An Ounce (or More) of Prevention: Getting Ready for OCR Breach Notification and Regulatory Investigations.

Future of Healthcare in Washington

April 2, 2014

CHRISTIANSEN IT LAW

WWW.CHRISTIANSENLAW.NET

Information Technology Law | Privacy / Security / Compliance | Contracting, Risk Management & Due Diligence

Presenter CV

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

- 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 AHLA ***Lawyers as Business Associates Toolkit***; 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, **Washington State Bar Association Health Law Section** (2012 – pres.)

- Adjunct Faculty, ***University of Washington Information School*** (2008 – 2012); ***Oregon Health and Sciences University Division of Medical Informatics and Outcomes Research*** (2000 – 2003)

- Publications include ***The HITECH Business Associate Contracts Bible*** (ABA 2013); ***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 and the Basic Strategy

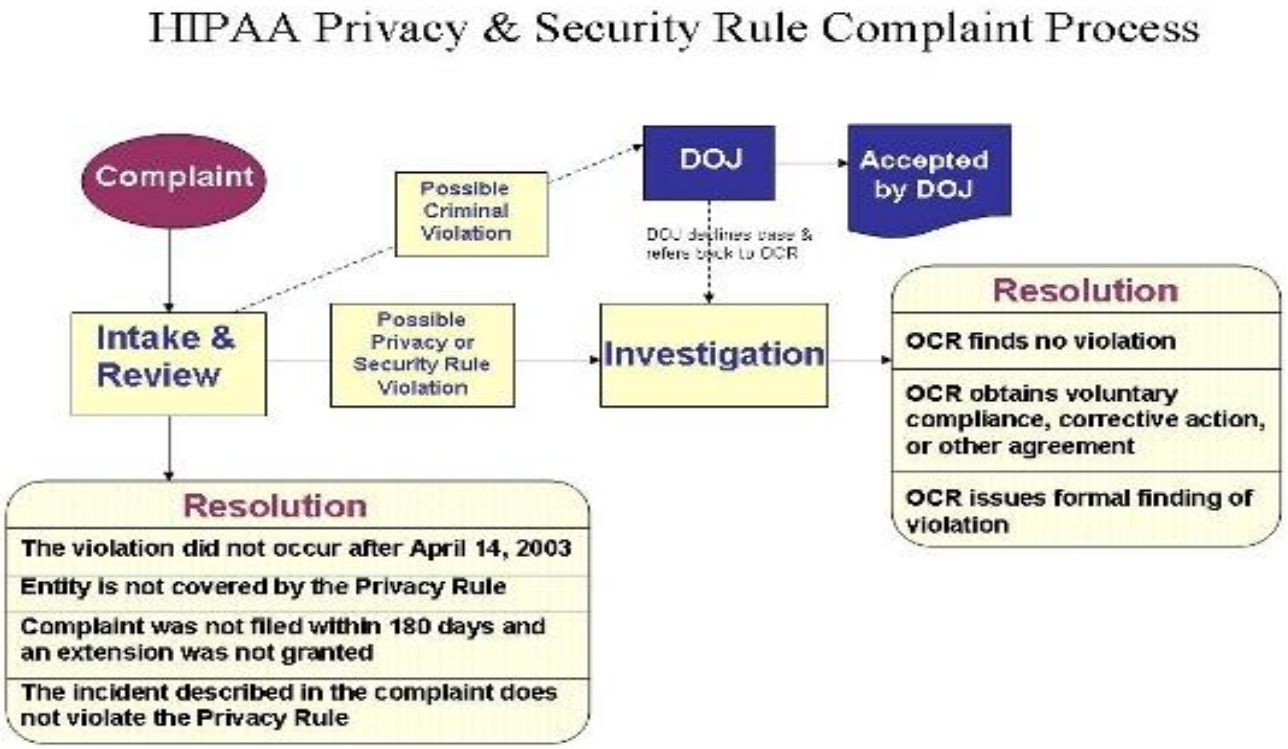
- Assume You Will Be Investigated by OCR
- Assume OCR Will Find Noncompliance
- Be Ready to Respond to the Investigation
- Minimize Your Noncompliance Exposures
- My "Top 4" Compliance Risks
  - Minimum Necessary
  - Security Risk Analysis
  - Encryption
  - Portable Devices

Assume You Will Be Investigated

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
  - 45 CFR § 160.306
  - Every complaint is reviewed and the allegations are analyzed for compliance implications. – Susan McAndrew
- HHS may conduct "compliance reviews" on own initiative
  - 45 CFR § 160.308
- May be triggered by security breach notification
  - Every breach involving more than 500 individuals is reviewed for privacy and security compliance. - Susan McAndrew

Assume You Will Be Investigated



- Source: OCR Health Information Privacy website

Assume You Will Be Investigated

"What OCR Considers During Intake & Review of a Complaint"

- "The alleged action must have taken place after the dates the Rules took effect."
- "The complaint must be filed against an entity that is required by law to comply with the Privacy and Security Rules."
- "A complaint must allege an activity that, if proven true, would violate the Privacy or Security Rule."
- "Complaints must be filed within 180 days of when the person submitting the complaint knew or should have known about the alleged violation of the Privacy or Security Rule. OCR may waive this time limit if it determines that the person submitting the complaint shows good cause . . . "
    - Source: OCR Health Information Privacy website

Assume You Will Be Investigated

Investigation of complaints

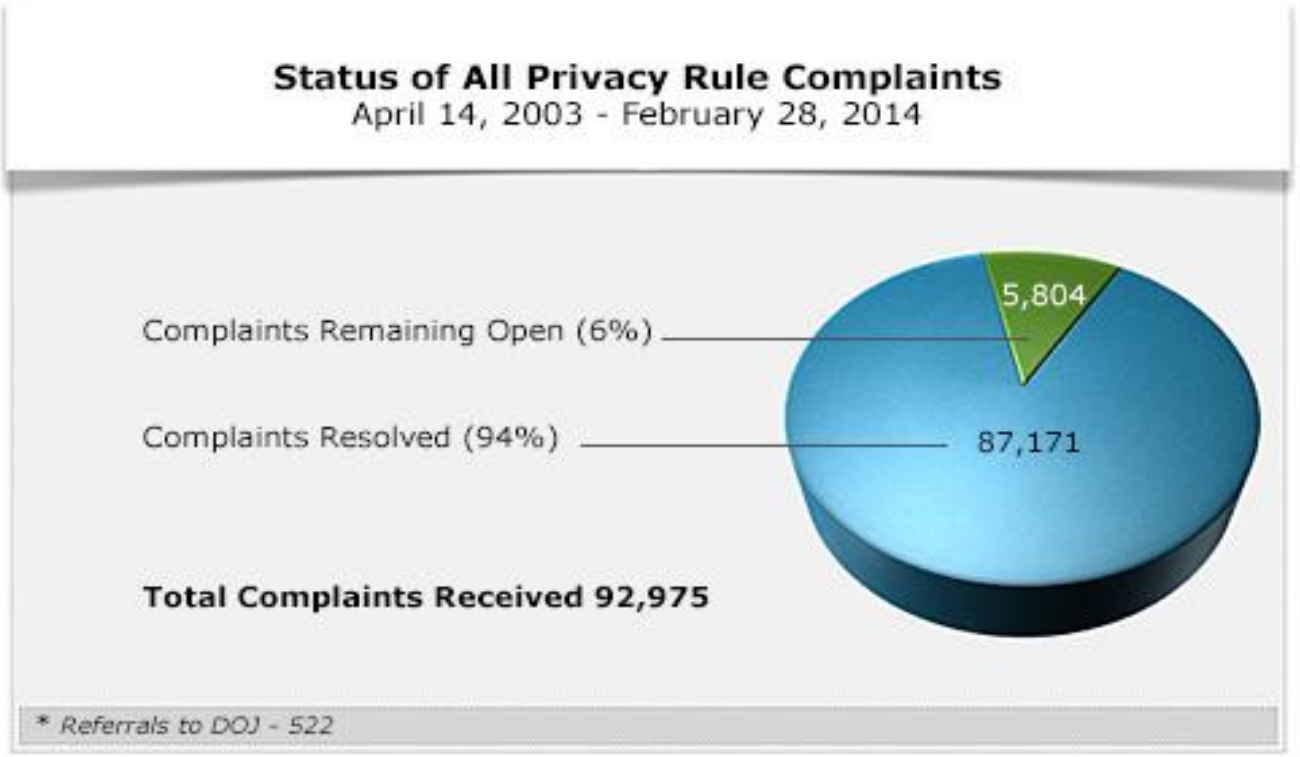
- DHHS to "describe acts or omissions which are basis of complaint at the time of initial written communication with the CE about the complaint"
  - Need not provide copy of the complaint
  - Need not include complainant's identity
    - 45 CFR § 160.306(c)
- Investigations initiated by complaint need not be limited to issues raised by complaint – and often are not
- OCR may issue subpoenas for witnesses, production of evidence

Assume You Will Be Investigated

Privacy Rule Complaints

- 92,975, April 2003 – February 2014
- 32,227 investigated
- 10,005 found no violation
- 22,222 corrective action completed
- 5,804 open as of February 28, 2014
- 522 referrals to U.S. Department of Justice for possible criminal prosecution
  - 54 accepted for pursuit of prosecution
    - Source: OCR Health Information Privacy website

Assume You Will Be Investigated



- Source: OCR Health Information Privacy website

Assume You Will Be Investigated

Security Rule Complaints, October 2009 – February 2014

- 813 investigated
- 598 corrective action completed
- 280 open as of February 28, 2014
- 65 no jurisdiction or no violation?
  - No explanation for difference between number investigated and sum of corrective actions plus open matters
    - Source: OCR Health Information Privacy website

Assume You Will Be Investigated

OCR Audit Program

- "The OCR HIPAA Audit program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. . . . The entire audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. . . .
  - "The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures. . . .
  - "The protocol covers Security Rule requirements for administrative, physical, and technical safeguards.
  - "The protocol covers requirements for the Breach Notification Rule."
    - Source: OCR Health Information Privacy website

Assume You Will Be Investigated

OCR Audit Program

- 2011 – 2012 Pilot Program
  - 115 Covered Entities audited
    - Source: OCR Health Information Privacy website
- Notice of planned "pre-audit survey" of up to 1,200 Covered Entities and Business Associates
  - "The survey will gather information about respondents to enable OCR to assess the size, complexity, and fitness of a respondent for an audit. Information collected includes, among other things, recent data about the number of patient visits or insured lives, use of electronic information, revenue, and business locations."
    - Source: Federal Register notice (February 24, 2014)

Assume You Will Be Investigated

Breaches

- *Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] of this part which compromises the security or privacy of the protected health information," not including:
  - 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.
  - "Secured" (properly encrypted or destroyed) PHI
    - 45 CFR § 164.402

Assume You Will Be Investigated

Breaches

- As of September 2013, "an acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of [a set of specified factors.]"
    - 45 CFR § 164.402
- If more than a "low probability" of "compromise:
  - If fewer than 500 individuals affected, notify individuals "without unreasonable delay" and no later than 60 days, and notify OCR within 60 days of calendar year end
  - If 500 or more individuals affected, notify individuals and OCR "without unreasonable delay" and no later than 60 days
    - 45 CFR §§ 164.404, .408

Assume You Will Be Investigated

Breaches, September 2009 – February 2014

- 834 reported, 500 individuals and over
- Skagit County – small breach example
  - "Skagit County, Washington, has agreed to settle potential violations of the . . . Privacy, Security, and Breach Notification Rules. Skagit County agreed to a $215,000 monetary settlement and to [enter into a resolution agreement with a corrective action plan] to correct deficiencies in its HIPAA compliance program."
  - "OCR opened an investigation . . . upon receiving a breach report that money receipts with . . . [ePHI] of seven individuals were accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the County. OCR's investigation revealed a broader exposure of [PHI] involved in the incident, which included the ePHI of 1,581 individuals. Many of the accessible files involved sensitive information . . . OCR's investigation further uncovered general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security, and Breach Notification Rules.
    - Source: OCR Health Information Privacy website

Assume OCR Will Find Noncompliance

- Presumption: Every major organization can be found in breach of some regulation
  - Privacy policies and procedures may be lacking, insufficient, ignored, misunderstood, deliberately circumvented
  - Security Rule standards are risk-based
    - Good: Allows for necessary variation
    - Bad: More stringent additional or alternate safeguards can almost always be identified
    - Risk management is only as good as your risk analysis
    - Risk analysis is always and only a snapshot – status at the time of observation
      - Hannaford Brothers (2008): Processor certified compliant one day after being notified of two month old malware operations
    - Risk analysis and management may be judged harshly in retrospect: Hindsight is 20/20

Be Ready to Respond to the Investigation

Investigation Principles

- OCR to "seek cooperation" in "obtaining compliance"
- OCR "may" provide "technical assistance" to assist with voluntary compliance
  - 45 CFR § 160.304
- Covered Entities and Business Associates must "keep such records" and submit "such compliance reports" as OCR determines necessary to determine compliance
- Covered Entities and Business Associates 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
  - 45 CFR § 160.310

Be Ready to Respond to the Investigation

Penalties for Not Cooperating

- "Cignet Health Fined a $4.3M Civil Money Penalty for HIPAA Privacy Rule Violations"
  - "In a Notice of Proposed Determination issued October 20, 2010 (NPD), OCR found that Cignet violated 41 patients' rights by denying them access to their medical records. . . .
  - "During the investigations, Cignet refused to respond to OCR's repeated demands to produce the records. Additionally, Cignet failed to cooperate with OCR's investigations of the complaints . . . OCR filed a petition to enforce its subpoena . . . and obtained default judgment against Cignet[.] . . . Cignet produced the [records,] but otherwise made no efforts to resolve the complaints through informal means.
  - "Covered entities are required under law to cooperate with the Department's investigations. OCR found that Cignet's failure to cooperate with OCR's investigations was due to willful neglect. The CMP for these violations is $3 million."
    - Source: OCR Health Information Privacy website

Be Ready to Respond to the Investigation

CMS Sample Checklist for HIPAA Onsite Security 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….

Be Ready to Respond to the Investigation

CMS Sample Checklist for HIPAA Onsite Security 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

Be Ready to Respond to the Investigation

CMS Sample Checklist for HIPAA Onsite Security 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

Minimize Your Noncompliance Exposures

Civil Monetary Penalties

- Violation not known (despite due diligence): $100/violation to $25,000 maximum
- Violation due to "reasonable cause:" $1,000/violation to $100,000 maximum
- Violation due to "willful neglect:" Increased to $500,000/violation to $1.5 million maximum
- "Continuing violations" penalized at one violation per day noncompliance continues
- One event or failure can constitute violation of multiple requirements

A heavy motivation for compliance and cooperation

Minimize Your Noncompliance Exposures

Civil Monetary Penalties

- Affirmative defenses: Violation due to "reasonable cause," not "willful neglect," and under correction
  - 45 CFR § 160.410
- Penalty aggravation/mitigation factors: Nature, harm caused by violation; intentional violation vs. violation "beyond control;" compliance history; financial factors
  - 45 CFR § 164.408

Minimize Your Noncompliance Exposures

Civil Monetary 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.
  - 45 CFR § 160.401

Minimize Your Noncompliance Exposures

Example: Unauthorized access

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

Minimize Your Noncompliance Exposures

Example: Defective business associate contract

- Clinic 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 clinic could not have known about this violation in the exercise of due diligence (unlikely?), $100/violation = $1,000 penalty
- If clinic permitted this due to reasonable cause (what would that be?), $1,000/violation = $10,000 penalty
- If clinic permitted this due to willful neglect (attended this presentation but failed to implement), $500,000/violation = $1.5 million penalty ($5 million, capped)

Minimize Your Noncompliance Exposures

Example: 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)

Minimize Your Noncompliance Exposures

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)

Minimize Your Noncompliance Exposures

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

Minimize Your Noncompliance Exposures

Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year

	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2013	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Mitigation
2012	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Mitigation
2011	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Mitigation
2010	Impermissible Uses & Disclosures	Safeguards	Access	Complaints	Minimum Necessary
2009	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints to Covered Entity
2008	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints to Covered Entity
2007	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2006	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2005	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Mitigation
2004	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Authorizations
partial year 2003	Safeguards	Impermissible Uses & Disclosure	Access	Notice	Minimum Necessary

Source: OCR Health Information Privacy website

Minimize Your Noncompliance Exposures

Reported Breach Characteristics

Number of Breaches	Source	Type of Breach	Individuals Affected
174	Laptop	Theft	4,002,721
72	Desktop Computer	Theft	6,444,702
41	Paper	Unauthorized Access/Disclosure	367,954
39	Paper	Other	406,646
39	Paper	Theft	85,493
32	Network Server	Hacking/IT Incident	1,811,510
31	Paper	Improper Disposal	326,179
30	Other Portable Electronic Device, Other	Theft	433,257
30	Other Portable Electronic Device	Theft	209,667
21	Other	Theft	1,074,877
21	Network Server	Unauthorized Access/Disclosure	177,067
20	Other	Unauthorized Access/Disclosure	204,984
17	Other	Loss	6,245,749
16	Network Server	Theft	591,768
16	Email	Unauthorized Access/Disclosure	261,250
15	Paper	Loss	55,390
13	Other	Other	476,473
13	Other Portable Electronic Device	Theft	57,629

Source: Health Information Privacy/Security Alert (March 2014)

Minimize Your Noncompliance Exposures

- "OCR's 2012 HIPAA pilot audit program uncovered a wide variety of HIPAA compliance failures, including Privacy Rule failures [and] Security Rule failures. . . . In fact, OCR's analysis of the 2012 pilot audit data revealed that two-thirds of the entities audited did not have a complete and accurate risk assessment."
- ". . . one of the primary areas of focus in the 2014 audits likely will be whether covered entities and business associates alike have conducted timely and thorough security risk assessments as required by HIPAA."
- "Another issue which is expected to be a focus of the 2014 audit program is the use of data encryption and an organization's underlying risk analysis in deciding whether to encrypt or not encrypt."
  - Reisz, Gruzs, and Canowitz, "OCR to Begin Second Round of HIPAA Audits," AHLA Health Information and Technology Practice Group Leadership (March 14, 2014)

Minimize Your Noncompliance Exposures

Target significant exposure areas

- Known types of risk causing large breaches
- Continuing violations
- Areas likely targeted by OCR

Minimize Your Noncompliance Exposures

My "Top 4"

- Minimum necessary
  - Continuing violation
  - "Issue 4" in "Top 5"
  - A "foundational" risk
- Security risk analysis
  - Continuing violation
  - Probably "Issue 2" in "Top 5" issues
  - Known OCR target
  - A "foundational" risk
- Portable devices/laptops
  - Really a subset of risk analysis
  - Theft is major cause of breaches with large data losses
- Data encryption
  - Also really a subset of risk analysis
  - Failure to encrypt without risk analysis is continuing violation
  - Known OCR target

Minimum Necessary

Why in the "Top 4?

- Minimum necessary policies and procedures define authorized roles, purposes for use and disclosure of PHI
- Use or disclosure in violation of minimum necessary policies and procedures is therefore potentially a breach
- Potential cause of patient complaints
- Lack of documentation is an easy determination for penalty purposes
- Lack of documentation is a continuing violation
- Every use or disclosure which is made without a policy is also a violation

Minimum Necessary

Enforcement Actions Involving Improper Use/Disclosure

- Pharmacy Chain Changes Process for Disclosures to Law Enforcement
- Health Plan Corrects Impermissible Disclosure of Protected Health Information
- Large Provider Revises Process to Prevent Unauthorized Disclosures to Employers
- Public Hospital Corrects Impermissible Disclosure of Protected Health Information in Response to a Subpoena
- Outpatient Surgical Facility Corrects Privacy Procedure in Research Recruitment
- Large Provider Revises Patient Contact Process
- Large Health Care Provider Restricts Use of Patient Records
- Hospital Revises Email Distribution as a Result of an Impermissible Disclosure
- Private Practice Revises Policies and Procedures Addressing Activities Preparatory to Research
- Hospital Implements New Policies for Telephone Messages
- Dentist Changes Process to Safeguard PHI

  – Source: OCR Health Information Privacy website

Minimum Necessary

Basic Rule

- When using, disclosing or requesting PHI, a Covered Entity or Business Associate must "make reasonable efforts to limit" PHI to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request."
- This requirement does not apply to:

  (i) Uses or disclosures to or by a health care provider for treatment.

  (ii) Uses or disclosures made to the individual.

  (iii) Uses or disclosures made pursuant to an authorization.

  (iv) Disclosures made to the OCR for regulatory purposes.

  (v) Uses or disclosures that are required by law.

  (vi) Uses or disclosures that are required for compliance with the Administrative Simplification regulations.

  – 45 CFR § 164.502(b)

Minimum Necessary

HITECH Amendments

- "A covered entity shall be treated as being in compliance with section 164.502(b)(1) . . . with respect to the use, disclosure, or request of protected health information ***only if the covered entity limits such protected health information, 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)
- OCR guidance called for by August 17, 2010 – expected publication date unknown

Minimum Necessary

HITECH Amendments

- "A limited data set is protected health information 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 SEE:

- "A covered entity may use or disclose a limited data set . . . only if the covered entity obtains . . . 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.
  - 45 CFR § 164.514(d)(4)
- Should this apply?
- Recommendation: Whenever possible define limited data set as minimum necessary by policy; should avoid need to agreement

Risk Analysis

- "An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."
  - 45 CFR § 160.308(a)(1)(ii)(A)
- ". . . OCR director Leon Rodriguez reported . . . that the covered entities audited in the pilot program often had conducted a 'shallow risk analysis' that was not properly updated as circumstances changed, such as the when the entities developed new business strategies or implemented new information systems."
  - Reisz, Gruzs, and Canowitz, supra.

Risk Analysis

Enforcement Actions Involving Lack of, Insufficient Risk Analysis

- Idaho State University Settles HIPAA Security Case for $400,000
- Dermatology practice settles potential HIPAA violations
- HHS settles with health plan in photocopier breach case
- WellPoint pays HHS $1.7 million for leaving information accessible over Internet
- HHS announces first HIPAA breach settlement involving less than 500 patients
- Massachusetts provider settles HIPAA case for $1.5 million
- Alaska settles HIPAA security case for $1,700,000
- HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards
  - Source: OCR Health Information Privacy website

Risk Analysis

- See ONC **Security Risk Assessment (SRA) Tool**
  - Published March 2014
  - Interactive online or paper versions
  - Not mandatory, other approaches are acceptable – but hard to argue with it
  - Is the online version protected against OCR? It's not confidential . . .
- **CAVEAT:**
  - Once you've performed your risk analysis, you must "implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level"
    - 45 CFR § 160.308(a)(1)(ii)(B)
  - Failure to do so would be willful neglect in violation of a wide range of requirements, many continuing
  - Who decides what is "reasonable and appropriate?"

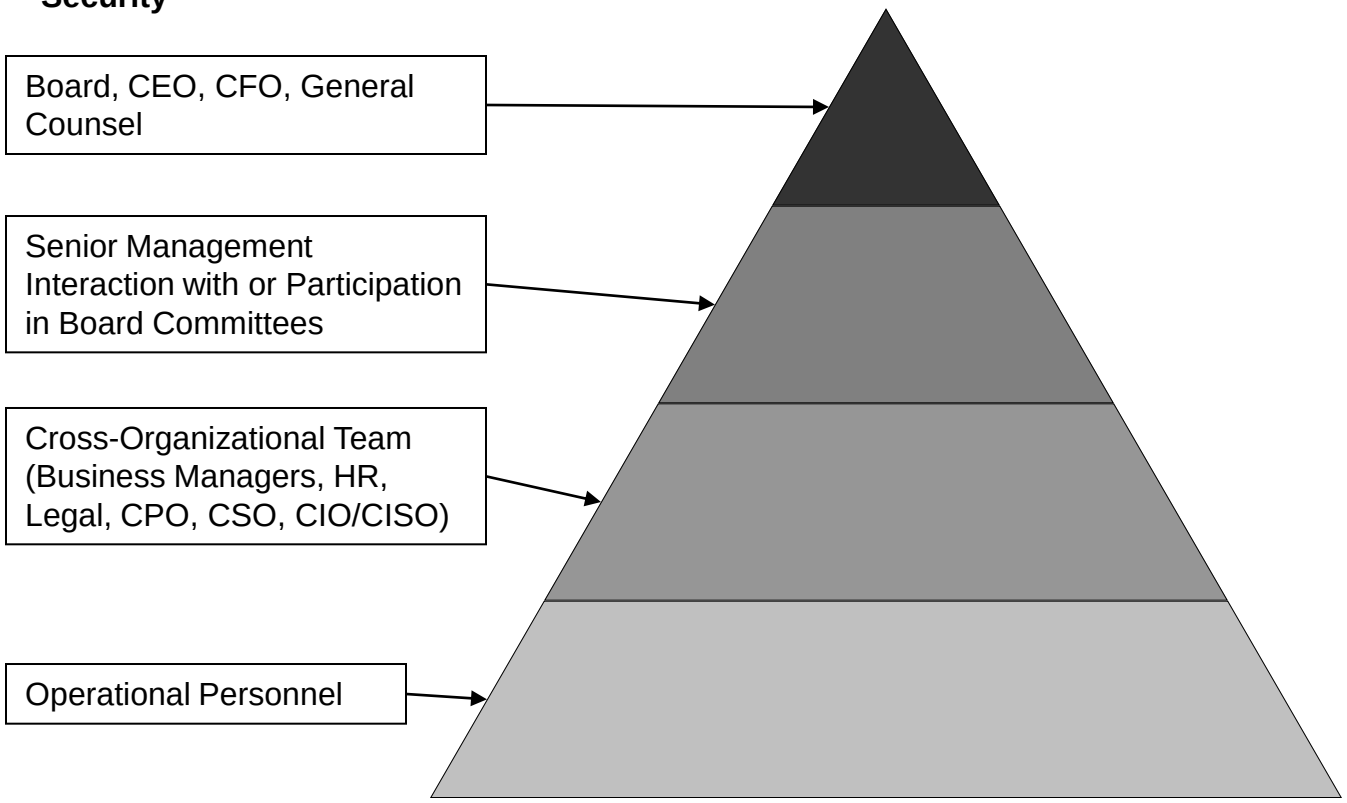
Risk Analysis

- Recommended: Contract through legal counsel
  - Can help keep findings – or at least, conclusions about findings and analyses of alternatives – confidential and privileged
  - Legal counsel probably cannot/almost certainly should not perform at least some technical tasks – subcontract to consulting firm via legal counsel
  - Can advise organization's executives and management about legal risks of alternative strategies
- Ensure documentation of risk acceptance decisions, and reasons for such determinations

Risk Analysis

Risk Analysis and Management

Based on Westby, **Roadmap to Enterprise Security**



Risk Analysis

What Kind of Information Security Are You Practicing?

- Functional or dysfunctional - do executives and board recognize and fulfill oversight obligations?
  - If they don't, who makes the decisions and takes the blame?
- Scope:
  - ICT: Information and communications technology only; or
  - 6PSTNI: People, products, plants (facilities and equipment), policies, processes, procedures, systems, technology, networks and information
  - The Security Rule assumes 6PSTNI

Encryption

Security Rule presumes encryption of data at rest and data in transmission

- "Addressable specifications" at 45 CFR §§164.312(a)(2)(iv), 312(e)(2)(ii)
- Addressable specification means encryption must be used unless the organization:
  - Has a documented analysis which demonstrates why encryption is not "reasonable and appropriate" for the protection of information, and
  - Implements an alternative, "more reasonable and appropriate" safeguard.
    - 45 CFR §§164.306(d)(3)
- Same principles as general risk analysis

Portable Devices

Security Rule Application – the Narrow View

- Inventory and tracking of devices (required)
  - 45 CFR § 164.310(d)(2)(iii)
- PHI "scrubbed" before disposal/re-use
  - 45 CFR § 164.310(d)(2)(i), (ii) (required)
- Encrypt "data at rest"
  - 45 CFR § 164.312(a)(2)(iv) (addressable)
- Authenticate for access
  - 45 CFR § 164.312(d) (required)
- Encrypt network transmissions
  - 45 CFR § 164.312(e)(2)(ii) (addressable)

Portable Devices

The Narrow View is Wrong – Correct Security Rule Application:

- Conduct "accurate and thorough assessment of . . . potential risks and vulnerabilities" affecting PHI
  - 45 CFR § 164.308(a)(1)(ii)(A)
- "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level"
  - 45 CFR § 164.310(d)(2)(i), (ii) (required)
- Given device risks, what suite of decurity measures should be used?

Portable Devices

Required Safeguards Should Include:

- Procedures for review of device activities
- User authorization, supervision, clearance and termination for device and system resources
- Device security awareness and training
- Malware protection
- Device and resource access monitoring
- User authentication management – device and resources
- Device and resource security incident reporting, response procedures
- Device contingency planning
- Device safeguard re-evaluation process
- Device PHI scrub before disposal, re-use
- Device inventory and tracking
- PHI backup and storage from device
- User ID for device access
- Automatic logoff from device
- Encryption of PHI on device
- Device audit trails
- Authentication of ePHI from device
- Transmission integrity controls, encryption for PHI in transmission to/from device

Basic Risk Managment

Document, document, document!

Questions? Thanks!