Finance/Compliance:
HIPAA Compliance: New HITECH Pitfalls, Enforcement and Penalties

WA-AK HFMA Conference & Trade Fair

February 21, 2013

Presenter CV

John R. Christiansen, J.D. - Christiansen IT Law

- Special Assistant Attorney General to Washington State Health Care Authority, health care information issues related to HIPAA, HITECH, and related issues

- Privacy and Security Expert, ***ONC/OCR Comprehensive Campaign for Communication and Education About the HITECH Act*** (2010 – pres.); Consultant, ***ONC State Health Policy Consortium*** (2010 – pres.); Technical Advisor, ***ONC Health Information Security and Privacy Collaboration*** (2005 – 2009)

- Chair, ***ABA HITECH Megarule/Business Associates Task Force*** (2009 – pres.); ***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)

- Executive Committee/Secretary, **Washington State Bar Association Health Law Section** (2012 – pres.)

- Adjunct Faculty, ***University of Washington Information School*** (2008 – pres.); ***Oregon Health and Sciences University Division of Medical Informatics and Outcomes Research*** (2000 – 2003)

- Publications include ***State and Federal Consent Laws Affecting Health Information Exchange*** (Nat'l Governors Association 2011); ***Policy Solutions for Advancing Interstate Health Information Exchange*** (Nat'l Governors Association 2009); ***An Integrated Standard of Care for Healthcare Information Security*** (2005); ***Electronic Health Information: Security and Privacy Compliance under HIPAA*** (2000); etc.

Our Agenda

- Update on the HITECH changes to HIPAA and some of their unexpected consequences.

- Trends in civil and criminal enforcement of HIPAA, and how to prepare for regulatory queries and investigations.

- How the new HIPAA penalty calculations shift the financial implications of HIPAA and HITECH compliance.

HIPAA/HITECH Privacy and Security

- HIPAA – the Health Insurance Portability and Accountability Act of 1996
  - Privacy Rule – effective 2003
  - Security Rule – effective 2005
- HITECH – the Health Information Technology for Economic and Clinical Health Act; part of 2009 stimulus bill
  - Supplements and amends HIPAA
    - Security Breach Notification Rule and Guidance – effective 2009
    - HIPAA Enforcement – effective 2009
    - HITECH Megarule – effective 2013
      - Modifications to the Privacy and Security Rules
      - Modifications to Security Breach Notification Rule
      - Modifications to Enforcement Rule
      - New rules under Genetic Information Nondiscrimination Act

HIPAA/HITECH Privacy and Security

- HIPAA Basics
  - What is protected?
    - Protected Health Information (PHI) – essentially any patient information, in any medium (written, oral, electronic), maintained for any purpose
    - Medical and health records; administrative, operating, business, research records, etc., etc., etc.

HIPAA/HITECH Privacy and Security

- HIPAA Basics
  - Who is regulated?
    - Covered Entities (CE) – Any health care provider which gets paid electronically, health plans, health care clearinghouses
      - Directly regulated under HIPAA – subject to regulatory obligations and penalties
    - Business Associates (BA) – Any person or organization which obtains or uses PHI to perform a service or function on behalf of a Covered Entity; technology services providers, professional services providers, consultants, etc., etc.
      - Not directly regulated under HIPAA – no regulatory obligations or penalties
      - Indirect regulation by requirement that CEs must have Business Associate Contract (BAC) with BA

HIPAA/HITECH Privacy and Security

- What the Megarule Added: For CEs
  - Miscellaneous minor changes to some disclosures
  - Marketing communications must disclose if CE receives third party remuneration
  - Fundraising communications must include opt-out
  - Some tweaks to Notice of Privacy Practices
  - Electronic records must be provided in electronic form if requested and “readily producible”
  - No disclosure to plans of information about treatment or services, upon request if paid for in full
  - No use of genetic information for insurance underwriting
  - A few other odds and ends
  - New BAC requirements – see below

HIPAA/HITECH Privacy and Security

- What HITECH Added: For BAs
  - Many, many more BAs!
  - Old BA definition: BA is an entity which performs an activity or functions for or on behalf of or provides a service to a CE, which involves use or disclosure of PHI
    - Remember: Under old rules BAs are not regulated, BACs provide indirect regulation

HIPAA/HITECH Privacy and Security

- Many, many more BAs!
  - New BA definition: BA is an entity which performs an activity or functions for or on behalf of or provides a service to a CE, which "creates, receives, maintains, or transmits" PHI, including health information organizations ("HIOs") and some personal health record ("PHR") vendors, **and including BA subcontractors**
  - New subcontractor definition: Entity to which a BA "delegates a function, activity, or service" involving PHI, other than workforce member

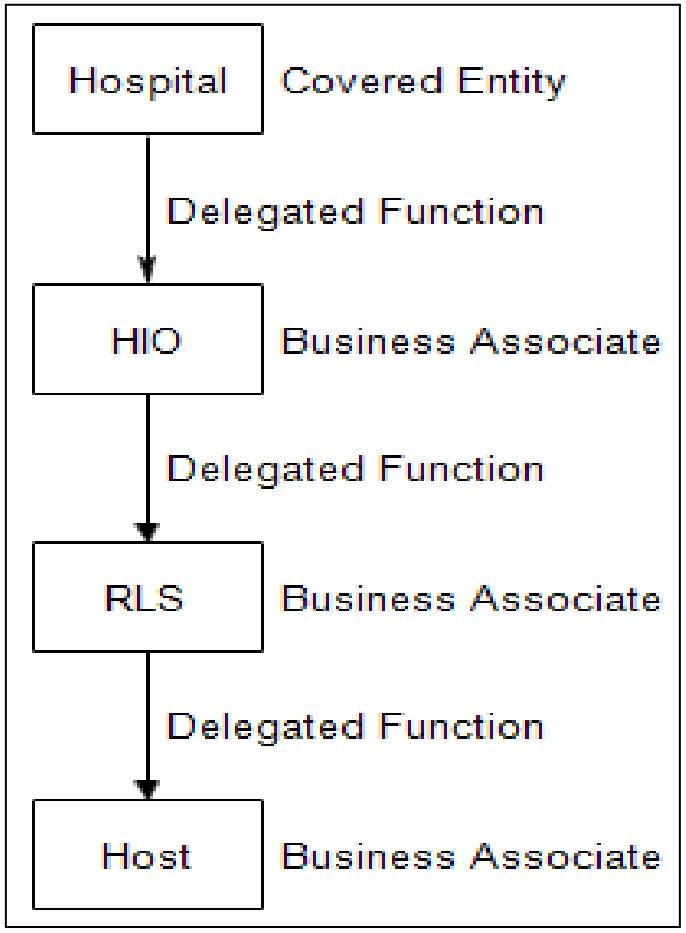
HIPAA/HITECH Privacy and Security

- Many, many more BAs!
  - If a BA delegates a function involving PHI to a subcontractor, that subcontractor becomes a BA
  - If the subcontractor/BA in turn delegates a function involving PHI to another subcontractor, that other subcontractor becomes a BA
  - And so on, as far as activities, functions and services involving PHI are delegated
- A “chain of trust” for PHI

HIPAA/HITECH Privacy and Security

- Example
  - Hospital contracts with HIO to provide health information exchange (“HIE”) services, involving transmission of PHI
  - HIO subcontracts with vendor to provide HIE record locator service to support HIE, involving use of PHI
  - Record locator service subcontracts with data hosting service to support record locator service, involving maintenance of PHI
  - HIO is BA of hospital, record locator service is BA of HIO, hosting service is BA of record locator service

HIPAA/HITECH Privacy and Security



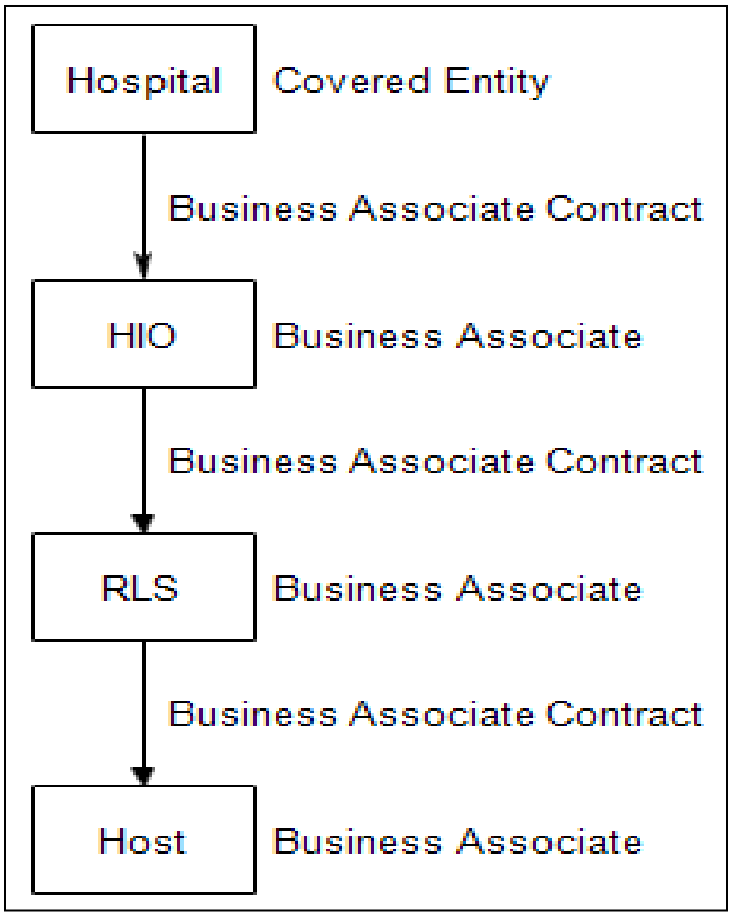
- "Upstream:" CE, or BA delegating function
- "Downstream:" BA to which function is delegated
- "First Tier" BA: BA with direct contract with CE
- "Second Tier" BA: BA with direct contract with First Tier BA (and Third, Fourth Tier, etc.)
- "Lower Tier" BAs: BAs below First Tier

HIPAA/HITECH Privacy and Security

- What HITECH Added: For BAs
  - Regulatory compliance obligations and liabilities
    - Compliance with the Security Rule;
    - Using and disclosing PHI only as permitted by the upstream BAC
    - Compliance with the Minimum Necessary rule
    - Notifying their upstream BA (or CE if applicable) in case of a security breach
    - Providing access to a copy of the electronic PHI in their possession to the CE or individual, as specified in their upstream BAC
    - Providing the information needed for an accounting of disclosures
    - Providing access to their records to OCR to investigate the BA's compliance
  - Requirement for implementing BACs with any Downstream BA

- Belt and Suspenders: Many BAC requirements are redundant to regulatory requirements

HIPAA/HITECH Privacy and Security



- CE is only required to have BAC with First Tier BA
- First Tier BA is only required to have BAC with Second Tier BA
- And so on

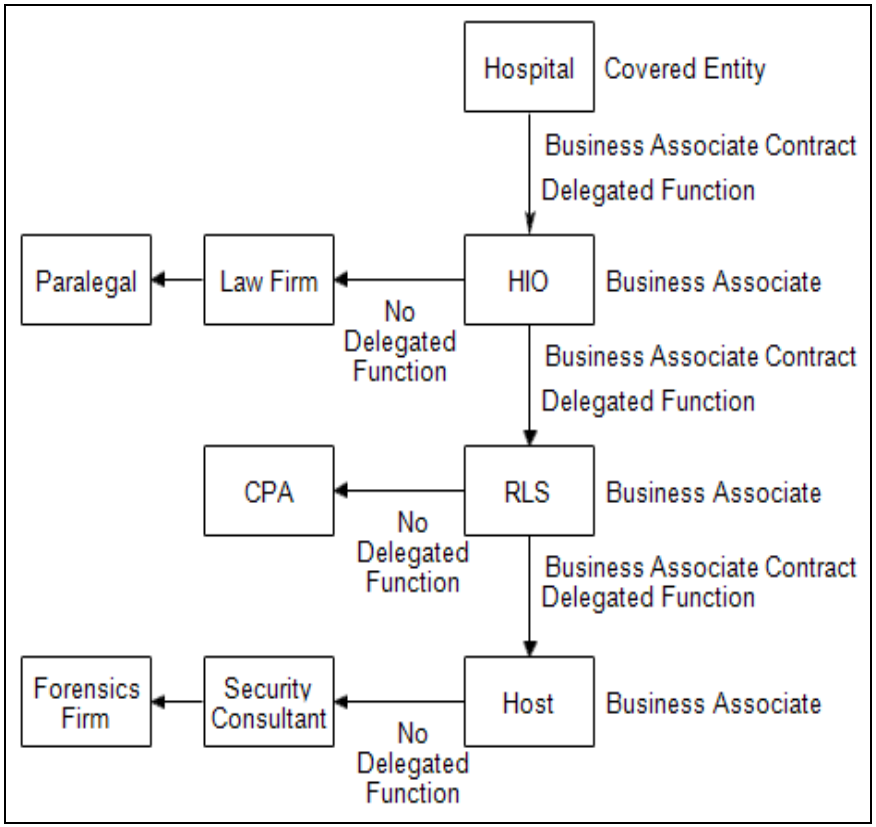
HIPAA/HITECH Privacy and Security

- BAC Requirements: Authorized PHI Uses and Disclosures
  - Prohibition of uses and disclosures of PHI not permitted by BAC
  - Permitted and required uses and disclosures of PHI, may not authorize use or disclosure not permitted to CE (required)
  - Permission to use PHI for BA “proper management and administration” (optional)
  - Permission to use PHI to carry out BA’s “legal responsibilities” (optional)
  - Permission to use PHI for data aggregation for purposes of CE at the top of the chain (optional)
  - Permission to disclose PHI to carry out BA’s “legal responsibilities” if “required by law” (optional)

HIPAA/HITECH Privacy and Security

- BAC Requirements: Authorized PHI Uses and Disclosures
  - Permission for BA to disclose PHI for BA's "proper management and administration," to a person from whom BA "reasonable assurances" that the PHI will be "held confidentially;" will only used or further disclosed as "required by law" or for the purposes for which the PHI was disclosed; that the person will notify the BA "any breach of PHI confidentiality; and that he person will implement "reasonable and appropriate security measures" to protect the PHI (optional)
    - ***This "person" is not a BA***
    - ***The "reasonable assurances" are not a BAC***

HIPAA/HITECH Privacy and Security



- BA Services Provider does not perform delegated function, activity or service
- BA Services Provider may use, disclose PHI for BA purposes
- BA Services Provider may use subcontractors, which are not BAs

HIPAA/HITECH Privacy and Security

- Other BAC Requirements
  - Requirement that BA comply with Security Rule (redundant to regulation)
  - Requirement that BA report security incidents and breaches (partially redundant)
    - Recommendation: Specify procedures to ensure coordination if necessary
  - Requirement that BA accept restrictions on use or disclosure of PHI agreed to by CE at top of chain (redundant)
  - Requirement to make PHI available to individuals consistently with the obligation of CE at top of chain (redundant)
  - Requirement that BA amend PHI consistently with obligations of CE the Covered Entity at top of chain
  - Requirement that BA provide information for accounting of disclosures by or for CE at top of chain (redundant)
  - If BA is carrying out CE Privacy Rule obligation, perform consistently with requirements for CE at top of chain
  - Requirement that BA make internal practices, books, etc. available to OCR for investigation of compliance by CE at top of chain

HIPAA/HITECH Privacy and Security

- Chain Problems in PHI Use and Disclosure Authorization
  - A BA may not authorize any use or disclosure of PHI not authorized by its Upstream BAC
  - Authorization in Downstream BAC must be equivalent to or more stringent than authorization in Upstream BAC
  - Upstream BAC provisions should allow for legitimate optional uses and disclosures

- Example:
  - HIO BAC with record locator service does not include optional provisions allowing disclosure of PHI to carry out legal responsibilities or proper management, or to BA Services Provider
  - Record locator service experiences security breach affecting PHI
  - Vendor is not authorized to retain security consulting or computer forensics firms to contain, mitigate and investigate breach

HIPAA/HITECH Privacy and Security

- Other Chain Problems
  - Pass-along of CE compliance obligations with delegated functions, activities
    - Example: Hospital outsources electronic health record (“EHR“) functions to application services provider
    - Hospital delegates provision of copies of records to individuals to vendor as part of EHR services
    - Vendor delegates health information management functions to HIM outsourcing firm
    - Outsourcing firm must be bound to 60 day turnaround, electronic format requirements applicable to provision of copies by hospital
  - Timing of security breach notification from Lower Tier BAs to CE, which has notification obligations
    - See below

HIPAA/HITECH Privacy and Security

- Compliance Timing
  - Megarule officially published January 25 (unofficially January 18)
  - Official effective date is March 26
  - "Compliance Date" is September 23 (180 days from March 26)
    - For all regulations "that become effective after January 25, 2013, covered entities and business associates must comply with the applicable new standards and implementation specifications, or modifications to standards and implementation specifications, no later than 180 days from the effective date of any such standards or implementation specifications."
    - No obligation to comply means no penalties for failure to comply

HIPAA/HITECH Privacy and Security

- Compliance Timing and BACs
  - No “grandfathered” contracts as proposed
  - Some BACs “deemed compliant” until September 22, 2014
    - To be “deemed compliant” a BAC must be:
      - In compliance with pre-HITECH HIPAA BAC requirements
      - In effect before January 25, 2013,
      - Not apply to agreements or arrangements which are renewed (for evergreen contracts) or amended before September 23, 2013
        - » In other words, if the underlying agreement of a BAC is renewed or amended, the BAC is no longer deemed compliant, even if the BAC is not amended
    - “Deemed compliant” status terminates on the earlier of:
      - Renewal or amendment of the underlying agreement, or
      - September 22, 2014

HIPAA/HITECH Privacy and Security

- Transition Management for CEs
  - Review various CE requirements, amend NOPP and policies, etc. as needed or desired
  - Identify all BAs and BACs
    - Specify any where “deemed compliant” status may be desired
    - Rank according to upcoming renewal or anticipated amendment dates
  - Develop form(s) of HITECH-compliant BAC in preferred form
    - Possible variations for different types of BA, e.g. different types of services vendor, consultants, etc.
    - Consider pros and cons of non-required provisions, e.g. indemnification for breach response costs
  - Develop a plan for rolling out HITECH-compliant BACs
    - Anticipate some may need negotiation, some may involve a “battle of the forms” between BACs, some BAs may be partially or entirely without a clue

HIPAA/HITECH Privacy and Security

- Transition Management for BAs
  - Do Security Rule gap analysis ASAP
    - Revising or implementing fully compliant security program by September 23 may be a challenge for some
  - Identify all Upstream CEs and BAs and Downstream BAs
    - If Lower Tier BA, identify CE at the top of the chain
    - Specify any where “deemed compliant” status may be desired
    - Rank according to upcoming renewal or anticipated amendment dates
  - Develop form(s) of HITECH-compliant BAC in preferred form
    - Possible variations for different types of CE and BA
    - Consider pros and cons of non-required provisions, e.g. indemnification for breach response costs
  - Develop a plan for rolling out HITECH-compliant BACs
    - Anticipate some may need negotiation, some may involve a “battle of the forms” between BACs, some CEs and BAs may be partially or entirely without a clue
    - Ensure consistency where necessary between Upstream and Downstream BACs

HITECH Security Breaches

- Interim Final Rule Updated by Megarule
  - Breach is any “acquisition, access, use, or disclosure” of “unsecured PHI in a manner not permitted under” the Privacy Rule “which compromises the security or privacy” of the PHI
    - Change from the IFR, which defined breach as compromise of PHI 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 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

HITECH Security Breaches

- "Unsecured PHI" does not include PHI rendered "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by" OCR

- Specified technologies and methodologies:
  - 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***

HITECH Security Breaches

- Interim Final Rule Updated by Megarule
  - Burden is now on CE or BA to demonstrate that there is a “low probability” that the PHI has been compromised “based on a risk assessment of least the following factors:
    - Nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification
    - The unauthorized person who used the PHI or to whom the disclosure was made
    - Whether the PHI was actually acquired or viewed
    - The extent to which the risk to the PHI has been mitigated

HITECH Security Breaches

- Notification by CE and/or BA
  - If 500+ individuals, notify OCR and individuals “without unreasonable delay,” no more than 60 days from discovery, subject to law enforcement delay as requested by law enforcement
    - Must include notification via “prominent media outlets”
  - If 500 or fewer, notify individuals within 60 days, OCR within 60 days of end of calendar year in which breach occurs
  - Breach considered “discovered” when actually known or “by exercising reasonable diligence” would have been known to CE
    - Breaches known to workforce members, agents of CE deemed “known” to CE
  - BA must notify CE of breach upon “discovery,” under same terms as CE “discovery”
  - Who’s an “agent?”

HITECH Security Breaches

- Breach Response and Notification Coordination Issues
  - Timing of BA notification: If BA is “agent” of CE, breach is deemed “discovered” by CE upon “discovery” by BA
    - Either avoid making BA an agent, or hold BA to rapid notification to allow timely CE notification
    - Lower Tier BAs should never be considered CE’s BA
    - May still be desirable to have Lower Tiers notify rapidly to avoid excessive response delay
  - Take state breach notification laws into account
    - State breach notification laws apply according to residency of individual, not location of breach, CE or BA
    - State authorities may require notification
    - Different notification standards may apply
    - BA may have independent notification requirements
  - Who pays? Is BAC really appropriate document? Is response cost exposure proportionate to overall contract benefits?

HIPAA/HITECH Enforcement

Expansion of Criminal/Civil Penalties to (BAs)

- In the case of a business associate that violates any provision of subsection (a) or (b), the provisions of sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d–5, 1320d–6) shall apply to the business associate with respect to such violation in the same manner as such provisions apply to a person who violates a provision of part C of title XI of such Act.
  - HITECH § 13404(c)

- 42 USC § 1320d-6: HIPAA criminal penalties
- 42 USC § 1320d-5: HIPAA civil penalties

HIPAA/HITECH Enforcement

HIPAA criminal penalties

- Criminal penalties may be imposed only upon proof beyond a reasonable doubt that a “person”:
  - Knowingly and
  - In violation of HIPAA or any of its regulations,
  - Either:
    - Uses “or causes to be used” a unique health identifier (as required by regulation, e.g. plan or provider number);
    - Obtains individually identifiable health information; or
    - Discloses individually identifiable health information to another person
      - 42 USC 1320d-6(a)

HIPAA/HITECH Enforcement

HIPAA criminal penalties

- Three levels:
  - "Simple" offense (proof of all elements)
    - Fine of not more than $50,000, not more than one year imprisonment, or both
  - "False pretenses" offense (proof of all elements, ***plus*** proof offense committed "under false pretenses"
    - Fine of not more than $100,000, not more than five years imprisonment, or both
  - "Bad intent" offense (proof of all elements, ***plus*** proof of "intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm")
    - Fine of not more than $250,000, not more than ten years imprisonment, or both
    - 42 USC 1320d-6(b)

HIPAA/HITECH Enforcement

HIPAA criminal penalties

- Proving the elements of the offense
  - "Knowingly:" Knowledge of facts indicating the existence of a violation, including actual and circumstantial knowledge, and failure to inquire where circumstances are suspicious
  - "In violation of" HIPAA provision: Must be required to comply as of time of offense
  - "Obtains" information: Includes any exercise of control, direct or indirect
    - Example: Supervisor instructs subordinate to copy information
  - "Disclose" information: Any "release, transfer, provision of access to or divulging in any other manner"

HIPAA/HITECH Enforcement

Several Prosecutions to Date; A Few Cases of Interest

- U.S. v. Holland, Miller and Griffin (2011)
  - Doctor and two hospital employees snooped in celebrity patient file
  - Doctor sentenced to one year probation, $50,000 fine, 50 hours community service educating professionals about HIPAA. Other employees sentenced to one year probation, $1,500 and $2,500 fine respectively.
- U.S. v. Zhou (2010)
  - Terminated physician snooped in co-workers', other patients medical records
  - Four months in prison
- U.S. v. Smith (2008)
  - Clinic nurse gave PHI to husband who used it to threaten data subject
  - Two years probation, community service
- U.S. v. Gibson (2004)
  - Phlebotomist at Seattle Cancer Care Alliance used PHI to obtain credit cards in patient's name

HIPAA/HITECH Enforcement

Basic principles

- OCR to “seek cooperation” in “obtaining compliance”
- OCR “may” provide “technical assistance” to assist with voluntary compliance
- CEs and BAs must “keep such records” and submit “such compliance reports” as OCR determines necessary to determine compliance
- CEs must cooperate with OCR 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 OCR

HIPAA/HITECH Enforcement

Initiation of Compliance Investigation

- Any “person who believes a [CE or BA] is not complying with the administrative simplification regulations” may file a complaint with HHS
  - Every complaint is reviewed and the allegations are analyzed for compliance implications. – Susan McAndrew, OCR Deputy Director
- OCR may conduct “compliance reviews” on own initiative
- OCR required to investigate where facts indicate possible “willful neglect”
  - “Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.”
- May be triggered by security breach notification
  - Every breach involving more than 500 individuals is reviewed for privacy and security compliance. - Susan McAndrew

HIPAA/HITECH Enforcement

Initiation of Compliance Investigation

- HITECH requires OCR to provide for "periodic audits" of compliance by CEs and BAs
- HITECH requires OCR to "formally investigate" a complaint if "preliminary investigation of the facts . . . indicate[s] . . . a possible violation due to willful neglect"
- State attorneys general granted civil penalties jurisdiction – and attorneys fees for successful action
  - Requires notice to OCR and opportunity to assume jurisdiction
  - OCR has provided training to state AG staff
- Investigations may result in "resolution agreements," including payment of non-penalty "resolution amount"
  - Providence Health & Services, $100,000
  - CVS, $2.25 million

HIPAA/HITECH Enforcement

Penalty proceedings

- If informal resolution not “satisfactory,” OCR to notify CE in writing. Burden on CE to satisfy OCR. If not satisfied, OCR may issue notice of proposed determination of civil monetary penalties
- Notice to include findings of fact which are penalty basis
- Target must pursue administrative appeal, through administrative law judge and internal DHHS Board of Appeals, before lawsuit

HIPAA/HITECH Enforcement

Privacy Rule enforcement from April 2003 (start of enforcement) through April 30, 2012:

- Over 70,107 complaints
  - 39,283 not eligible for enforcement (no jurisdiction, etc.)
  - 16,105 resolved with corrective action plans
  - 8,310 finding no violation

Security Rule enforcement from October 2009 (start of enforcement reporting) through March 31, 2012:

- 559 complaints
  - 377 resolved with corrective action plans
  - 257 still pending

HIPAA/HITECH Penalties

- Pre-HITECH
  - Civil monetary penalty (CMP) maximum is $100/violation, to calendar year (Jan. 1 – Dec. 31) $25,000 maximum for “all violations of an identical requirement or prohibition”
- Core Concepts:
  - Single acts/events can implicate multiple requirements or prohibitions
  - Continuing violations – “a requirement or prohibition that is of an ongoing nature” – are counted at one per day of continuation

HIPAA/HITECH Penalties

- HITECH requires CMPs and monetary settlements to be used by OCR for enforcement or distribution to affected individuals
- Distributions to “individuals harmed” by a violation to be determined by rule per methodology to be established by GAO
  - GAO report due August 2010, status unknown
  - Distribution rule due February 2012, status unknown (not included in Megarule)

HIPAA/HITECH Penalties

HITECH Penalties

Table 1 – Categories of Violations and Respective Penalty Amounts Available		
Violation Category – Section 1167(a)(1)	**Each violation**	**All such violations of an identical provision in a calendar year**
(A) Did Not Know	**$100 - $50,000**	**$1,500,000**
(B) Reasonable Cause	**$1,000 - $50,000**	**$1,500,000**
(C) Willful Neglect - Corrected	**$10,000 - $50,000**	**$1,500,000**
(D) Willful Neglect - Corrected	**$50,000**	**$1,500,000**

HIPAA/HITECH Penalties

Penalty determination

- Affirmative defenses: Violation due to “reasonable cause,” not “willful neglect,” and under correction
- Penalty aggravation/mitigation factors: Nature, harm caused by violation; intentional violation vs. violation “beyond control;” compliance history; financial factors

HIPAA/HITECH Penalties

- *Reasonable cause* means circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.
- *Reasonable diligence* means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
- *Willful neglect* means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

HIPAA/HITECH Penalties

Example 1: Unauthorized access

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

HIPAA/HITECH Penalties

Example 1 continued: Unauthorized access constitutes security breach

- Unauthorized access is discovered during OCR investigation of unrelated complaint two years after event
- BA failed to notify 20 affected individuals for two years
  - One or 20 separate continuing violations? 730 violations (2 x 360) or 14,600 violations (2 x 365 x 20)
- BA failed to notify OCR within 60 days of end of calendar year of breach
  - One continuing violation for ten months: 300 violations
- "Could not have known:" Probably not acceptable
- "Reasonable cause:" Probably not acceptable
- Willful neglect, not corrected: $500,000/violation
  - $3 million penalty
    - 730 x $500,00 = $3.65 **b**illion, capped at $1.5 million
    - 300 x $500,000 = $1.5 **b**illion, capped at $1.5 million

HIPAA/HITECH Penalties

Example 2: Defective business associate contract

- CE 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 could not have known about this violation in the exercise of due diligence (probably not acceptable): $100/violation = $1,000 penalty
- If CE permitted this due to reasonable cause (what would that be?): $1,000/violation = $10,000 penalty
- Probably would be held CE permitted this due to willful neglect: $500,000/violation = $1.5 million penalty
  - 10 x $500,000 = $5 million, capped at $1.5 million

HIPAA/HITECH Penalties

Example 3: Negligent disposal of media

- CE 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)
  - Probably also presumed security breach if PHI was not properly encrypted

HIPAA/HITECH Penalties

Example 3 continued: 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)

HIPAA/HITECH Penalties

Example 3 continued: 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)
- Security Breach Notification Rule notification requirements
  - 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: $95,000
  - Reasonable cause: $500,000
  - Willful neglect: $7.5 million

HIPAA/HITECH Penalties

- ***Phoenix Cardiac.*** Small physician practice permitted its physicians to use unencrypted, standard commercial email and cloud-based online calendaring for communications and scheduling including unencrypted PHI. $100,000 fine and a corrective action plan
- ***Blue Cross Blue Shield of Tennessee.*** Health insurer experienced theft of 57 hard drives, unencrypted information on over one million individuals. $1.5 million settlement payment and corrective action plan
- ***Cignet Health***. 41 patients of this four clinic health care provider complained to OCR Cignet would not grant access to their records. Cignet ignored OCR investigative requests. OCR court order for production of the records, to which Cignet responded by producing records on some 4,500 patients, rather than the relevant 41. CMPs of $4.3 million, largely based on continuing violations for failing to provide individuals with record access and failing to cooperate with DHHS

HIPAA/HITECH Penalties

- ***State of Minnesota v. Accretive Health*** (filed January 2012): Action against debt collection agency – i.e., Business Associate – based on loss of laptop storing unencrypted PHI on 23,531 patients of two hospital systems. HIPAA, state privacy law violations, state debt collection violations. Seeking penalties and injunctive relief.
- ***State of Vermont v. Health Net*** (settled January 2011): Action against health insurer based on disappearance of hard drive storing unencrypted PHI on 1.5 million individuals, "including 525 Vermonters," and not notifying affected individuals for six months. HIPAA, state law violations. $55,000 fine, consent decree including mandatory audit and reporting to State for two years.
- ***State of Connecticut v. Health Net*** (settled July 2010): Action based on same incident as Vermont, 500,000+ Connecticut residents affected. HIPAA, state law violations. $250,000 fine, corrective action plan.

Avoiding/Mitigating Penalties

- Well-managed compliance program
- Accountable program management
- Policies and Procedures
- Training and awareness
- Internal auditing, testing and reporting
- Services provider due diligence, tight contracting, oversight
- Readiness to respond to security incidents and breaches
- Readiness to respond to regulatory inquiries

Avoiding/Mitigating Penalties

Document, Document, Document!

Questions? Thanks!