HIPAA Compliance in 2013:

National Association for Home Care & Hospice
March on Washington
March 18, 2013

Today’s Speakers

Marcia Augsburger
• Partner, DLA Piper, LLP (US)
• Firm HIPAA Officer and HIPAA Working Group Co-Chair

John DiMaggio
• President, CEO of MCS2 Healthcare Security Solutions

Tiffani V. Williams
• Associate, DLA Piper, LLP (US)
Overview

› Part I: HIPAA Overview
  ◦ HIPAA Basics
  ◦ HITECH Act Overview
  ◦ Key HIPAA Final Rule Changes

› Part II: HIPAA/HITECH Security
  ◦ What's at Stake?
  ◦ Implementing Risk Management Plans
  ◦ Protecting Healthcare Information

› Part III: Enforcement & Compliance
  ◦ Enforcement Landscape
  ◦ Preparing for Compliance Audits
  ◦ Contesting Fines

Part I: HIPAA Overview

Tiffani V. Williams, Associate, DLA Piper, LLP (US)
HIPAA Basics


- Required HHS to establish standards for the electronic exchange, privacy, and security of health information.

- HIPAA Administrative Simplification Rules:
  - Privacy Rule
  - Security Rule
  - Enforcement Rule
  - Unique Identifier Rule
  - Transactions and Code Sets Rule

HIPAA Basics (cont’d)

- **Covered Entity (CE):**
  - **Health Plans:** Individual and group plans that provide or pay the cost of medical care.
  - **Health Care Providers:** Any provider who electronically transmits health information in connection with standardized transactions regulated by HIPAA (e.g., claims transactions, benefit eligibility inquiries, etc.).
    - Covers transactions conducted either directly or indirectly by the provider.
    - Includes all “providers of services,” (e.g., institutional providers such as home health agencies), “providers of medical or health services,” and any other person or organization who furnishes, bills, or is paid for health care.
  - **Health Care Clearinghouses:** Entities that process nonstandard information they receive from one entity into a standard format (or vice versa).
    - Billing services, repricing companies, etc.

- **Business Associate (BA):**
  - A person or organization (other than an employee of the CE) that performs certain functions or activities on behalf of the CE that involves the use or disclosure of protected information.
HIPAA Basics (cont’d)

- **Protected Health Information or PHI**
  - Individually identifiable health information held or transmitted by a CE or BA in any form or media (e.g., electronic, paper, oral).
  - Information that can identify an individual or that can reasonably be expected to identify an individual that relates to:
    - Past, present, or future physical or mental condition.
    - Provision of health care.
    - Past, present, or future payment for the provision of health care.

The HITECH Act

- Enacted as part of the American Recovery and Reinvestment Act in 2009.
- Required expansive changes to HIPAA:
  - Applying HIPAA privacy and security requirements directly to BAs.
  - Establishing mandatory security breach reporting requirements.
  - Creating new privacy requirements for CEs and BAs.
  - Establishing new criminal and civil penalties for noncompliance.
- Since HITECH, HHS issued proposed and interim final regulations to implement its changes.
The Final Omnibus HIPAA Rule

On January 25, 2013, the Office of Civil Rights (OCR) published an omnibus regulation finalizing HHS’ previously-issued regulations:

◦ Proposed Rule modifying the Privacy, Security, and Enforcement Rules.
◦ Interim Final Rule adopting changes to the Enforcement Rule.
◦ Interim Final Rule on Breach Notification for Unsecured Protected Health Information.
◦ Proposed Rule modifying the Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA).

Redefining A “Business Associate”

Pursuant to the final rule, BAs are entities that:

› Create,
› Receive,
› Maintain, and/or
› Transmit PHI on behalf of a covered entity.
Business Associates

- The final rule makes clear that BAs include:
  - Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services to a CE and requires routine access to PHI.
  - A person that offers a PHR to one or more individual on behalf of a CE (e.g., PHR vendors).
  - A subcontractor that creates, receives, maintains, or transmits PHI on behalf of a BA.
  - Organizations that perform certain patient safety activities (e.g., Patient Safety Organizations).

Subcontractors As Business Associates

- The final rule applies the BA provisions of the HIPAA Rules to subcontractors.
  - A person to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the BA’s workforce.
  - Subcontractors that are involved with the creation, receipt, maintenance or transmission of PHI must be in compliance with the applicable HIPAA Rules.
  - BAs must obtain satisfactory assurances in the form of a BA agreement or otherwise that a subcontractor will comply with HIPAA requirements.
Business Associate Liability

**Before:**
- BAs are contractually liable for failing to comply under BA agreements with covered entities.

**Now:**
- BAs are directly liable for:
  - Uses and disclosures of PHI that are not in accord with its BA agreement or the Privacy Rule;
  - Failing to disclose PHI when required for investigative purposes or when individuals request copies of their PHI;
  - Failing to make reasonable efforts to limit information disclosed to the minimum necessary;
  - Failing to enter into BA agreements with subcontractors, and;
  - Contractually liable for any obligations in its BA agreements.

---

Breach Notification Rule

**What is a breach?**
- **Interim Final Rule:** Acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule that “compromises” the security or privacy of the PHI.
  - Poses a significant risk of financial, reputational, or other harm to the individual (i.e., Harm Standard).
- **Final Rule:** An impermissible use or disclosure of PHI 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 or an exception applies.
New Risk Assessment Standard

- A CE or BA may only elect not to provide a breach notification if a full, objective analysis of certain enumerated factors, results in a demonstrable low probability that the PHI has been compromised.

- Risk assessments must include at least the following 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.

Discovery Of The Breach

- **When is a breach discovered?**
  - A breach is treated as discovered by a CE or BA as of the first day on which an employee, officer, or other agent of the CE or BA knows or should know by exercising “reasonable diligence” of the breach.

  - The “reasonable diligence” required is the care that would be expected from a person aiming to satisfy a legal requirement under similar circumstances.

    - Did the CE or BA take reasonable steps to learn of breaches?
    - Where there any indications of a breach that a person seeking to satisfy the rule would have investigated under similar circumstances?
Notification of Individuals

- CEs must notify individuals of a breach without unreasonable delay, but in no case later than 60 calendar days from the discovery of the breach.
  - Clock starts when the incident is first known; not when the investigation of the incident is complete.
  - Both actual written notice and substitute notice to affected individuals if contact information is insufficient or out-of-date.

  Substitute Notice:
  - For fewer than 10 individuals – Alternate form of written notice, telephone, or other means.
  - For 10 or more individuals – Conspicuous posting on the home page of the CE’s website or notice in major print or broadcast media in the geographic areas where the affected individuals reside, including a toll-free number where individuals can contact the CE.

Content of Notification

- A notice of breach must include the following information, to the extent possible:
  - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
  - A description of the types of unsecured PHI involved (such as whether full name, social security number, date of birth, home address, account number, diagnosis, types of treatment, disability code, or other information were involved);
  - Any steps individuals should take to protect themselves from potential harm resulting from the breach;
  - A brief description of what the CE involved is doing to investigate the breach, mitigate the harm to individuals, and to protect against any further breaches; and
  - Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an email address, website, or postal address.
Notification of Media

- Breach involving more than 500 individuals in any one state or jurisdiction:
  - Notification of a prominent media outlet serving the state or jurisdiction where the affected individuals reside.
  - Without unreasonable delay and not later than 60 calendar days after discovery of the breach.
  - Content of notification requirements apply.

Notification of HHS

- Breach involving fewer than 500 individuals:
  - CEs must notify HHS not later than 60 days after the end of the calendar year in which the breaches were “discovered” not in which the breach occurred.
  - CEs must still notify individuals promptly as required.

- Breach involving 500 or more individuals:
  - CEs must notify HHS of all breaches “immediately.”
    - Sent concurrently with notification to the individual – i.e., without unreasonable delay and not later than 60 calendar days from the discovery of the breach.
Notification By Business Associates

- **Notification of the CE**: BAs must notify CEs of a breach without unreasonable delay and **no later than 60 calendar days** from the discovery of the breach.

- **Discovery**: Breach is discovered as of the first day it is known to the BA or by exercising reasonable diligence would have known of the breach.

- **Content**: To the extent possible, the identification of the affected individuals and any other information the CE is required to provide in its notification.

Prohibition On The “Sale” Of PHI

- CEs and BAs are prohibited from receiving direct or indirect remuneration in exchange for the disclosure of PHI without authorization from the individual.
  - Applies to financial and nonfinancial benefits (e.g., in kind benefits).
  - The “sale” of PHI does not encompass payments a CE may receive in the form of grants or arrangements to perform programs or activities where the provision of PHI to the payer is a byproduct of the service being provided.

- **Exceptions**:
  - Public health purposes.
  - Research disclosures.
    - Remuneration must be a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes.
  - Disclosures for the transfer, merger, or consolidation of all or part of a CE with another CE, or an entity following such activity will become a CE, and related due diligence.
  - Activities paid by a CE to a BA performed on behalf of the CE.
Uses And Disclosures Of PHI For Marketing Purposes

**Before:**

- CEs must obtain a valid authorization from individuals before using or disclosing PHI to market a product or service to the individual.
- “Marketing” is making a communication about a product or service that encourages a person to purchase or use the product.
- Certain health-related communications were excluded from the marketing definition.

**Now:**

- Final Rule requires authorization for all treatment and health care operations communications where the CE receives financial remuneration (directly or indirectly) from a third party.
- Maintains certain exceptions involving remuneration:
  - Face-to-face communications
  - Refill reminders
- “Remuneration” only applies to financial payments.

Uses and Disclosures of PHI for Fundraising

**Before:**

- CEs are permitted to use or disclose to a BA or an institutionally related foundation certain PHI for the CE's fundraising from that individual without authorization.
- CE must notify individuals in its Notice of Privacy Practices that it may contact them to raise funds and how to opt out of such communications.

**Now:**

- With each fundraising communication, CEs must provide individuals with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications.
- A CE may not condition treatment or payment on the choice to receive fundraising communications.
- A CE may not make such communications to an individual who has opted out.
- A CE may provide individuals with an opportunity to opt back in.
### Right to Request Restrictions Of Uses And Disclosures

<table>
<thead>
<tr>
<th>Before:</th>
<th>Now:</th>
</tr>
</thead>
<tbody>
<tr>
<td>‣ CEs must allow individuals to request restrictions to the use and disclosure of their PHI for treatment, payment, and health care operation purposes, as well as for disclosures to family members.</td>
<td>‣ CEs must comply with an individual’s request to restrict disclosure of PHI to a health plan for the purpose of carrying out payment or health care operations and if the restriction applies to PHI that pertains <em>solely</em> to a health care item or service for which the health care provider has been paid out-of-pocket in full.</td>
</tr>
<tr>
<td>‣ CEs are not required to agree to such requests.</td>
<td></td>
</tr>
</tbody>
</table>

### Expansion Of Individuals’ Right To Access Electronic Health Information

<table>
<thead>
<tr>
<th>Before:</th>
<th>Now:</th>
</tr>
</thead>
<tbody>
<tr>
<td>‣ Individuals generally have a right to review or obtain copies of their PHI to the extent such information is maintained in a designated record set(s) of a CE.</td>
<td>‣ Upon request, CEs must provide an electronic copy of the individual’s electronically- maintained PHI in one or more designated record sets in the electronic form and format requested if it is readily producible or in a readable electronic form and format (e.g., PDF) as agreed to by the CE and the individual.</td>
</tr>
<tr>
<td></td>
<td>‣ If requested, a CE must transmit a copy to another person designated by the individual.</td>
</tr>
<tr>
<td></td>
<td>‣ Reasonable cost-based fee permitted.</td>
</tr>
<tr>
<td></td>
<td>‣ CEs have 30 days to comply with a one-time 30-day extension.</td>
</tr>
</tbody>
</table>
Protection Of PHI About Decedents

Before:

- CEs must protect the privacy of a decedent’s PHI in generally the same manner and to the same extent that is required for the PHI of a living individual.

Now:

- CEs are required to comply with the requirements of the Privacy Rule with regard to the PHI of a deceased individual up to 50 years from the date of death.
- Individually identifiable health information of a person who has been deceased for more than 50 years is no longer “PHI.”
- The new limitation under the Privacy Rule does not override or modify existing State or other laws that may afford longer privacy protections.

Protection Of PHI About Decedents (cont’d)

Before:

- CEs must protect the privacy of a decedent’s PHI in generally the same manner and to the same extent that is required for the PHI of a living individual.

Now:

- CEs are permitted to disclose a decedent’s PHI not only to a decedent’s personal representative, but also to family members and others who were involved in the care or payment for care of the decedent prior to death unless doing so is inconsistent with any prior expressed preference of the individual that is known to the CE.
- CEs must have “reasonable assurances” that the individual was involved in the care or payment for care of the decedent prior to death and is not required to make the disclosure if circumstances indicate otherwise.
Changes To The Notice Of Privacy Practices (NPP)

Before:
- Generally, CEs must have and distribute an NPP to individuals.
- NPPs describe the uses and disclosures of PHI a CE is permitted to make, the CE’s legal duties and privacy practices with respect to PHI, and the individual’s rights concerning PHI.
- NPPs are also subject to certain content and format requirements.

Now:
- NPPs must contain statements indicating that:
  - Most uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require authorization.
  - Other uses and disclosures not described in the NPP will be made only with authorization.
  - Individuals have the right to opt out of fundraising communications if a CE intends to contact an individual to raise funds for the CE.

Changes To The Notice Of Privacy Practices (NPP) (cont’d)

Before:
- Generally, CEs must have and distribute an NPP to individuals.
- NPPs describe the uses and disclosures of PHI a CE is permitted to make, the CE’s legal duties and privacy practices with respect to PHI, and the individual’s rights concerning PHI.
- NPPs are also subject to certain content and format requirements.

Now:
- Individuals have a new right to restrict certain disclosures of PHI to a health plan where the individual has paid out-of-pocket in full.
- Affected individuals have the right to be notified following a breach of unsecured PHI.
Distribution Of NPPs

- Health care providers are not subject to any new requirements for the distribution of revised NPPs.
  - Health care providers with direct treatment relationships with an individual must make available a revised NPP, upon request, on or after the date of revision and have the NPP at the delivery site posted in a clear and prominent location.
  - Providers are not required to print and hand out NPPs to all individuals seeking treatment. Providers are only required to provide copies of NPPs to, and obtain a good faith acknowledgement of receipt from, new patients.
  - To the extent that some CEs have already revised their NPPs in response to the HITECH changes or State law requirements, so long as individuals have been informed of all material changes to the NPP and the current NPP is consistent with the final rule, covered entities are not required to revise and distribute another NPP upon publication of the final rule.

Compliance Dates

- The final rule was effective on March 26, 2013.
- Adopts proposed 180-day compliance period, requiring compliance on September 23, 2013.
  - 180-day compliance period will also apply to future modifications to the HIPAA rules, unless otherwise specified.
- The 180-day period does not apply to:
  - Modifications to the Enforcement Rule, which were effective as of the final rule unless otherwise specified.
  - The Breach Notification Rule, which was effective on September 23, 2009. During the compliance period, CEs and BAs must comply with the requirements of the Interim Final Rule.
  - Provisions were HHS provides an alternate effective date:
    - CEs and BAs are permitted to operate under existing BA agreements for up to one year beyond the compliance date of the final rule unless the entities have renewed or modified their contract following the compliance date for the modifications.
Part II: HIPAA/HITECH Security

John DiMaggio, President, CEO of MCS2 Healthcare Security Solutions

HITECH Goals
• Government Involvement for Adoption
• Financial Incentives for Adoption
• Savings
• Strengthen Privacy & Security Laws

Recent Omnibus Modifications
• Business Associates
• Breach Reporting
• Enforcement
• Privacy
Needs

- Protect patient health information
- Prepare for audit or incident
- Comply with the HIPAA Security Rule
- Correct any compliance gaps
  - Cost effectively
  - Quickly
  - Prioritized manner
  - Best practices
- Maintain compliance

What Is At Stake?

<table>
<thead>
<tr>
<th>Civil Monetary Penalties</th>
<th>Other Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min. $50,000/violation</td>
<td>Legal</td>
</tr>
<tr>
<td>Max. $1,500,000/calendar year</td>
<td>Accelerated Remediation</td>
</tr>
<tr>
<td>Min. $10,000/violation</td>
<td>Public Relations</td>
</tr>
<tr>
<td>Max. $50,000/violation</td>
<td>Reputation</td>
</tr>
<tr>
<td>Max. $1,500,000/calendar year</td>
<td></td>
</tr>
</tbody>
</table>

Min. $10,000/violation
Max. $50,000/violation
Max. $1,500,000/calendar year

Min. $100/violation
Max. $50,000/violation
Max. $1,500,000/calendar year
### Enforcement

<table>
<thead>
<tr>
<th>Office for Civil Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Compliance Investigations</td>
</tr>
<tr>
<td>• HIPAA Audits</td>
</tr>
<tr>
<td>Department of Justice</td>
</tr>
<tr>
<td>• Criminal Prosecution</td>
</tr>
<tr>
<td>State Attorney General</td>
</tr>
<tr>
<td>• Civil Actions</td>
</tr>
<tr>
<td>Dept. of Health &amp; Human Services</td>
</tr>
<tr>
<td>• Meaningful Use Attestation Audits</td>
</tr>
</tbody>
</table>

### What Do You Need?

- Current Risk Assessment
- Current Policies & Procedures, Documentation
- Active Risk Management Plan

![Risk Management Process Diagram](Diagram)
Risk Assessment

- “Look under all the rocks”
- Perform the assessment in a “compliant” and defensible manner
- Address each component of the regulations
- Show your work

Who Does It Impact?

- Security
- Compliance
- Legal
- Investors
- Auditors
- C-Suite
- Business Associates
- Customers
- I.T.
What Is Security? CIA

- Confidentiality
- Integrity
- Availability
- Electronic Protected Health Information (“e-PHI”)

How To Protect Information – Safeguards

Confidentiality Integrity Availability

- Physical
- Administrative
- Technical
Core Groups

- Access Control
- Security Awareness
- Contingency Planning
- Security Planning
- Personnel Security
- Risk Assessment
- Media Protection
- Physical and Environmental
- Transmission Integrity
- Identification and Authentication
- Audit and Accountability
- System Integrity
- System Maintenance

Core Elements

- Policy
- Procedures
- Documentation
- Technology
Laptops

- Access Control
- Security Awareness
- Contingency Planning
- Security Planning
- Personnel Security
- Risk Assessment
- Media Protection
- Physical and Environmental
- Transmission Integrity
- Identification and Authentication
- Audit and Accountability
- System Integrity
- System Maintenance

Policy Examples – Laptops

Purpose

To define and document procedures and controls that protect the integrity and confidentiality of PROTECTED information stored on digital media in accordance with HIPAA Security 45 CFR 164.308(a)(3)(ii)(A), 164.310(c), 164.310(d)(1), 164.310(d)(2)(i-iv) and 164.312(c)(1).

Policy

Appropriate procedures and controls shall be established and implemented to prevent unauthorized access to PROTECTED information stored on Digital Media. Media Protection controls and procedures shall be regularly reviewed for appropriateness and effectiveness.
Procedure Examples – Laptops

Digital Media Access
ORGANIZATION shall restrict access to Digital Media containing PROTECTED information.

All Portable Digital Media containing PROTECTED information must be authorized and approved by Information Services (IS).

IS shall establish and maintain a list of all Portable Digital Media containing PROTECTED information. The documentation shall specify the type of media, individuals authorized to access the media, and measures taken to restrict unauthorized access.

All portable Digital Media containing PROTECTED information shall be identified with appropriate human readable markings, if technically feasible, unless the media is confined to controlled areas.

Portable Digital Media
All portable Digital Media containing PROTECTED information must be authorized and approved by the IS department.

All portable Digital Media containing PROTECTED information must be encrypted.

Mobile & Portable Device Security
ORGANIZATION information systems shall implement appropriate security measures for mobile and portable devices (e.g. laptops, tablets, smart phones) that access ORGANIZATION information systems.

Technology – Laptops

Encryption
Approved Devices
Business Associates

- Who
- What
- Agreements
- Current

HIPAA Audits

- History
- Process
- What they want
Where Does Security Fit Inside Your Organization?

Who Owns it?

- I.T.
- Compliance
- Legal

Summary

- Perform a Comprehensive Risk Assessment
- Develop a Plan
- Manage the Plan
- Repeat
- Be Practical
Part III: Enforcement & Compliance

Marcia Augsburger, Partner, DLA Piper, LLP (US)
January 17, 2013. The Department of Health and Human Services, through OCR, issued the final rule modifying HIPAA, HITECH, and GINA to strengthen the privacy and security protection for individuals’ health information and make certain other modifications to improve their workability and effectiveness and to increase flexibility for and decrease burden on the regulated entities.

2011–2012: Increased Enforcement Activity

- First Civil Monetary Penalty Imposed
- 7 Resolution Agreements
January, 2013:

OCR reached agreement with Hospice of Northern Idaho, which suffered theft of unencrypted laptop containing PHI on less than 500 patients (i.e., CE could maintain a breach log and only report to the Secretary annually.

OCR faulted Hospice for failing to conduct risk analysis and for lacking policies or procedures to address mobile device security as required by HIPAA.

Hospice was fined $50,000 and entered a 2-year corrective action plan.

Cleaning up from a HIPAA breach costs an organization $2.4 m. If, like most hospitals, the organization has an average profit margin or operating income of 2.5%, it will take $96m to replace that revenue.
Early Findings From Pilot Project

- Lack of Risk Assessments
- “Privacy challenges widely dispersed”
- Failure of the organization to prioritize HIPAA compliance
- Policies and procedures (not having them, not following them)

Above All: RISK ASSESSMENTS.
- **Privacy Rule Requirements:**
  - Notice of Privacy Practices
  - Rights to request privacy protection for PHI
  - Access of individuals to PHI
  - Administrative requirements
  - Uses and disclosures of PHI
  - Amendment to PHI
  - Accounting of Disclosures
- **Security Rule Requirements**
- **Breach Notification Rule Requirements**
HHS-OIG 2008 Report:

“Our ongoing audits of various hospitals nationwide indicate that CMS needs to become proactive in overseeing and enforcing implementation of the HIPAA Security rule by focusing on compliance reviews. Preliminary results of these audits show numerous, significant vulnerabilities in the systems and controls intended to protect ePHI at covered entities.”

---

Unfortunately, workers are the “weakest link.”
Social Sciences Experiments at United Health Services, Cleveland Clinic and Kaiser Foundation Health Plan

- E-mails with virus
- Guy posing as IT guy
- CD that workers couldn’t resist installing

Preparing Employees For On-Site Visits By Regulators

1. DON’T PANIC!
2. Don’t borrow trouble.
3. Identify what needs to be done immediately upon receipt of the audit demand and act without hesitation.
   - Contact company’s compliance officer and in-house or outside counsel;
   - Identify involved staff and alert them to what’s coming in a calm, non-accusatory way (with counsel’s involvement).
4. Identify the proper lead spokesperson (Privacy Officer?) and support personnel, including IT spokesperson (Security Officer?) and define their roles.

5. Accustom staff and yourself to copying counsel on all communications and having counsel attend all major meetings.

6. Work with leadership/management to insure resources are available to devote necessary time and attention to the investigation.

7. Meet with all involved staff to identify and resolve all concerns in advance.
   - Stop, Look, and Listen – especially Listen
   - Ask
   - Plan
   - Execute

8. Spend time creating a polished presentation.
The more you look like you have your act together the more you are perceived to have it together.

Effectiveness is questionable: The most common cause of a breach is insider negligence (46%), such as loss of a laptop or thumbdrive with PHI by an employee.

Action Item: CEs must modify and redistribute their notices of privacy practices.

Action Item: CEs, BAs, and Sub–BAs must develop a risk assessment tool that incorporates the new 4 part “breach” test.

Action Item: CEs, BAs, and Sub–BAs must re-train their employees and focus more on mobile devices.
What Causes Most Breaches And How Do You Stop Them?

<table>
<thead>
<tr>
<th>What Causes Them?</th>
<th>What Prevents Them?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Study Says:</td>
<td>Study Says:</td>
</tr>
<tr>
<td>Employee Negligence (46%)</td>
<td>Evaluate Privacy Controls</td>
</tr>
<tr>
<td>Employee Mistakes (42%)</td>
<td>Control devices</td>
</tr>
<tr>
<td>Criminal Attacks (33%)</td>
<td>Employee Training</td>
</tr>
</tbody>
</table>

Potential Criminal Liability Relating To Federal Audits

When A Deficiency Is Found During An Audit

What you should do:
- Contact legal counsel
- Under cover of legal privilege:
  - Correct the deficiency and develop evidence of cure/mitigation
  - Obtain evidence about consequences /lack thereof
- Assess the seriousness
- Prepare response

What you should NOT do:
- Panic
- Wait
- Cover up/Obstruct

Violation Found: Outcomes

- Door # 1: Voluntary Compliance
- Door # 2: Settlement: Resolution Agreement CAP Monitor
- Door # 3: Civil Monetary Penalty
#2: Resolution Agreements

- Increasingly common
- Settlement agreement between OCR and CE
- Does not include:
  - Findings of fact
  - Finding of violation
  - Admission of guilt
- Generally includes Corrective Action Plan
- Usually includes Settlement Payment
- Typically 3 year duration

#3: Civil Monetary Penalty (CMP)

- HITECH significantly increased civil monetary penalties that OCR can impose and set min/max based on state of mind / culpability.
- $ ranges based on the level of culpability (tier);
- Calculated per violation, per day, with annual maximum.
Penalties Under The Final Rule

<table>
<thead>
<tr>
<th>Categories of Violators and Respective Penalty Amounts Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violation category</td>
</tr>
<tr>
<td>Did Not Know</td>
</tr>
<tr>
<td>Reasonable Cause</td>
</tr>
<tr>
<td>Willful Neglect—Corrected</td>
</tr>
<tr>
<td>Willful Neglect—Not Corrected</td>
</tr>
</tbody>
</table>

Affirmative Defenses

Violation occurred pre–2/18/09
- Entity did not know, and by exercising reasonable diligence would not have known, of the violation
- Failure to comply is due to reasonable cause and not willful neglect, and entity corrects within 30 days of actual notice of date should have known (OCR can extend)
- Offense is punishable by criminal sanction

Violation occurred post–2/18/09
- Failure to comply is not due to willful neglect and entity corrects within 30 day period after actual notice or date should have known (OCR can extend)
- Offense is punishable by criminal sanction (for violations after 2/17/11 HIPAA criminal penalty was imposed)
The Appeal Process

Notice of Determination → 90 days → Request ALJ Hearing → ALJ Decision

Appeal to HHS Departmental Appeals Board → 60 days → Appeal to US Court of Appeals

Thank you!
If you have any questions, please do not hesitate to contact us.

- Marcia Augsburger
  DLA Piper LLP (US)
  400 Capitol Mall
  Suite 2400
  Sacramento, CA 95814-4428
  Phone: 916–930–3255
  Email: marcia.augsburger@dlapiper.com

- John DiMaggio
  MCS2 Healthcare Security Solutions
  8704 Cotter Street
  Lewis Center, OH 43035
  Phone: 614–270–9623
  Email: john.dimaggio@mcs2solutions.com

- Tiffani V. Williams
  DLA Piper LLP (US)
  500 8th Street N.W.
  Washington, DC 20004
  Phone: 202–799–4320
  Email: tiffani.williams@dlapiper.com