access to ePHI that are consistent with the Security Rule.	164.308(a)(4)	Isolating Health Care Clearinghouse Functions (R) - If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.
		Access Authorization (A) - Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process or other mechanism.
		Access Establishment and Modification (A) - Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program or

Legislative Brief

HITECH Act: Compliance Steps

		process.
Security Awareness and Training - Implement a security awareness and training program for all members of its work force (including management).	164.308(a)(5)	Security Reminders (A) - Periodic security updates.
		Protection from Malicious Software (A) - Procedures for guarding against, detecting and reporting malicious software.
		Login Monitoring (A) - Procedures for monitoring login attempts and reporting discrepancies.
		Password Management (A) - Procedures for creating, changing and safeguarding passwords.
Security Incident Procedures - Implement policies and procedures to address security incidents.	164.308(a)(6)	Response and Reporting (R) - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents; and document security incidents and their outcomes.
Contingency Plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	164.308(a)(7)	Data Backup Plan (R) - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
		Disaster Recovery Plan (R) - Establish (and implement as needed) procedures to restore any loss of data.
		Emergency Mode Operation Plan (R) - Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
		Testing and Revision Procedures (A) - Implement procedures for periodic testing and revision of contingency plans.
Applications and Data Criticality Analysis (A) - Assess the relative criticality of specific applications and data in support of other contingency plan components.		
Evaluation	164.308(a)(8)	(R) - Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the Security Rule's requirements.
Business Associate Contracts & Other Arrangements - A covered entity may permit a business associate to create, receive, maintain or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.	164.308(b)(1)	Written Contract or Other Arrangement (R) - Document the satisfactory assurances through a written contract or other arrangement with the business associate.

Legislative Brief

HITECH Act: Compliance Steps

Physical Safeguards		
Facilities Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	164.310(a)(1)	Contingency Operations (A) - Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		Facility Security Plan (A) - Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		Access Control and Validation Procedures (A) - Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		Maintenance Records (A) - Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).
Workstation Use	164.310(b)	(R) - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.
Workstation Security	164.310(c)	(R) - Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.
Device and Media Controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	164.310(d)(1)	Disposal (R) - Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.
		Media Reuse (R) - Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.
		Accountability (A) - Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
		Data Backup and Storage (A) - Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.
Technical Safeguards		
Access Control - Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.	164.312(a)(1)	Unique User Identification (R) - Assign a unique name and/or number for identifying and tracking user identity.
		Emergency Access Procedure (R) - Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
		Automatic Logoff (A) - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Legislative Brief

HITECH Act: Compliance Steps

		Encryption and Decryption (A) - Implement a mechanism to encrypt and decrypt ePHI.
Audit Controls	164.312(b)	(R) - Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
Integrity - Implement policies and procedures to protect ePHI from improper alteration or destruction.	164.312(c)(1)	Mechanism to Authenticate Electronic PHI (A) - Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
Person or Entity Authentication	164.312(d)	(R) - Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
Transmission Security - Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	164.312(e)(1)	Integrity Controls (A) - Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.
		Encryption (A) - Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Source: 45 CFR Part 164, Subpart C and Appendix A – Security Standards Matrix.
<http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf>

This Brown & Brown Consulting Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

(EAS 1/10)

Content copyright © 2009-10 Zywave, Inc. Images copyright © 2000 Getty Images, Inc. All rights reserved.