

**New Business Associate
Requirements: Ready in 30
Minutes**

Overview

- n Review HITECH Act/ARRA overview and timelines
- n Specific provisions for business associates (BAs), covered entities (CEs), and PHR vendors under HIPAA and HITECH/ARRA
- n When is a vendor a BA or a PHR vendor?
 - HHS v FTC notification
 - Contractual requirements
- n Review penalties for non-compliance
- n Steps to take to ensure compliance

HITECH/ARRA privacy goals

- n Better protect information in the electronic age
- n Hold those who handle protected health information (PHI) accountable for breaches and disclosures
- n Give patients the right for full disclosure accounting
- n Apply requirements to business associates and technology vendors who may not be covered under HIPAA
- n Stepped up enforcement
- n Harsher penalties including responsibility for employees not just company!

HITECH Act Deadlines

- n Breach notification
 - HHS rule for covered entities and business associates
 - Effective September 23, 2009
 - FTC rule for PHR vendors
 - Effective September 24, 2009
 - Full enforcement, including penalties not effective until February 22, 2010
- n Stepped up penalties for privacy violations currently in effect

HITECH Act Deadlines

- n New marketing requirements
 - Effective February 17, 2010
- n Accounting for disclosures by covered entities with EHRs
 - If EHR in place prior to January 1, 2009, deadline is January 1, 2014
 - If EHR in place after January 1, 2009, then accounting must begin for disclosures either on or after January 1, 2011 or on the date that EHR system implemented

**HITECH Act/ARRA
Provisions for BAs and PHR
vendors**

Expanded responsibilities for BAs

- n Under Privacy Rule, business associates must only use or disclose information in a manner permitted by CEs
- n Under Security rule BAs must
 - Comply with administrative, technical, and physical safeguards and requirements and
 - Implement security policies and procedures in the same manner as CEs
- n Contractual breaches by covered entities must be cured by BAs or report to HHS

New rules for PHR vendors

- n PHR vendors not covered by HIPAA Privacy or Security Rules
 - HITECH/ARRA does not include PHR vendors not performing BA functions under the Privacy and Security Rules
 - HITECH/ARRA requires that vendors transmitting organizational data to CEs with EHRs requiring regular access to this information are business associates, not PHR vendors
- n PHR vendors regulated primarily by Federal Trade Commission (FTC) requirements and not HHS through HIPAA

**Information and guidance
from government to date**

Breach Notification Requirements

Breach defined

- n Unauthorized access, use, or disclosure of unsecured protected health information (PHI) in a manner not permitted under the HIPAA privacy rule that compromises security or privacy of such information
 - Allows uses and disclosures pursuant to HIPAA Privacy Rule
 - Narrow application, does not apply to other Privacy Rule provisions or state privacy laws
 - Does not apply to Security Rule

Breach defined

- n No reporting required if entity determines no significant risk of financial, reputational or other harm to the individual
 - Risk assessment provision included in final rule and considered controversial

Breach defined

- n Unsecured PHI is not protected through a technology or methods approved by US Department of Health & Human Services (HHS) that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals

Acceptable methods to secure PHI

n Encryption

- Data at rest: NIST Special Publication 800-111
- Data in motion: FIPS 140-2; NIST Special Publications 800-52, 800-77, 800-113, others

n Data must be destroyed in the following manner

- Paper records: shredded or destroyed to avoid PHI reconstruction
- Electronic media: destroyed or purged per

Who must provide breach notification?

- n Covered entities
 - Must notify individuals whose unsecured protected health information (PHI) has been or is reasonably believed to be accessed, acquired, or disclosed as result of breach pursuant to HHS rule
- n Business associates
 - Must inform CE and CE sends out notice
- n PHR vendors must notify individuals according to same criteria as CEs and BAs except under FTC rule

HHS breach notification rule

- n Exceptions to breach notification requirements under HHS rule
 - Unintentional acquisition, access, or use of PHI by a workforce member person acting under the authority of a covered entity or business associate if
 - Such acquisition, access, or use was made in good faith and within the scope of authority, and
 - Does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule
 - Workforce defined as
 - Volunteers, employees, interns, etc under the direct control of CE whether paid or not or
 - BA working under the control of a CE

HHS breach notification rule

- n Exceptions to breach notification requirements under HHS rule
 - Unintentional acquisition, access, or use of PHI by a workforce member or inadvertent disclosure to another individual at CE or BA with no further disclosure under the rules of HIPAA
 - Disclosure is made to an individual who in good faith is not believed to retain the information
- n Reporting may be delayed if necessary for law enforcement because notice or posting would impede criminal investigation or damage national security

FTC breach notification rule

- n Applies to all PHR vendors, including non-profits generally outside FTC jurisdiction
- n Applies to foreign entities with customers in the United States
- n Rule contains a presumption that any access results in unauthorized access unless reliable evidence suggests otherwise or unauthorized access could not have occurred
- n Access authorized by individual not considered breach
- n FTC rule does not weigh the potential harm to

FTC breach notification rule

- n Exceptions to notification requirements
 - If an entity maintains strong breach detection measures and a breach occurs but is not discovered
- n Reporting may be delayed if necessary for law enforcement because notice or posting would impede criminal investigation or damage national security

Breach notification requirements

Provision	HHS requirement for CEs/ BAs	FTC requirement for PHR Vendors
Timing of notice	Upon discovery of breach notify affected individuals without unreasonable delay no later than 60 calendar days after discovery date	Same as HHS provision
Records involving 500 individuals or more in a certain state or jurisdiction	Must contact individuals and local media outlets	Same as HHS provision
General reporting when 500 or more individuals	Report to HHS within 60 days of discovery http://transparency.cit.nih.gov/breach/index.cfm	Report to FTC within 10 days of discovery by completing form on http://www2.ftc.gov/os/2009/08/R911002hbnform.pdf
Breaches involving fewer than 500 people	To HHS annually thru weblink above By March 1, 2010 for 2009 breaches	To FTC by 60 th day of calendar year following breach using weblink above

General requirements for notice content under both HHS and FTC rules

- n Written notice must be sent through first-class mail or email if individual provides explicit permission
- n Substitute notice may be provided if reasonable attempts to contact individuals have failed or if current contact information is unavailable
- n If 10 or more individuals involved, posting on company website or through media outlets with toll free number available for a period of 10 days

Disclosures & patient rights

- n Broadens right to receive PHI disclosure accounting
- n CEs/BAs use/maintain EHR systems must account for disclosures for treatment, payment, health operations for 3 years prior to request
- n May charge nominal fee
- n Minimum necessary to meet request
 - HHS Secretary to issue guidance by August 2010
- n Rules will be issued 6 months after EHR, HIT standards
- n May request restriction of disclosure to health entity for payment if they pay out of pocket for items

Minimum necessary & limited data Sets

- n HITECH/ARRA tightens requirements passed by HIPAA for minimum necessary and limited data sets
 - For now to comply to the extent practical, must limit disclosures to the minimum necessary for to accomplish the intended purpose
 - HHS guidance in August 2010 will further clarify these requirements

New enforcement penalties

Violation Category	Each Violation	All such violations for identical violations per calendar year
Did not know	\$100 - \$50,000	\$1.5 million
Reasonable cause	\$1,000-\$50,000	\$1.5 million
Willful neglect: corrected	\$10,000-\$50,000	\$1.5 million
Willful neglect: not corrected	\$50,000	\$1.5 million

Adapted from HIPAA Administrative Simplification: Enforcement
45 CFR Part 160
Published October 30, 2009

Role of state attorneys general

- n HITECH allows state attorneys general authorized to bring civil actions against when state residents adversely affected
 - In some cases, might be more stringent penalties for state
- n Maximum penalty may be up to \$25,000/year for all identical violations of a requirement plus attorney fees
- n HIPAA/ARRA/HITECH does not provide individuals a private right of action to bring enforcement actions
 - State laws allowing for private citizen action could apply

Next steps to ensure compliance with new rules

- n Ensure that breach notification requirements are in place and begin logging breaches
 - Remember: reporting to HHS/FTC still required despite enforcement delay
- n Review existing BA agreements and determine whether new agreements are necessary
 - Discussion: are new agreements necessary or can HITECH be incorporated by reference
- n Conduct a documented risk assessment of security rules
 - Security rules provide lawyers and government officials with limited subject matter knowledge an objective checklist to find fault

Link to security rule

[http://www.cms.hhs.gov/SecurityStandard/Downloads/
securityfinalrule.pdf](http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf)

Link to privacy rule and information

<http://www.hhs.gov/ocr/privacy/>

HHS OCR privacy list serve

[http://www.hhs.gov/ocr/privacy/
hipaaunderstandingcoveredentities/listserv.html](http://www.hhs.gov/ocr/privacy/hipaaunderstandingcoveredentities/listserv.html)

Next steps to ensure compliance with new rules

- n Update policies and procedures and ensure appropriate documentation
- n Prepare for EHR disclosure requirements by establishing a process
- n Review insurance policies for consistency with current obligations, risks, and liabilities

Why should you care?

Health Net sued in CT

1/13/2010

- n First lawsuit under new HITECH provisions for breach
- n Health Net lost records of 1.5 million people, including 446K in CT
 - Unencrypted data from portable data drive in May 2009
 - Information included Social Security numbers and bank account numbers
 - Reporting did not occur until 6 months later in November 2009

Health Net sued in CT

1/13/2010

- n CT attorney general alleges the following
 - Failure to effectively train and supervise workforce on policies and procedures regarding use, maintenance, and disclosure of protected patient information
 - Improper delay of notification with no reasonable legal basis
 - Delay resulted in unfair trade practices under CT law

Health Net sued in CT

1/13/2010

- n Health Net defends
 - Data breach did not result in misuse of information and no harm to individuals
 - Offered 2 years of
 - credit monitoring services
 - \$1 million in identity theft insurance
 - fraud resolution services

Why else should you care?

- n Federal and state governments deprived of tax dollars looking for “alternative” funding sources through penalties and fines
- n Lawyers seek more deep pockets in health care breach cases and identity theft cases
- n Loss of reputation and therefore customers

Mary Jo Carden, RPh, JD
Carden & Associates
202-904-2482

MCarden@CardenAssociates.net