HIPAA Omnibus Final Rule Changes
Breach Notification & Enforcement
Plus An Audit Update
Today’s Speakers

Verne Rinker, JD, MPH
Health Information Privacy Specialist
Office for Civil Rights/HHS

Susan A. Miller, JD
Attorney, Co-Chair, WEDI Breach Notification, Enforcement and Cloud Computing

Ruth A. Carr, JD, LL.M.
Attorney, Co-Chair, WEDI Breach Notification
HIPAA Omnibus Final Rule Changes to Breach Notification

Verne Rinker, JD, MPH
Health Information Privacy Specialist
Office for Civil Rights/HHS
Important Dates

HITECH Omnibus Final Rulemaking

• Published in Federal Register – 78 FR 5566, January 25, 2013

• Effective Date – March 26, 2013

• Compliance Date – September 23, 2013
45 C.F.R. 164.404

(a)(1) A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

IFR [74 FR 42740, August 24, 2009]
Effective: September 23, 2009
**Breach Definition Changes**

45 C.F.R. 164.402

*Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

IFR [74 FR 42740, August 24, 2009]
(1)(i) ...compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual.

HITECH Omnibus FR [78 FR 5566, January 25, 2013]
(2)...an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the CE or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors...
Final Rule changed:

Definition of “breach” (45 C.F.R. 164.402)

- Impermissible use or disclosure of PHI is presumed to be breach, unless entity demonstrates and documents low probability PHI was compromised
- Harm standard removed
- Risk assessment modified to consider at least 4 factors

Exclusions for inadvertent, harmless mistakes remain

Exception for limited data sets without dates of birth & zip codes removed
Breach Notification

- Makes permanent the notification and other provisions of the 2009 Interim Final Rule (IFR), with only minor changes/clarifications
  - E.g., clarifies that notification to Secretary of smaller breaches to occur within 60 days of end of calendar year in which breaches were discovered (versus occurred)
Enforcement Expectations

Breach Notification

• Expect more uniformity in assessing incidents for breach notification purposes
• Continue to investigate major breaches and identify systemic or significant compliance problems to address by corrective action and resolution agreements
• Alert for incidents of failure to report – particularly if willful neglect is present
• Looking for ways to incentivize preventative action in most common problem areas
Breach Notification Highlights
September 2009 - April 15, 2013

• 571 reports involving over 500 individuals
• Over 79,000 reports involving under 500 individuals
• Top types of large breaches
  – Theft
  – Unauthorized Access/Disclosure
  – Loss
• Top locations for large breaches
  – Laptops
  – Paper records
  – Desktop Computers
  – Portable Electronic Devices
Breach Notification:
500+ Breaches by Type of Breach

- Unauthorized Access/Disclosure: 20%
- Theft: 52%
- Loss: 13%
- Hacking/IT Incident: 8%
- Improper Disposal: 5%
- Unknown: 2%

July 17, 2013
OCR / WEDI Webinar
Breach Notification:
500+ Breaches by Location of Breach
BREACH NOTIFICATION

RUTH A. CARR, JD, LL.M.
WEDI CO-CHAIR, BREACH NOTIFICATION
CHANGES IN FINAL RULE

• Definition of Breach (45 C.F.R. 164.402)
  – Impermissible use or disclosure of (unsecured) PHI is presumed to be a breach unless the covered entity or business associate, demonstrates a low probability that the PHI has been compromised or an exception applies

• Burden of proof: demonstrate that all notifications were provided or that an impermissible use or disclosure did not constitute a breach

• No “harm” standard as under Interim Final Rule

• Modified the required risk assessment
“UNSECURED PHI” IS:

• “Unsecured protected health information” means protected health information [PHI] that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance under section 13402(h)(2) of Pub. L. 111-5.
“Breach” means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E which compromises the security or privacy of the protected health information.

An unauthorized acquisition, access, use, or disclosure of PHI must compromise the security or privacy of such information to be a breach
- Statutory exceptions in HITECH Act
- Regulatory exceptions in Final Rule
A Breach shall be treated as discovered by a covered entity on the first day the breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity.

- Not discovered only when management knows!
- Time for notifications starts when breach is discovered or should have been discovered.
RISK ASSESSMENT

Risk Assessment under the Final Rule requires consideration of at least these four factors:

– the nature and extent of the PHI involved, including the types of identifiers and the 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; and

– the extent to which the risk to the PHI has been mitigated
Evaluate the nature and the extent of the PHI involved, including types of identifiers and likelihood of re-identification of the PHI:

- Social security numbers, credit cards, financial data (risk of identity theft or financial fraud)
- Clinical detail, diagnosis, treatment, medications
- Mental health, substance abuse, sexually transmitted diseases, pregnancy
Consider the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made

- Does the unauthorized person who received the information have obligations to protect its privacy and security?
- Does the unauthorized person who received the PHI have the ability to re-identify it?
RISK ASSESSMENT FACTOR 3

• Consider whether the PHI was actually acquired or viewed or if only the opportunity existed for the information to be acquired or viewed

  – Example: Laptop computer was stolen, later recovered and IT analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the entity could determine the information was not actually acquired by an unauthorized individual, although opportunity existed
Consider the extent to which the risk to the PHI has been **mitigated**

- Example: Obtaining the recipient’s satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement, etc.) or will be destroyed (if credible, reasonable assurance)
ASSESSMENT CONCLUSION

• Evaluate the overall probability that the PHI has been compromised by **considering all the factors in combination** (and more, as needed)

• Risk assessments should be
  – Thorough,
  – Completed in good faith, and
  – Conclusions should be reasonable

• If evaluation of the factors fails to demonstrate that low probability that the PHI has been compromised, **breach notification** is required
A Covered entity or business associate has the discretion to provide the required notifications following an impermissible use or disclosure of protected health information without performing a risk assessment.
SAFE HARBOR

• Encryption

• “Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals” (74 Federal Register, Pages 42740, 42742)

• No breach notification required for PHI that is encrypted in accordance with the guidance
PRACTICAL POINTERS

• Review and update policies and procedures
• Train entire workforce in updated policies, including prompt reporting, evaluating and documenting incidents and possible breaches
• Prepare an Incident Response Team
  – Include Privacy Officer, Security Officer, Attorney, Communications, Operations, Budget/Finance, any outside contractors who may be needed quickly
  – Prioritize, confer and practice for potential events
  – Have budget contingency prepared
A breach often triggers news media attention, even without notification by you. Be ready!

- Have a designated spokesperson, who
  - Is part of the Incident Response Team
  - Understands basics of the law and regulations
  - Knows what facts are available, including the projected time of the internal investigation
  - Is calm, honest and forthright
  - Will respect news media deadlines
  - Is “camera ready!”
HIPAA Omnibus Final Rule Changes
Enforcement and an Audit Update

Verne Rinker, JD, MPH
Health Information Privacy Specialist
Office for Civil Rights/HHS
HITECH Enforcement History

IFR [74 FR 56123, October 30, 2009]
Effective: November 30, 2009
• New tiered penalty amounts for violations occurring on or after February 18, 2009
• Modified affirmative defenses

NPRM [75 FR 40868, July 14, 2010]
• Proposed required investigation / formal enforcement for willful neglect
• Proposed adding business associates as applicable
• Preamble discussion of culpability tiers
Omnibus Final Rule/HITECH – What’s New for Enforcement

• Makes permanent the increased civil monetary penalty (CMP) amounts and tiered levels of culpability from 2009 Interim Final Rule

• Clarifies “Reasonable Cause” Tier

• “Willful Neglect” cases do not require informal resolution

• Intentional wrongful disclosures may be subject to civil, rather than criminal, penalties
Enforcement

• Makes permanent the changes from the October 2009 Interim Final Rule
  – New CMP structure
  – Revised limitations on the Secretary’s authority to impose CMPs
Enforcement

• **Definition of Reasonable Cause**
  
  – **Old Definition:** Circumstances that would make it unreasonable for the CE, despite the exercise of ordinary business care and prudence, to comply
  
  – **New Definition:** Act or omission in which a CE (or BA) knew, or by exercising reasonable diligence would have known, that the act or omission was a violation, but in which the CE (or BA) did not act with willful neglect
  
  • Prevents a gap in penalty scheme
Factors in Determining the Amount of a CMP

- **Old Rule**
  - Secretary has discretion with respect to whether and how to apply list of mitigating/aggravating factors in determining CMP amount

- **New Rule**
  - Secretary required to base her determination on nature and extent of the violation and extent of the harm resulting from the violation
Enforcement

• Factors in Determining Amount of a CMP
  – Affirmative Defenses
    • Old Rule
      – No CMP where a violation is criminally punishable
    • New Rule
      – No CMP where a violation is criminally punished
## HITECH Enforcement CMP Tiers

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Identical Violations per Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
### Enforcement Expectations
#### Complaint Investigation and Resolution

As of December 31, 2012

<table>
<thead>
<tr>
<th>As of December 31, 2012</th>
<th>TOTAL (since 2003)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaints Filed</td>
<td>77,200</td>
</tr>
<tr>
<td>Cases Investigated</td>
<td>27,500</td>
</tr>
<tr>
<td>Cases with Corrective Action</td>
<td>18,600</td>
</tr>
<tr>
<td>Civil Monetary Penalties &amp; Resolution Agreements (since 2008)</td>
<td>$15.2 million</td>
</tr>
</tbody>
</table>

July 17, 2013

OCR / WEDI Webinar
Enforcement Expectations
Resolution Agreements

• Five Resolution Agreements and Corrective Action Plans Negotiated in 2012 ($4.85 million)

• Two Resolution Agreements and Corrective Action Plans Negotiated in 2013 ($450,000)

• Expect continued growth and emphasis on significant cases – remain small proportion of all the cases we look at

• Enforcement of compliance with new provisions after September 2013 -- continue to enforce with respect to existing provisions not subject to change
HIPAA Audit Program: An Update
## Multi-year Audit Plan

<table>
<thead>
<tr>
<th>Description</th>
<th>Vendor</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit program development study</td>
<td>Booz Allen Hamilton</td>
<td>Closed 2010</td>
</tr>
<tr>
<td>Covered entity identification &amp; cataloguing</td>
<td>Booz Allen Hamilton</td>
<td>Closed 2011</td>
</tr>
<tr>
<td>Develop audit protocol and conduct audits</td>
<td>KPMG, Inc.</td>
<td>Closed 2011-2012</td>
</tr>
<tr>
<td>Evaluation of audit program</td>
<td>PWC, LLP</td>
<td>Open Conclude in 2013</td>
</tr>
</tbody>
</table>
Enforcement Expectations
Audit Program

• Completed Audits of 115 entities
  – 61 Providers, 47 Health Plans, 7 Clearinghouses
• Total 979 audit findings and observations
  – 293 Privacy
  – 592 Security
  – 94 Breach Notification
• Smaller entities struggle with all three areas
• Still assessing need to follow-up on individual auditees
• Help identify compliance areas of greatest weakness
• Evaluation underway to make audits a permanent part of enforcement efforts
Overall Findings & Observations

No findings or observations for 13 entities (11%)
- 2 Providers, 9 Health Plans, 2 Clearinghouses

Security accounted for 60% of the findings and observations—although only 28% of potential total.

Providers had a greater proportion of findings & observations (65%) than reflected by their proportion of the total set (53%).

Smaller, Level 4 entities struggle with all three areas
Overall Cause Analysis

• For every finding and observation cited in the audit reports, audit identified a “Cause.”

• Most common across all entities: entity unaware of the requirement
  – in 30% (289 of 980 findings and observations):
    • 39% (115 of 293) of Privacy
    • 27% (163 of 593) of Security
    • 12% (11) of Breach Notification

Most causes related to elements of the Rules that explicitly state what a covered entity must do to comply.

• Other causes noted included but not limited to:
  – Lack of application of sufficient resources
  – Incomplete implementation
  – Complete disregard
Next Steps for OCR

Formal Program Evaluation 2013

Internal analysis for follow up & next steps
- Creation of technical assistance based on results
- Determine where entity follow up is appropriate
- Identify leading practices

Revise Protocol to reflect Omnibus Rule

Ongoing program design and focus
- Business Associates
- Accreditation /Certification correlations?
HIPAA Audit Webpage
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

OCR offers a wide range of helpful information about health information privacy including educational resources, FAQ’s, rule text and guidance for the Privacy, Security, and Breach Notification Rules
http://www.hhs.gov/ocr/privacy/
INCREASED ENFORCEMENT

SUSAN A. MILLER, JD
HEALTH TRANSACTIONS, INC.
Enforcement Evolution

- HITECH Act significantly strengthened HIPAA enforcement
- Interim Final Enforcement Rule (Oct. 2009)
  - Created 4 categories of culpability with corresponding penalties (and tightened other areas as well)
  - Took effect immediately
- Omnibus Rule → final enforcement rule
- Enforcement Rule applies to covered entities and business associates
Applicability

• Enforcement Rule originally applied only to covered entities
• Enforcement Rule now applies to
  – Covered entities and
  – Business associates
Focus on Willful Neglect

• Willful neglect: Conscious, intentional failure or reckless indifference to the obligation to comply with HIPAA
• OCR will investigate all cases of possible willful neglect
• OCR will impose penalty on all violations due to willful neglect
Investigations

• Who may investigate:
  – HHS Office for Civil Rights
  – State Attorneys General
  – U.S. Department of Justice

• Enforcement actions
  – Civil
  – Criminal
Criminal Penalties

- Department of Justice (knowingly obtaining or disclosing PHI in violation of HIPAA):
  - $50,000 and/or up to one year imprisonment
  - $100,000 and/or up to five years imprisonment if false pretenses
  - $250,000 and/or up to ten years imprisonment if commercial advantage, personal gain, or malicious harm
How Investigations Begin

- Complaints to OCR
- OCR Compliance review
- Breach report to OCR
- OCR Audits
Actions by State Attorneys General

• HITECH permits State attorneys general to bring actions under HIPAA

• Civil Penalties
  – Up to $100 per violation
  – Up to $25,000 per calendar year for all violations of an identical provision
  – Attorneys’ fees

• Likely to combine with charges under state law

• May not adhere to HHS guidance
Preemption

• GINA: A provision of State law that requires a use or disclosure of genetic information for “underwriting purposes”
• Would be preempted by the Privacy Rule
• Unless an exception applies (see § 160.203)
Liability for Agents

• Covered entity is liable for acts of agents within scope of agency
  – Includes members of workforce
  – Includes agents who are business associates, regardless of whether BA contract is in place

• Business associate also is liable for acts of agents within scope of agency
  – Workforce
  – Agents who are subcontractor business associates
Who Is an Agent?

- Subject to the Federal common law on agency
- Fact specific: taking into account
  - Business associate contract and
  - Totality of circumstances of relationship
- Preamble: Does the covered entity have the authority to control the business associate’s conduct in the course of its performance? (Same for BA and subcontractor)
- Does covered entity have authority to provide interim instructions or directions?
No Culture of Compliance

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Valuation</th>
<th>All identical violations for Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect – corrected in 30 days</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect – not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

Limits are per type of violation, e.g., four types of continuous violations over three years could equal $18 million
### Top Privacy Issues (Based on complaints)

**Top Issues of 2004**

1. Impermissible Uses and Disclosures
2. Lack of Safeguards
3. Failure to Provide Access
4. More than Minimum Necessary
5. Authorizations

**Top Issues through 2012**

1. Impermissible Uses and Disclosures
2. Lack of Safeguards
3. Failure to Provide Access
4. More than Minimum Necessary
5. Lack of Administrative Safeguards of ePHI
# Top Security Issues (Based on complaints)

<table>
<thead>
<tr>
<th>Top Issues of 2005-2009</th>
<th>Top Issues of 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Information access management</td>
<td>1. Risk Analysis</td>
</tr>
<tr>
<td>2. Access controls</td>
<td>2. Security Incident Response and Reporting</td>
</tr>
<tr>
<td>5. Device and media controls</td>
<td>5. Encryption and Decryption (Data in Storage)</td>
</tr>
</tbody>
</table>
Overview of Settlements and CMPs

- 12 settlements, 1 civil monetary penalty
- Average settlement amount ~ $920,000
- Average settlement’s corrective action plan is about 2.4 years
- Some settlements also involved FTC
- 5 of 12 settlements include independent on-site monitoring
Settlements/CMPs
(Settlements represent allegations and not formal findings)

• Providence
  – Loss of backup tapes/laptops (over 350,000 affected)
  – Backup tapes/laptops left unattended/unsecured
  – Significant news story
  – OCR/CMS settlement for $100,000, 3-year CAP, internal monitoring (2008)

• CVS/Rite Aid
  – Improper disposal of prescriptions/pill bottle labels
  – Policy on proper disposal was not working
  – Several TV news stories
  – OCR/FTC settlement for $2.25 million/$1 million, external monitoring and 20-year FTC consent order (2010-11)
Settlements/CMPs
(Settlements represent allegations and not formal findings)

- **Management Services Organization of Washington**
  - Improper disclosure to affiliate for marketing
  - Part of a false claims action
  - OCR (part of OIG/DOJ/OCR) settlement for $35,000, 2-year CAP, internal monitoring (2010)

- **Cignet Health**
  - Failure to provide patients with records and failure to cooperate with OCR investigation/subpoena
  - CMP for $4.3 million (2011)
Settlements/CMPs
(Settlements represent allegations and not formal findings)

• Health Net
  – Portable hard drive lost with 1.5M patient records
  – Six-month delay in notifying individuals
    (pre-HIPAA breach rule)
  – Connecticut AG settlement for $250,000 (2010),
    Vermont AG settlement for $55,000 (2011),
    Connecticut Insurance Commissioner, fine for $375,000 (2011)

• Massachusetts General
  – Loss of 192 paper records (including HIV information)
  – Alleged overall issues with policies on transport of records offsite
  – Significant news coverage
  – OCR settlement for $1 million, 3-year CAP, internal monitoring (2011)
Settlements/CMPs
(Settlements represent allegations and not formal findings)

• **UCLA**
  – Impermissible viewing of PHI (involving celebrity records)
  – Significant news story
  – OCR settlement for $865,500, 3-year CAP, external monitoring (2011)
  – Also led to criminal convictions

• **Accretive Health**
  – Minnesota AG filed suit for data breach involving 25,500 patients (2012)
  – First HIPAA action against business associate
  – BA engaged in multiple lines of business collecting PHI for hospitals (revenue cycle, “quality and total cost of care” initiative)
  – Part of global $2.5 million settlement
Settlements/CMPs
(Settlements represent allegations and not formal findings)

• **BCBS of Tennessee**
  – Theft of 57 hard drives containing customer service audio/video (more than 1,000,000 affected)
  – Server closet was impacted by facility relocation
  – OCR settlement for $1.5 million, 450-day CAP, internal monitoring (2012)

• **Phoenix Cardiac Services**
  – Electronic PHI accessible to public (e-mail, calendar); lack of general security compliance and business associate contract
  – Small physician practice
  – OCR settlement for $100,000, 1-year CAP, no monitoring (2012)
Settlements/CMPs
(Settlements represent allegations and not formal findings)

- **Alaska Department of Health and Social Services**
  - Theft of portable hard drive (may not have even contained PHI)
  - Lack of general Security Rule compliance
  - OCR settlement for $1.7 million, 3-year CAP, external monitoring (2012)

- **Massachusetts Eye & Ear Infirmary**
  - Theft of laptop with PHI of 3,500 individuals (laptop had numerous safeguards)
  - Lack of risk analysis and sufficient security measures
  - OCR settlement for $1.5 million, 3-yr CAP, ext monitoring (2012)
Settlements/CMPs
(Settlements represent allegations and not formal findings)

• Hospice of Northern Idaho
  – Theft of laptop
  – Lack of risk analysis/adequate policies
  – $50,000 settlement/2 year CAP
  – First small breach to result in a settlement
Plus 2 More!

• **Idaho State University** Settles HIPAA Security Case for $400,000 (2013)
  • Breach ePHI of 17,500 individuals - patients at an ISU clinic
    • unsecured for at least 10 months - due to the disabling of firewall protections of servers

• **Shasta Regional Medical Center** Settles HIPAA Security Case for $275,000 (2013)
  • A compliance review of SRMC following a LA Times article
    • Impermissible disclosure by intentionally disclosing PHI to multiple media outlets on at least three separate occasions, without a valid written authorization
WellPoint, Inc. Settles HIPAA case for $1.7 million (2013)

OCR began its investigation following a breach report submitted by WellPoint of security weaknesses in an online application database left the ePHI of 612,402 individuals accessible to unauthorized individuals over the Internet.

- Beginning on Oct. 23, 2009, until Mar. 7, 2010

WellPoint did not:

- Adequately implement policies and procedures for authorizing access to the online application database
- Perform an appropriate technical evaluation in response to a software upgrade to its information systems
- Have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database

OCR enforcement actions to date:

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html
Create a culture of compliance

- OCR aggressively enforcing the HIPAA Privacy, Breach and Security Rules
- OCR suggests that covered entities and business associates should have a robust HIPAA privacy and security compliance program, including:
  - Employee Training
  - Vigilant implementation of policies and procedures
  - A prompt action plan to respond to incidents and breaches
  - Regular internal audits
Future Webinars

• July 26 – Business Associates
  • Modified definition
  • BA liability
  • Privacy and Security rule provisions applicable to BA

• August/September- Drill Downs.... Details TBD
Thank You for participating in today’s webinar