

## Privacy, Security, and Enforcement

Angela K. Dinh, MHA, RHIA, CHPS  
Director, Professional Practice



## Objectives

- ARRA/HITECH Review
- July 2010 NPRM Review
  - What's not included?
- HIPAA Enforcement
- Accounting of Disclosures
- Q&A



## ARRA/HITECH Review

- American Recovery and Reinvestment Act
- Health Information Technology for Economic & Clinical Health provisions

3



## ARRA/HITECH Review

- February 2009
- HIPAA markedly expanded and penalties stiffened under ARRA/HITECH
- Proposed Changes
  - Privacy
  - Security
  - Enforcement



4

A

## Notice of Proposed Rule Making (NPRM)

- NPRM for HIPAA Privacy, Security and Enforcement Rules – July 14, 2010
  - Compliance is proposed to be 180 days after the final rule except for certain business associate agreements
  - Compliance for small health plans will be the same
  - In the future there will be no difference in compliance for small health plans with regards to privacy, security, and enforcement

5



## Not in July 2010 NPRM

- Still Waiting
  - Risk assessment for "Harm"
  - Changes in state preemption
  - Clear guidance on Minimum Necessary
  - Encryption is still "Addressable"



## HITECH Overview

- Proposed changes:
  - Business Associates
  - Minimum Necessary/Limited Data Set
  - Deceased Individuals
  - Childhood Immunizations
  - Disclosure and Sale of Health Information
  - Marketing
  - Fundraising
  - Research
  - Requested Restrictions
  - Electronic Access
  - Notice of Privacy Practice

7



## Business Associates (BA)

- BA are incorporated into certain privacy, security and enforcement regulations
- Need for new agreements
- Subcontractors
- HIEOs, PSO and PHRs



8



## Minimum Necessary

- Two Tiered approach:
  - CE limits use, disclosure, requests for 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

9



## Minimum Necessary Does Not Apply

- Disclosures or requests by a health care provider for treatment
- Uses or disclosures made to an individual who is the subject of the information
- Uses or disclosures made pursuant to an authorization
- Uses or disclosures required for compliance with HIPAA
- Uses or disclosures made to the Secretary of the Department of Health and Human Services ("Secretary") required for compliance with or enforcement of HIPAA
- Uses or disclosures that are required by law

10



## Decedents

- Involved in care or payment of the deceased
- Not considered PHI if deceased for more than 50 years

11



## Childhood Immunizations

- Proposed changes to allow CE to release proof of immunization to a school without having to obtain a written authorization
  - CE must still obtain disclosure agreement (oral or otherwise) from parent, guardian, or individual
  - Affected by State law



12



## Disclosure & Sale of PHI

- Does not permit a CE or BA to directly or indirectly receive remuneration in exchange for PHI of an individual unless covered by a valid authorization
  - authorization must specify whether the entity receiving the PHI can further exchange the information for remuneration



## Disclosure & Sale of PHI: Exceptions

- Public health data as defined in HIPAA
- Research data as defined in HIPAA
- When the purpose of the exchange is for:
  - Treatment
  - Health care operations
  - Remuneration
  - Providing an individual with a copy of the individual's PHI
  - Otherwise determined by the Secretary in regulations to be similarly necessary and appropriate.



## Marketing

- Expands and defines what can be considered marketing and when an authorization is necessary
- Defines financial remuneration – which is necessary to define some of the marketing situations and the selling of PHI
- Require individual authorization before marketing communication can be received
- Allow individual to opt-out of receiving marketing communications
- Provide statutory exception for prescription refill reminders

15



## Fundraising

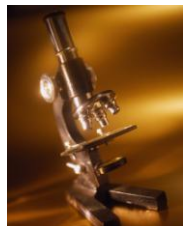
- Opportunity to opt out
- CE may not condition treatment or payment on choice

16



## Research

- Use of compound authorizations
- Authorizing future research use or Disclosure



17



## Restrictions

- HIPAA's right to request privacy protections will remain
- Additional restriction requirement limited to restricting PHI disclosed for payment and operations when service is paid out of pocket in full
- 45 CFR 164.522(a) will still be needed to cover all other restriction requests

18



## Electronic Access to Designated Record Set (DRS)

- CE's that use or maintains an EHR with respect to PHI of an individual, the individual shall have a right to obtain from such CE a copy of such information in an electronic format.
- The individual has a right to direct the CE to transmit a copy directly to another entity or person.
- The CE may not charge the individual any more than its labor costs to respond to a request for a copy of the record.
- In providing the individual with an electronic copy of PHI the CE should ensure that reasonable safeguards are in place

19



## Update Notice of Privacy Practices

- Revise and distribute existing notices
  - Indicate uses and disclosures not described in the notice will require authorizations
  - Expand on reminders
  - Include new Restriction requirement

20



## Update Notice of Privacy Practice

- ARRA to be updated for
  - Business Associates
  - Restrictions
- July NPRM
  - Uses and Disclosures that requires an authorization
  - Marketing updates
  - Opt in/out Fundraising
- AOD
  - Right to request an access report
  - PHI may be used or disclosed for research (OCR looking for comment)



## NPRM Security Changes

- Added “and business associates” with the “covered entities”
- Definition of “electronic media”
- Annual Review of Risk Assessments



## Enforcement

- November IFR is still in effect
- Expanded to include BAs and their agents (subcontractors)
- Investigations will occur when a preliminary review of a complaint indicates possible violation due to willful neglect
- OCR using IFR for penalties



MA

## Enforcement

- OCR is recruiting enforcement agents heavily and has upped their pay scale
- HITECH describes how monies collected for civil penalties will be used and eventually allows individuals to get a cut of the monies if they were harmed by breaches
- OCR HIPAA audits are mandated, not just complaint driven as in the past



24

## OCR HIPAA Audits Underway!

HHS Contractor

- KPMG
  - 150 organizations
  - Variety of sizes
  - By 2012
  - 20 have been identified



AHIMA

## OCR HIPAA Audits Underway!

- OCR will base its decision to audit upon risk not on complaints or reported privacy or security breaches.
- HHS will play an active role in audits
- Audits will include site visits, interviews with leadership, documentation, an examination of operations, and an assessment of the consistency with which process is married to policy.
- Each audit will be followed by a report that will, address compliance efforts and any corrective actions taken.

AHIMA

## Audit Preparation Tips

- Up to date policies and procedures
- Privacy and security training completed
- Effective Privacy and Security compliance program and incidence response
- Security risk assessment and documentation of risk management decision-making process
- Hold mock audits
- **Document! Document! Document!**

AHIMA

## State AG's to Enforce HIPAA

- OCR training includes:
  - Overview of Privacy and security
  - Investigation techniques
  - Preemption Review
  - OCR's enforcement role
  - State attorney's general role and responsibilities
  - HIPAA enforcement and support



AHIMA

## Civil Money Penalties

Four tiered structure - Penalties based on culpability and increase with each tier:

1. Reasonable cause
2. Knowledge and reasonable diligence
3. Willful neglect violation corrected
4. Willful neglect violation *not* corrected



AHIMA

## Civil Money Penalties

Penalties applied will take into consideration the following:

- Violations before or after HITECH
- Nature and extent of the violation
- Harm resulting from the violation (not harm as discussed in Breach Notification)
- History of compliance

AHIMA

## Violations and Breaches

- Snooping into electronic records, unauthorized access, is definitely a privacy violation, maybe a reportable Breach
- Inadvertent access by employees, as long as they immediately close the records they accessed without reading is not a Privacy Breach
- Misdirected faxes are a Privacy Violation as are lost, mailed paper record copies are too, may also be technically a 'Breach'



## Violations and Breaches

- CE must make 'Harm Determination', whether there is a potential for reputational or financial harm resulting from the violation . If there is the potential for harm to the Individual (and the PHI is unsecured according to definition) then the violation is a Breach and both the Individual and OCR must be notified.
- Breach Notification is already in effect. Make sure you are reporting annually!



## Breach Facts

- Types
  - 54% due to Theft
  - 19% Unauthorized Access
  - 14% Loss
  - 6% Hacking
  - 5% Improper Disposal
  - 2% Other
- Total Number
  - 18,059,831



<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>



## Lessons Learned

- Cases in 2011
  - Massachusetts General
  - Cignet
  - UCLA
  - TriCare/DoD



## NPRM: Accounting of Disclosures

- Accounting of disclosures (AoD) is focused on types of disclosures most likely to impact individual
- Access report focused on what most patients want to know - who has seen their health information



## AoD: Why Change?

- Aligns accounting of disclosures with other HIPAA rights
- Lists only exceptions
- Very few requests
- Current process is burdensome



## AoD: Current and Proposed

AoD Current	AoD Proposed
All PHI	PHI in DRS only
Maintain Disclosures for past 6 years	Maintain Disclosures for past 3 years
Implement 2011 (for EHR after 2009) and 2012 (for EHR before 2009)	240 Days after Final Rule
60 days to Respond	30 Days to respond with one 30 day extension
<ul style="list-style-type: none"> <li>Excludes TPO</li> <li>Disclosures only</li> <li>Paper or electronic</li> </ul>	<ul style="list-style-type: none"> <li>Excludes TPO</li> <li>Disclosures only</li> <li>Paper or electronic</li> </ul>



AoD Current	AoD Proposed
Must report all disclosures not authorized by the patient	<b>Excludes</b> <ul style="list-style-type: none"> <li>Adult or Child abuse/neglect/domestic violence</li> <li>Healthcare oversight</li> <li>Research</li> <li>Decedents (to coroner, ME, Funeral Dir. and for organ donation)</li> <li>Protective services of President</li> <li>Required by law (expect Courts or for law enforcement)</li> </ul>
	<b>Includes:</b> <ul style="list-style-type: none"> <li>Impermissible Disclosures – when there is no breach notice</li> <li>Public Health (except child abuse)</li> <li>Judicial and Administrative proceedings</li> <li>Law enforcement</li> <li>Workers comp.</li> </ul>



AoD Current	AoD Proposed
<b>Content for Disclosure Report</b> <ul style="list-style-type: none"> <li>Date of each disclosure</li> <li>For Multiple disclosures to the same person/entity for the same purpose, provide frequency, and the date of last disclosure</li> <li>Name of person (if known) and entity</li> <li>Brief description of PHI disclosed</li> <li>Brief statement of purpose</li> </ul>	<b>Content for Disclosure Report</b> <ul style="list-style-type: none"> <li>Date may be approximate</li> <li>Multiple disclosures may use a date range/frequency</li> <li>Name of recipient</li> <li>Brief description of type of information</li> <li>Brief description of purpose</li> </ul>



## Access Report

- Expands beyond privacy right
  - Individual have right to know who accessed PHI
  - Does not distinguish between disclosures and uses



Access Reports Proposed
Electronic systems only
PHI in DRS only
Maintain Disclosures for past 3 years
Implement 2013 (for EHR after 2009) and 2014(for EHR before 2009)
30 Days to respond with one 30 day extension
Does not distinguish between 'uses' and 'Disclosures' and include TPO
<b>Content of Report:</b> <ul style="list-style-type: none"> <li>Date/Time of access</li> <li>Name of person (if known) or entity</li> <li>Description of what was accessed – if available</li> <li>Description of user action – if available</li> </ul>
Includes business associations (at the option of the individual)
Provide options to limit request to specific date, time period or person
Must provide report in machine readable form and format (e.g. Word, Excel, PFD)
Update NPP to reflect addition of access report

## States

- California has been assessing large fines for relatively small Breaches (\$25,000 - \$250,000) and must be reported within 5 working days
- Connecticut within 5 business days
- State AGs are being trained by OCR (at OCR expense) to enforce HIPAA Privacy
  - This radically expands enforcement
- State preemption remains the same. HIPAA and this Act remain the floor.
- AHIMA has feedback from US Congress that Privacy is considered by the public to be at risk and is a bi-partisan belief that enforcement needs to be stronger



## Examples of Policies to be Created or Updated

1. Toolkit Overview and Privacy Event Checklist
2. Privacy GAP Checklist
3. Breach Determination and Notification
4. Breach Determination and Reporting State vs. Federal
5. Appropriate Access of Protected Health Information (PHI)
6. Confidentiality of Hospital Information
7. Minimum Necessary, Limited Data Set for Disclosure and De-identification of PHI
8. Designated Record Set
9. Individual Access to PHI
10. Disclosure of PHI
11. Fax Policy
12. Request for Amendment of PHI
13. Request to Restrict Use and Disclosure of PHI
14. Request for Accounting of Disclosure (AOD)
15. Authorization for Use and Disclosure of PHI for Marketing Purposes
16. Authorization for use and Disclosure of PHI for Research Purposes
17. Access and Privacy Monitoring
18. Appropriate Access Committee
19. Review and Resolution of Privacy Complaints
20. Privacy/Security Event, Breach, Harm Threshold Analysis and Notification
21. Breach Determination Questions & Answers
22. Breach Determination Decision Tree
23. Mitigation of Improper Use or Disclosure of PHI
24. Enforcement and Discipline for Privacy Violations
25. Request for Audit Log Search of Access to PHI
26. Business Associate Agreement (BAA)
27. Notice of Privacy Practice
28. PHR Privacy and Data Exchange – TBD
29. Sale of PHI – TBD

43



## Examples of Forms to be Created or Updated

- A. NPP Acknowledgment Form
- B. Reporting a Privacy/Security Event or Suspected Privacy/Security Violation
- C. Privacy/Security Event Investigation Form
- D. Processing a Report of a Privacy/Security Event
- E. Privacy/Security Event Corrective Action
- F. Request for Access to PHI
- G. Request for AOD
- H. Request for Amending PHI
- I. Denial of Amendment for PHI
- J. Authorization to Verbally Disclose Health Information
- K. Authorization to Disclose Health Information
- L. Authorization to Request Health Information
- M. Breach Notification Letter
- N. Request for Audit Log Search
- O. Request for Audit Log Search Results or Denial
- P. BA Letter for Breach
- Q. HIPAA Manager Training PowerPoint
- R. HIPAA Training PowerPoint
- S. HIPAA Training Test

44



## Questions?



45



## Resources

### Publications

- e-Alert
- Journal of AHIMA
- Advance
- Perspectives in HIM

### AHIMA Websites:

- Advocacy and Policy Center: [www.ahima.org/advocacy](http://www.ahima.org/advocacy)
- ARRA/HITECH: [www.ahima.org/arra](http://www.ahima.org/arra)

### Other:

- Health Information Xperts Privacy Toolkit – Kelly McLendon, RHIA – [www.hixperts.com](http://www.hixperts.com)

46



## Resources

- ♦ 42 CFR Parts 412, et al. Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Proposed Rule (Meaningful Use)
  - Pages 1857 - 1864 - Federal Register / Vol. 75, No. 8 / Wednesday, January 13, 2010 / Proposed Rules: <http://edocket.access.gpo.gov/2010/pdf/E9-31217.pdf>
- HIPAA Audits Begin – Adam Green <http://www.dwt.com/LearningCenter/Advisories?find=450543>
- DoD hit with lawsuit over lost Tricare data <http://www.armytimes.com/news/2011/10/military-dod-hit-with-lawsuit-over-lost-tricare-data-101311/>



## Resources

- [A HIPAA Security Overview](#)
- [Fundamental of the Legal Health Record and Designated Record Set](#)
- [HIPAA Privacy and Security Training \(Updated\)](#)
- [Limiting the Use of the Social Security Number in Healthcare](#)
- [Notice of Privacy Practices \(Updated\)](#)
- [Preemption of the HIPAA Privacy Rule \(Updated\)](#)
- [Protecting Patient Information after a Facility Closure \(Updated\)](#)



## Resources

- [Regulations Governing Research \(Updated\)](#)
- [Retention and Destruction of Health Information](#)
- [Sanction Guidelines for Privacy and Security Violations](#)
- [Securing Wireless Technology for Healthcare](#)
- [Security Risk Analysis and Management: An Overview \(Updated\)](#)
- [Security Audits of Electronic Health Information \(Updated\)](#)
- [The 10 Security Domains](#)



**THANK YOU!**

**Angela K. Dinh, MHA, RHIA, CHPS**  
**Director, Professional Practice**  
[angela.dinh@ahima.org](mailto:angela.dinh@ahima.org)

