

New Realities of Security and Business Associates Under ARRA

CHITA Forum
October 28, 2009

© 2009 Christiansen IT Law

John R. Christiansen, J.D.
Christiansen IT Law
Privacy/Security/Compliance

2212 Queen Anne Avenue North #333
Seattle, Washington 98109
206.301.9412
john@christiansenlaw.net

Presenter CV

***John R. Christiansen, J.D.* - Christiansen IT Law
Information Technology Law: Privacy, Security, Compliance
and Risk Management**

- Chair, ***ABA HITECH Business Associates Task Force*** (2009 – present); ***Committees on Healthcare Privacy, Security and Information Technology*** (2004 – 06); on ***Healthcare Informatics*** (2000 – 04); and ***PKI Assessment Guidelines Health Information Protection and Security Task Group*** (2000 – 2003)
- Adjunct Faculty, ***University of Washington Information School***; and ***Oregon Health and Sciences University Division of Medical Informatics and Outcomes Research*** (2000 – 2003)
- Technical Advisor, ***Health Information Security and Privacy Collaboration*** (2005 – present)
- Publications include ***Policy Solutions for Advancing Interstate Health Information Exchange*** (Nat'l Governors Association 2009); ***Legal Speed Bumps on the Road to Health Information Exchange***, *Journal of Health and Bioscience Law* (2008); ***An Integrated Standard of Care for Healthcare Information Security*** (2005); ***Electronic Health Information: Security and Privacy Compliance under HIPAA*** (2000); etc.

Our Agenda

- What Is HITECH? A Brief Background
- Business Associates Overview: Old and New Basics
- Enforcement and Penalties
- Business Associates Drill-Down
 - Security Compliance
 - Privacy Compliance
- Security Breach Notification: New HITECH and Old State Law
 - Business Associate Contracts

HITECH Background

- The American Recovery and Reinvestment Act of 2009
 - H.R. 1, Pub.L. 111-5 (February 17, 2009)
 - “ARRA” or “the Stimulus Bill
 - 407 pages
- Title XIII of ARRA: Health Information Technology for Economic and Clinical Health Act
 - HITECH Act
 - 53 pages
- Subtitle D: Privacy
 - 21 pages

HITECH Background

- Principally intended as stimulus vehicle
 - Various funding streams for electronic health record (EHR) and related standards, support infrastructure
- Principal regulatory agency: U.S. Dep't of Health and Human Services (DHHS)
- Subtitle D: Privacy
 - Supplements (does not really amend) HIPAA privacy and security regulations
 - Confidence builder for acceptance of increased EHR use, by tightening requirements for use, disclosure, protection of protected health information (PHI)
 - Drafted in haste and it shows
 - Look for unintended, unanticipated consequences

HITECH Background

Subtitle D principal concepts:

- Extend regulation over key healthcare information technology players
- Create new security breach notification requirements
- Increase penalties and tighten enforcement
- Tighten some PHI use and disclosure limitations
- Tweak patient/consumer data access rights

HITECH Background

Subtitle D structure:

- Incorporates key HIPAA regulatory definitions by reference: business associate (BA), covered entity (CE), disclose, protected health information (PHI), use, etc.
- Adds new statutory requirements to existing HIPAA statutory and regulatory requirements
- Mostly does not formally repeal or amend existing HIPAA requirements
 - Some implied amendments appear unavoidable
- Requires some new regulations and some new regulatory guidance

HITECH Background

Compliance dates for BAs

- Default compliance date: February 17, 2010
 - HITECH § 13423
- Security breach notification: September 23, 2009
 - Security breach notification **enforcement** date extended to February 17, 2010
- Enhanced penalties for violations due to “willful neglect:” February 17, 2011

HITECH Background

Other compliance dates:

- Minimum necessary rule: Statutory compliance now, regulatory compliance some time after August 17, 2010
- Electronic health records (EHR) accounting of disclosures: Current EHR users, January 1, 2014 (may be extended to 2016); EHR acquired after January 1, 2009, date of acquisition or January 1, 2011 (may be extended to 2013)
- Prohibition on EHR and PHI sales: April 17, 2011

Business Associates Overview

Defining Business Associates (BAs)

- Covered Entities (CE) – Category of entity regulated by HIPAA
 - Health plan - Any organization which pays health benefits, except accident insurance
 - Health care clearinghouse - Any organization which processes HIPAA electronic transactions
 - Health care providers
 - 45 CFR § 160.103
- No jurisdiction to require compliance by other types of entity
 - BA requirements as a legal workaround to extend PHI protection to unregulated entities

Business Associates Overview

Defining BAs

- Business associate
 - A “person” to whom the covered entity discloses protected health information so the person can carry out, assist with, or perform a function or activity **on behalf** of the covered entity.
 - 45 CFR § 160.103
- Examples
 - Claims processing, transcription service, ASP, utilization review, quality assurance, etc.
 - Legal, actuarial, accounting, collections, consulting, accreditation, financial, etc. services
 - “Any other function or activity regulated by” HIPAA

Business Associates Overview

Business Associate Contracts (BACs)

- CE may disclose PHI to/allow BA to create or receive PHI on CE's behalf upon "satisfactory assurance" BA will "appropriately safeguard" PHI
 - 45 CFR § 164.502
- "Satisfactory assurance" is business associate contract (BAC) including required provisions (or equivalent memorandum of understanding if governmental entities, plan document provisions if group health plan)
 - 45 CFR § 164.504(e)

Business Associates Overview

BA-related penalties

- CE may be penalized if CE “knew of a pattern of activity or practice” of the BA “that constituted a material breach or violation” of the BAC, unless:
 - The CE took “reasonable steps to cure the breach or end the violation” and, “if such steps were unsuccessful:”
 - Terminated the BAC, if “feasible,” or if not “feasible” reported the problem to DHHS
 - 45 CFR §.504(e)(1)(ii)
- Before HITECH, no jurisdiction to penalize BAs

Business Associates Overview

New HITECH BA Rules

- BAs required to comply with HIPAA security regulations and HITECH security requirements
- BAs required to comply with HITECH privacy requirements
- BAs required to comply with requirements of Privacy Rule BAC provisions
- HITECH privacy and security requirements incorporated in BACs
- BAs required to terminate BAC or notify DHHS of CE breach or violation
- BAs may be audited by DHHS
- BAs subject to civil and criminal penalties for HIPAA privacy or security regulation violations

Civil Enforcement

Basic principles

- DHHS to “seek cooperation” in “obtaining compliance”
- DHHS “may” provide “technical assistance” to assist with voluntary compliance
 - 45 CFR § 160.304
- CEs must “keep such records” and submit “such compliance reports” as DHHS determines necessary to determine compliance
- CEs must cooperate with DHHS investigations and permit access (during “normal business hours”) books and records, etc.
- If requested information is in possession of another who refuses to cooperate, certify efforts to DHHS
 - 45 CFR § 160.310

Civil Enforcement

Record maintenance and OCR access

- Not clear that regulations apply to BAs under HITECH
 - Not part of the regulations specifically applied
 - No penalty against BA for noncompliance?
 - (No penalty against CE for noncompliance?)
 - Noncompliance likely to result in “unsatisfactory” informal resolution and initiation of penalty proceedings
- BAs nonetheless required to maintain documentation required by Security Rule, 45 CFR §164.316

Civil Enforcement

Basic principles

- Any “person who believes a [CE – or BA] is not complying with the administrative simplification regulations” may file a complaint with HHS
 - 45 CFR § 160.306
- HHS may conduct “compliance reviews” on own initiative
 - 45 CFR § 160.308
- May be triggered by publicity re security breach – see security breach notification discussion
 - See e.g. Providence Health & Services, investigation after public notification re security breach affecting over 200,000 individuals

Civil Enforcement

Basic principles

- HITECH requires DHHS to provide for “periodic audits” of compliance by CEs and BAs
 - HITECH § 13411
- HITECH requires DHHS to “formally investigate” a complaint if “preliminary investigation of the facts . . . Indicate[s] . . . a possible violation due to willful neglect”
 - HITECH § 13410(a)(2)

Civil Enforcement

CMS Sample Checklist for HIPAA Onsite Investigations

Personnel that may be interviewed

- President, CEO or Director
- HIPAA Compliance Officer
- Lead Systems Manager or Director
- Systems Security Officer
- Lead Network Engineer . . .
- Computer Hardware Specialist
- Disaster Recovery Specialist . . .
- Facility Access Control Coordinator (physical security)
- Human Resources Representative
- Director of Training
- Incident Response Team Leader
- Others as identified....

Civil Enforcement

CMS Sample Checklist for HIPAA Onsite Investigations

Documents and other information that may be requested for investigations/reviews

a. Policies and Procedures and other Evidence that Address the Following:

- Prevention, detection, containment, and correction of security violations
 - Employee background checks and confidentiality agreements
 - Establishing user access for new and existing employees
 - List of authentication methods used to identify users authorized to access EPHI
 - List of individuals and contractors with access to EPHI to include copies pertinent business associate agreements
 - List of software used to manage and control access to the Internet
 - Detecting, reporting, and responding to security incidents (if not in the security plan)
 - Physical security
 - Encryption and decryption of EPHI
-
- Cont'd

Civil Enforcement

CMS Sample Checklist for HIPAA Onsite Investigations

b. Other Documents:

- Entity-wide Security Plan
- Risk Analysis (most recent)
- Risk Management Plan (addressing risks identified in the Risk Analysis)
- Security violation monitoring reports
- Vulnerability scanning plans
 - Results from most recent vulnerability scan
- Network penetration testing policy and procedure
 - Results from most recent network penetration test
- List of all user accounts with access to systems which store, transmit, or access EPHI (for active and terminated employees)

- Cont'd

Civil Enforcement

Investigations in general

- OCR may issue subpoenas for witnesses, production of evidence
- CE (and BA) may not “threaten, intimidate, coerce, harass, discriminate against, or take any other action” against witness or complainant (may be penalized separately)
- Testimony to be recorded and transcribed
 - 45 CFR §§ 160.314, 316
- May result in “resolution agreements,” including payment of “resolution amount”
 - Providence Health & Services, \$100,000
 - CVS, \$2.25 million

Civil Enforcement

Penalty proceedings

- If informal resolution not “satisfactory,” OCR to notify CE (BA) in writing
- CE (BA) may request hearings on notice of proposed determination
- Formal hearing(s) before administrative law judge (ALJ), including right to attorney, discovery, witnesses, briefs, etc.
- After exhaustion of administrative remedies, including DHHS Board appeal, parties may go to court

Civil Monetary Penalties

Penalty determination

- Violation not known (despite due diligence): Remains at \$100/violation to \$25,000 maximum
- Violation due to “reasonable cause:” Increased to \$1,000/violation to \$100,000 maximum
- Violation due to “willful neglect:” Increased to \$500,000/violation to \$1.5 million maximum
 - HITECH § 13410
- All penalties currently effective except “willful neglect”
- DHHS required to publish regulations on “willful neglect” and required to impose penalties for it beginning February 17, 2011

Civil Monetary Penalties

Example: Unauthorized access

- CE (BA) allows employee to access PHI on 20 individuals in [single?] computer file
- CE (BA) has separate obligation to each individual
- Unauthorized access to PHI of 20 individuals = 20 violations
- If CE (BA) could not have known about this violation in the exercise of due diligence (unlikely?), \$100/violation = \$2,000 penalty
- If CE (BA) permitted this due to reasonable cause (what would that be?), \$1,000/violation = \$20,000 penalty
- If CE (BA) permitted this due to willful neglect (attended this seminar but failed to implement), probably, as of February 2011, \$500,000/violation = \$1.5 million penalty (\$10 million, capped)

Civil Monetary Penalties

Example: Defective business associate contract

- CE (BA) enters into five business associate contracts authorizing PHI uses not permitted by Privacy Rule and not including required safeguards provision
- 5 violations each of 2 separate provisions = 10 violations
- If CE (BA) could not have known about this violation in the exercise of due diligence (unlikely?), \$100/violation = \$1,000 penalty
- If CE (BA) permitted this due to reasonable cause (what would that be?), \$1,000/violation = \$10,000 penalty
- If CE (BA) permitted this due to willful neglect (attended this seminar but failed to implement), probably, as of February 2011, \$500,000/violation = \$1.5 million penalty (\$5 million, capped)

Civil Monetary Penalties

Example: Negligent disposal of media

- Security Rule media re-use specification (100 violations)
 - Didn't know: \$10,000
 - Reasonable cause: \$100,000
 - Willful neglect: \$1.5 million (\$50 million, capped)
- Privacy Rule "little security rule" specification (1,000 violations)
 - Didn't know: \$25,000 (\$100,000, capped)
 - Reasonable cause: \$100,000 (\$1 million, capped)
 - Willful neglect: \$1.5 million (\$500 million, capped)
- Security Rule information access management standard (100 or 1,000 violations? – assume 100)
 - Didn't know: \$10,000 (\$100,000, capped)
 - Reasonable cause: \$100,000 (\$1 million, capped)
 - Willful neglect: \$1.5 million (\$50 million, capped)

Civil Monetary Penalties

Example: Negligent disposal of media

- CE (BA) re-sells 100 used computers without scrubbing hard drives containing PHI on 1,000 individuals. Potential violations:
- Security Rule media re-use specification (100 violations)
- Privacy Rule “little security rule” safeguards specification (1,000 violations)
- Security Rule information access management standard (100 or 1,000 violations?)
- Privacy Rule prohibited PHI use standard (1,000 violations)

Civil Monetary Penalties

Example: Negligent disposal of media

- Privacy Rule prohibited PHI use standard (1,000 violations)
 - Didn't know: \$25,000 (\$100,000, capped)
 - Reasonable cause: \$100,000 (\$1 million, capped)
 - Willful neglect: \$1.5 million (\$500 million, capped)

- Total
 - Didn't know: \$70,000
 - Reasonable cause: \$400,000
 - Willful neglect: \$6 million

Civil Monetary Penalties

Other enforcement rules

- State attorneys general granted civil penalties jurisdiction – and attorneys fees for successful action
 - Requires notice to DHHS and opportunity to assume jurisdiction
- Affected individuals may be awarded penalty share per regulations to be effective beginning February 17, 2012
 - HITECH § 13410

BA Security Drill-Down

BA Security Rules:

- Sections 164.308, 164.310, 164.312, and 164.316 of [the Security Rule] shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.
 - HITECH § 13401(a)

BA Security Drill-Down

BA Security Rules:

- Included from Security Rule:
 - 45 CFR §164.308: Administrative safeguards
 - 45 CFR §164.310: Physical safeguards
 - 45 CFR §164.312: Technical safeguards
 - 45 CFR §164.316: Policies and procedures documentation
- Not included:
 - 45 CFR §164.302: Applicability
 - 45 CFR §164.304: Definitions
 - 45 CFR §164.306: General rules
 - 45 CFR §164.314: Organizational requirements

BA Security Drill-Down

Implications of failure to include:

- Applicability: Limited to CEs. Irrelevant as superseded by HITECH
- Definitions: Odd but apparently meaningless. Defined terms in included regulations presumably have the same meaning for BAs as CEs
- General rules: Odd and may have some unpredictable implications.
- Organizational requirements: Odd and possibly meaningless.
 - Requires “terminate contract or notify DHHS” provision. Same requirement imposed on BA via HITECH § 13404(b)
 - Requires CE to have BAC with required provisions. Requirement to implement such BAC is also in Administrative Safeguards, 45 CFR § 164.308(b)

BA Security Drill-Down

General rules

- High-level requirements: Ensure confidentiality, integrity, availability of PHI; protect against reasonably anticipated threats and hazards to PHI, and reasonably anticipated, improper uses and disclosures; ensure compliance
 - Standard security objectives; exclusion of “reasonably anticipated” a problem?
- Flexible approach: Allows CEs to use “reasonable and appropriate” safeguards based on consideration of factors including CE characteristics, systems, costs and risks to PHI
 - Exclusion interpreted as limiting BA flexibility?
- “Required” (R) vs. “addressable” (A) specifications – addressable may use alternative controls to specification, if written analysis supports
 - Exclusion interpreted as limiting BA flexibility?

BA Security Drill-Down

- Administrative safeguards (45 CFR §164.308)
- Standard: Security management process
 - Specifications
 - Risk analysis (**R**): “Accurate and thorough assessment of potential risks and vulnerabilities”
 - Risk management (**R**): Security measures “sufficient to reduce risks and vulnerabilities,” to ensure confidentiality, integrity and availability, protect against reasonably anticipated threats or hazards, protect against improper uses or disclosures, and ensure workforce compliance
 - Sanction policy (**R**): Against workforce for failure to comply with security policies and procedures
 - Information system activity review (**R**): Regular review of audit logs, access reports, security incident tracking reports

BA Security Drill-Down

- Administrative safeguards (45 CFR § 164.308)
- Standard: Assigned security responsibility
 - No separate specification; identify security official responsible for policy and procedure development and implementation
- Standard: Workforce security
 - Specifications
 - Authorization and/or supervision **(A)**: Of workforce with access to electronic protected health information
 - Workforce clearance procedure **(A)**: For determination whether access rights are appropriate
 - Termination procedures **(A)**: To end access to electronic protected health information when employment terminated or clearance determined inappropriate

BA Security Drill-Down

- Administrative safeguards (45 CFR § 164.308)
- Standard: Information access management
 - Specifications
 - Isolate health care clearinghouse functions (**R**)
 - Access authorization (**A**): Policies and procedures to grant users access to system resources allowing access to electronic protected health information (e.g. workstations, transactions, processes)
 - Access establishment and modification (**A**): Policies and procedures to establish, document, review and modify users' access authorizations

BA Security Drill-Down

- Administrative safeguards (45 CFR § 164.308)
- Standard: Security awareness and training program (all workforce, “including management”)
 - Specifications
 - Security reminders **(A)**
 - Protection from “malicious software” **(A)**: Guarding against, detecting, reporting viruses, etc.
 - Log-in monitoring **(A)**: Procedures for monitoring log-in attempts and reporting “discrepancies”
 - Password management **(A)**: Creation, changing and safeguarding

BA Security Drill-Down

- Administrative safeguards (45 CFR 164.308)
- Standard: Contingency planning (emergency and “other occurrences” such as fire, vandalism, system failure, natural disaster) for information systems
 - Specifications
 - Data backup plan (**R**)
 - Disaster recovery plan (**R**)
 - Emergency mode operation (**R**)
 - Plan testing and revision (**A**)
 - Applications and data criticality analysis (**A**): “Assess relative criticality of specific applications and data”
- Standard: Evaluation
 - No separate specification; “technical and nontechnical evaluation,” periodic and “in response to environmental or operational changes,” of extent to which policies and procedures meet Security Rule requirements

BA Security Drill-Down

- Administrative safeguards (45 CFR § 164.308)
- Standard: Business associates
 - Specifications (45 CFR § 164.314)
 - Contract or “other arrangement” required before covered entity “may permit a business associate to create, receive, maintain, or transmit electronic protected health information” on its behalf
 - Not required for transmissions to providers for treatment, by group health plan, HMO, health insurance issuer on behalf of group health plan to plan sponsor, or transmission to government agencies providing public benefits
 - Contract must include provisions (45 CFR 164.314(a) that:
 - Business associate will “implement administrative, physical and technical safeguards that reasonably and appropriately protect” electronic protected health information **(R?)**
 - Any business associate agent or subcontractor will also implement such safeguards **(R?)**
 - Business associate will report “any security incident of which it becomes aware” **(R?)**
 - Contract may be terminated for breach of material term **(R?)**

BA Security Drill-Down

Physical safeguards (45 CFR §164.310)

- Standard: Facility access controls: Policies and procedures to limit physical access to information systems, while permitting authorized access
 - Specifications:
 - Contingency operations **(A)**: Procedures for access to restore lost data under disaster recovery and emergency mode operations
 - Facility security plan **(A)**: To safeguard facility and equipment against unauthorized access, tampering, theft
 - Access control and validation **(A)**: Control and validate individuals' access to facility and equipment, including visitor control and software testing/revision access control
 - Maintenance records **(A)**: Security-related facility elements (e.g. hardware, walls, doors, locks)

BA Security Drill-Down

- Physical safeguards (45 CFR § 164.310)
- Standard: Workstation use
 - No separate specification; policies and procedures to specify proper workstation functions, manner of performing functions, and physical attributes of workstation “surroundings”
- Standard: Workstation security
 - No separate specification; physical safeguards to restrict access to authorized users
- Standard: Device and media controls (hardware, electronic media)
 - Specifications:
 - Disposal (**R**)
 - Media Re-use (**R**)
 - Accountability (**A**): Records of “movement of hardware and electronic media and any person responsible therefore”
 - Data backup and storage (**A**): “Create retrievable, exact copy of electronic protected health information, when needed, before movement of equipment”

BA Security Drill-Down

Technical safeguards (45 CFR § 164.312)

- Standard: Access controls
 - Specifications:
 - Unique user identification (**R**): Unique name or number for identifying and tracking
 - Emergency access procedure (**R**): For obtaining access to electronic protected health information
 - Automatic log-off (**A**): Session termination after predetermined period of inactivity
 - Encryption and decryption (**A**): Electronic protected health information in storage

BA Security Drill-Down

Technical safeguards (45 CFR § 164.312)

- Standard: Audit controls
 - No separate specification; “hardware, software or procedural mechanisms that record and examine” system activity
- Standard: Integrity (protection against improper alteration or destruction)
 - Specification **(A)**: Electronic mechanisms
- Standard: Person/entity authentication (confirmation of identity)
 - No separate specification; procedures to verify identity
- Standard: Transmission security
 - Specifications:
 - Integrity controls **(A)**: Ensure information is not improperly modified without detection
 - Encryption **(A)**

BA Security Drill-Down

Policies, procedures, documentation (45 CFR § 164.316)

- Standard: Policies and procedures
 - No separate specification; may be changed at any time but changes must be documented
- Standard: Documentation (policies and procedures; security actions, activities, assessment; in writing or electronic)
 - Specifications:
 - Time limit (**R**): Six years from later of creation or applicability
 - Availability (**R**): To individuals responsible for implementing documented procedures (presumably also to HHS)
 - Updates (**R**): Periodic review, and in response to “environmental or operational changes”

BA Security Drill-Down

New BA Security Rules:

- HITECH security requirements included
 - “This title” presumably means Title XIII – not just Subtitle D
 - Subtitle D requirements:
 - § 13401 – redundant, recursive
 - § 13401 – security breach notification – unless that’s “Privacy”
 - Future standards adopted under § 3004?

BA Security Drill-Down

New BA Security Rules:

- BA compliance requirements
 - Implement security program meeting all the security regulation requirements
 - Also review CMS Sample Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews for supplemental perspective
 - Coordinate with CE(s) – some security measures may interfere with common or shared activities or systems
 - Examples: Transmission encryption, system access, authorization roles – there are others
 - Look for problems with differing risk tolerances

BA Security Drill-Down

New BA Security Rules:

- Security Rule BAC subcontractor compliance problem
 - 45 CFR § 164.308(b) requires CE to implement BAC “in accordance with” 45 CFR § 164.314(a)
 - 45 CFR § 164.314(a) was not included
- Is BA required to implement BAC imposing BA requirements on CE?
- Is BA required to implement BAC imposing BA requirements on subcontractors?
- Best guess: No.
 - HITECH § 13400 incorporates regulatory definitions of CE and BA
 - HITECH § 13404(b) provides that “CE = BA” for BAC termination purposes; HITECH § 13402(a) does not
 - BA subcontractor would not (usually!) “obtain PHI on behalf of CE”
 - Therefore subcontractor is not a BA

BA Privacy Drill-Down

New BAC Privacy Rules:

- [A BA may use and disclose PHI obtained pursuant to a BAC only] in compliance with each applicable requirement of [45 CFR § 164.504(e)]. The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.
 - HITECH § 13404(a)
- 45 CFR § 164.504(e): Privacy Rule BAC standard and specifications

BA Privacy Drill-Down

New BAC Privacy Rules:

- Privacy Rule compliance in general not required of BAs, but compliance with Privacy Rule BAC requirements is
- Penalties may be imposed on BA for failure to comply with BAC requirements in regulations, not in BAC
 - Compliance with defective BAC would not be sufficient
- HITECH privacy requirements applied to BAs
 - “This subtitle” presumably means Subtitle D, not Title XIII as a whole (regulations codified by “parts” and “subparts”)
 - Subtitle D requirements applicable to CEs – security breach notification, health plan PHI disclosure restrictions, new minimum necessary provisions, new EHR accounting of disclosures rules, new patient access to information rules, new limitations on EHR sales and marketing

BA Privacy Drill-Down

Privacy Rule BAC compliance therefore requires BA to:

- Provide for permitted uses/disclosures of PHI by BA on behalf of CE, and may provide for same for “proper management and administration” of BA
- Prohibit PHI uses/disclosures not permitted by BAC or “as required by law”
- BA to use “appropriate safeguards” to prevent non-permitted uses/disclosures of all PHI – electronic, written, oral
- Report to CE any non-permitted use/disclosure of PHI, and any “security incident of which [the BA] becomes aware”
- Ensure that BA agents/subcontractors agree to same “conditions/restrictions” as BA
- Make PHI available for individual access and amendment, and provide for accounting of disclosures
- Make BA “internal practices, books and records” available to DHHS for review in determining CE’s HIPAA compliance
- Provide for return/destruction/”escrow” of PHI upon termination of BAC
- Authorize termination of BAC if CE “determines” that BA has “violated a material term”
 - 45 CFR §.504(e)

BA Privacy Drill-Down

Health plan disclosures restriction

- “In the case that an individual requests that a [CE or BA] restrict the disclosure of the [PHI] . . . the [CE or BA] must comply with the requested restriction if—
 - “Except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and
 - “The [PHI] pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.”
 - HITECH §13405(a)
- Could this be used to e.g. interfere with health plan review of pre-existing conditions, rescission based on information not provided?
 - E.g. request to law firm representing plan, seeking care information?
 - Does formal discovery become necessary?

BA Privacy Drill-Down

HITECH minimum necessary rules

Existing rules

- “When using or disclosing [PHI] or when requesting [PHI] from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.”
- Exceptions for provider-provider treatment, use or disclosure to or as authorized by individual, to DHHS for investigations/penalty proceedings, required by law or for HIPAA compliance purposes
 - 45 CFR § 164.502(b)

BA Privacy Drill-Down

HITECH minimum necessary rules

Existing rules

- Applies to requests for PHI by CEs, as well as their disclosures
- For recurring types of disclosures, implement (written) policies and procedures identifying persons or classes of persons permitted to receive, and scope of information
- For all other types of disclosures, case-by-case determination using pre-established (written) criteria
 - Document case-by-case determinations
 - 45 CFR § 164.514(d)

BA Privacy Drill-Down

HITECH minimum necessary rule

- “A [CE or BA] shall be treated as being in compliance with section 164.502(b)(1) . . . with respect to the use, disclosure, or request of [PHI] only if the [CE or BA] limits such [PHI], to the extent practicable, to the limited data set . . . or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively.”
- Subject to same exceptions as apply under regulations
 - HITECH § 13405(b)
- Regulations provided for; two phase compliance:
 - Statutory compliance: February 17, 2009 – August 17, 2010+ (18+ months)
 - Regulatory compliance: Regulation effective date forward

BA Privacy Drill-Down

HITECH minimum necessary rule

- A limited data set is [PHI] that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
 - Name address, phone, fax, email, SSN, other ID, vehicle/device ID, URL/IP address, biometrics, photos
 - 45 CFR § 164.514(d)(2), (3)
- But use of limited data sets requires CE (BA) to implement data use agreement governing use and disclosure of limited data set PHI

BA Privacy Drill-Down

HITECH minimum necessary rule

- Agreement required. A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.
- Content required:
 - Permitted uses and disclosures of PHI (as BAC)
 - Establish who is permitted to use or receive limited data set (not as in BAC)
 - Provide that limited data set recipient will not use other than as permitted by agreement or required by law, will use appropriate safeguards, will report non-permitted uses or disclosures, will ensure agents/subcontractors will agree to same restrictions (as BAC)
 - Will not identify (i.e., re-identify) PHI or contact individual data subjects
 - 45 CFR § 164.514(e)(4)

BA Privacy Drill-Down

HITECH minimum necessary rule

- Can services be provided using a limited data set? If so, consider revising BAC to be consistent with data use agreement
 - Appears not to be the case that data use agreement could be used instead of BAC for HITECH minimum necessary purposes
- If services cannot be provided using a limited data set, are they provided on a standardized (routine/recurring) basis? If so, implement policies and procedures consistent with existing minimum necessary rule
- If services are not routine/recurring, develop and implement criteria for determining PHI which is necessary for services

BA Privacy Drill-Down

Prohibition on EHR record, PHI sales

- A [CE or BA shall not directly or indirectly receive remuneration in exchange for any [PHI] unless the [CE – or BA?] obtained from the individual . . . a valid authorization that includes . . . a specification of whether the [PHI] can be further exchanged for remuneration by the entity receiving [PHI] of that individual.
- Not including remuneration “by a [CE] to a [BA] for activities involving the exchange [sic] of [PHI] that the [BA] undertakes on behalf of and at the specific request of the [CE] pursuant to a [BAC].”
 - HITECH § 13405(d)
- Ensure BAC provides language interpretable as “request” for activities

BA Privacy Drill-Down

Accounting of disclosures rule

- Individual entitled to accounting for disclosures made for six years prior to request, except for:
 - Treatment, payment, health care operations;
 - To the individual;
 - Incidental to permitted uses and disclosures
 - Pursuant to an authorization
 - Directories, care support, certain notifications
 - National security
 - To correctional institutions or law enforcement
 - As part of a limited data set
 - 45 CFR § 164.528(a)

BA Privacy Drill-Down

New rule for electronic health records (EHR) users

- “In applying [45 CFR § 164.528], in the case that a [CE] uses or maintains an [EHR] with respect to [PHI] —
 - “The exception [for treatment, payment and health care operations] shall not apply to disclosures through an [EHR] made by such entity of such information; and
 - “An individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such [CE] during only the three years prior to the date on which the accounting is requested.”
 - HITECH § 13405(c)
- Disclosures to law firm for many services would be part of health care operations
 - Confidentiality, privilege implications for law firms serving providers with EHRs?

Security Breach Notification

- HITECH's two breach notification regulatory tracks:
- HITECH § 13402 – “Standard HIPAA”
 - U.S. Department of Health and Human Services (“DHHS”)
 - Draft regulation issued April 17, published 74 Federal Register 19006 (April 27, 2009); “interim final rule” *Breach Notification for Unsecured Protected Health Information* published 74 Federal Register 42740 (August 24, 2009)
- HITECH § 13407 – PHRs
 - U.S. Federal Trade Commission (“FTC”)
 - Notice of proposed rulemaking published at 74 Federal Register 17914 (April 20, 2009); final *Health Breach Notification Rule* published at 74 Federal Register 42962 (August 25, 2009)
 - PHR breach rules “temporary” pending Federal Trade Commission study, report to Congress, additional legislation

Security Breach Notification

HITECH § 13402 excepts PHI which is not “unsecured”

- “Secure” as provided in DHHS regulatory guidance (see below)
- Encryption per HITECH guidance should satisfy state requirements

Security Breach Notification

Guidance on how to “secure” PHI and PHR information published on DHHS website, includes:

- Encryption of “data at rest” consistent with NIST Special Publication 800–111, ***Guide to Storage Encryption Technologies for End User Devices***
- Encryption of “data in transmission” consistent with Federal Information Processing Standards (FIPS) 140–2; NIST Special Publications 800–52, ***Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations***; 800– 77, ***Guide to IPsec VPNs***; or 800–113, ***Guide to SSL VPN***
- Media containing information has been:
 - If paper, film, or other hard copy, shredded or destroyed so information cannot be read or reconstructed
 - If electronic, has been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, ***Guidelines for Media Sanitization***

Security Breach Notification

Analysis: Breach

- HITECH § 13402, 45 CFR § 164.402 (HIPAA CEs and BAs): Risk-based
 - Breach is a compromise which “poses a significant risk of financial, reputational, or other harm to the individual”
 - Breach does not include:
 - Good faith, unintentional acquisition by person otherwise authorized to access PHI, with no retention of information
 - Inadvertent disclosure by person authorized to access PHI at CE or BA to another authorized person at same CE or BA, or organized health care arrangement, with no further non-permitted use or disclosure
 - Disclosure to unauthorized person, where a CE or BA has a good faith belief that s/he would not reasonably have been able to retain such information.

Security Breach Notification

Analysis: Notification

HITECH § 13402

- Breach “discovered” as of “the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.”
- Notification “without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach,” subject to delay based on law enforcement determination notification would interfere with investigation or “cause damage to national security”

Security Breach Notification

Analysis: Notification

HITECH § 13402

- First class mail, or email if individual specifies a preference
- If 10 or more individuals with contact information insufficient/out-of-date, **required** website posting or notice to “major media” in individuals’ residential area
- If 500 or more individuals, required “prominent media outlet” notification
- If 500 or more individuals, mandatory immediate notice to DHHS
- DHHS website posting of breaches involving 500 or more individuals
- Mandatory annual submission of breach logs to DHHS

Security Breach Notification

Analysis: Penalties

- HITECH § 13402: HIPAA civil monetary penalties against CEs, BAs
 - Defendant CE or BA has burden of proof and persuasion
 - “When a [CE or BA] knows of an impermissible use or disclosure of protected health information, it should maintain documentation that all required notifications were made, or, alternatively, of its risk assessment . . . or the application of any exceptions to the definition of “breach” to demonstrate that notification was not required.”
 - Preamble to Interim Final Security Breach Notification Rule

Security Breach Notification

Analysis: BA Obligations

HITECH:

- § 13402: BA required to notify CEs of breaches, including “identification of each [potentially affected] individual.”
- 60 day notification period begins for CE upon receipt of BA notice – unless the BA is the CE’s “agent.” See HITECH § 13402(c)

Security Breach Notification

Analysis: BA Obligations

- Agency determined by federal common law. Preamble to Interim Final Rule
 - “Agency is the fiduciary relationship that arises when one person (a "principal") manifests assent to another person (an "agent") that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act.” §1.01 ***Restatement (Third) of Agency***
 - “An agent has actual authority to take action designated or implied in the principal's manifestations to the agent and acts necessary or incidental to achieving the principal's objectives, as the agent reasonably understands the principal's manifestations and objectives when the agent determines how to act.” § 2.02(1) ***Restatement (Third) of Agency***

BAC Drill-Down

New BAC Rules:

- HITECH §§ 13401(a), 13404(a) provide that HITECH requirements “of this title” (HITECH) and “of this subtitle” (Subtitle D of HITECH) “shall be incorporated into the business associate agreement between the [BA and CE].”
- Does “shall be incorporated” mean:
 - “Are hereby incorporated by law” without further action required by the parties?
 - That the parties “are hereby directed to incorporate the requirements into their BACs” by amendment or update?
- We might (or might not) have OCR guidance by the time you see this slide

BAC Drill-Down

New BAC Rules:

- What is “incorporated” from HITECH?
 - Security breach notification requirements
- Prohibition on health plan disclosures of fully-paid out-of-pocket care, upon request
- Requirements for compliance with minimum necessary/limited data set rules
- Where CE uses EHR, accounting of disclosures requirements, effective depending on date of EHR acquisition and regulations
- Prohibition on sale of EHR records or PHI, effective February 2011
- Where CE uses EHR, individual right of access to electronic data from EHR
- Prohibition on use of PHI for marketing without individual authorization
- Requirement of BAC for any PHI transmission services provider (regional health information organization [RHIO], etc.

BAC Drill-Down

Suggestions for Dealing with BACs

- If OCR says amend, amend
 - If OCR says amend right away, we have a lot of work to do fast
 - If OCR says amend but enforcement will be stayed, we have a lot of work to do but hopefully more time to do it in
- If OCR says incorporated by law, amend anyway
 - Statutory provisions are hard to interpret as contract terms – especially HITECH
 - Statutory obligations do not define details of contract compliance
 - E.g. security breach notification requirements do not specify CE notice terms, procedures for response coordination, cost allocations, etc.
- Staged amendment processes
 - Implement new forms to use going forward – new and renewing contracts
 - Ensure BACs are identified and subject to management
 - Communicate SOON with key BA or CE business partners

BAC Drill-Down

New BAC Termination Rules:

- [45 CFR § 164.504(e)(1)(ii)] shall apply to a [BA] . . . in the same manner that such section applies to a CE, with respect to compliance with the standards in [45 CFR §§ 164.502(e), 164.504(e), except that in applying [45 CFR §164.504(e)(1)(ii)] each reference to the [BA], with respect to a [BAC], shall be treated as a reference to the [CE] involved in such contract.
 - HITECH § 13404(b)
 - 45 CFR § 164.504(e)(1)(ii): Termination of business associate contract for breach
 - 45 CFR § 164.502(e), .504(e): Business associate disclosure and contract standards and specifications

BAC Drill-Down

Old Termination Rule:

- A **[CE]** is not in compliance with the standards in §164.502(e) and paragraph (e) of this section, if the **[CE]** knew of a pattern of activity or practice of the **[BA]** that constituted a material breach or violation of the **[BA's]** obligation under the contract or other arrangement, unless the **CE** took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful: (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to **[DHHS]**
 - 45 CFR § 164.504(e)(1)(ii)

BAC Drill-Down

New Termination Rule:

- A **[BA]** is not in compliance with the standards in §164.502(e) and paragraph (e) of this section, if the **[BA]** knew of a pattern of activity or practice of the **[CE]** that constituted a material breach or violation of the **[CE's]** obligation under the contract or other arrangement, unless the **[BA]** took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful: (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to **[DHHS]**
 - 45 CFR § 164.504(e)(1)(ii)

BAC Drill-Down

What are a CE's obligations under a BAC?

- Existing BAC required provisions binding CE:
 - Terminate the BAC for BA violation
- HITECH required provisions binding CE:
 - Security breach notification requirements
 - Prohibition on health plan disclosures
 - Minimum necessary/limited data set rules
 - EHR accounting of disclosures requirements (effective depending on date of EHR acquisition and regulations)
 - Prohibition on sale of EHR records or PHI (effective February 2011)
 - Individual right of access to electronic data from EHR
 - Prohibition on use of PHI for marketing
 - Requirement of BAC for any PHI transmission services provider

Questions? Thanks!

John R. Christiansen, J.D.

Christiansen IT Law

Privacy/Security/Compliance

2212 Queen Anne Avenue North #333

Seattle, Washington 98109

206.301.9412

john@christiansenlaw.net