Preventing a Breach:

*Lessons Learned from OCR Resolution Agreements*

Sara M. Goldstein, Esq., General Counsel
Legal Disclaimer

• Nothing in this presentation should be considered to be, was intended to be, or should be used as, legal advice. This PowerPoint is designed to provide general information and should not be used as a substitute for professional service or advice in any specific situations. Since I am not your attorney, I cannot give you legal advice. Please consult your facility’s legal counsel if you have questions.
Preventing a Breach:

*Lessons Learned from Recent OCR Resolution Agreements*

**Agenda:**

1. HIPAA Enforcement – *Background*
2. OCR Enforcement Results
3. Resolution Agreements / Civil Monetary Penalties
4. Top HIPAA Privacy and Security Rule Compliance Issues
5. Examples of these Issues in Resolution Agreements / Civil Monetary Penalties
6. Lessons Learned from Resolution Agreements / Civil Monetary Penalties
7. Potential Problems on the Horizon
8. Closing Remarks
MRO Overview

- 2nd Largest ROI Provider
- 3,700 Locations
- 98% Client Retention
- 20% Growth
- #1 KLAS
- 2002
- 2013 – 2014
  - 2015/2016

Copyright © MRO Corporation 2016
HIPAA Enforcement

Through the Health Insurance Portability and Accountability Act (HIPAA), the HHS Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy, Security, and Breach Notification Rules and it does so in several ways:

– Investigates complaints filed with it,

– Conducts compliance reviews of Covered Entities;

– Performs education and outreach to foster compliance with the HIPAA Privacy, Security, and Breach Notification Rules’ requirements, and

– Works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA
HIPAA Enforcement

• Complaint - 45 CFR §160.306(a)-(b)
  – Can be filed with the Secretary of HHS by anyone who feels that a Covered Entity (CE) or Business Associate (BA) violated theirs or someone’s else’s health information privacy rights or committed another violation of the HIPAA Privacy, Security, or Breach Notification Rules

• Breach - 45 CFR §164.402
  – an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the Protected Health Information (PHI)

<table>
<thead>
<tr>
<th>Previously (Pre-Final Omnibus Rule)</th>
<th>Currently (Post-Final Omnibus Rule)</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to determine whether an impermissible use or disclosure of PHI constitutes a Breach …</td>
<td>The impermissible use or disclosure of PHI is a Breach if such use or disclosure poses a significant risk of financial, reputational, or other harm to the individual.</td>
</tr>
</tbody>
</table>

Sources: 45 CFR §§ 160.300 – 160.316; 164.400–414
http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Copyright © MRO Corporation 2016
HIPAA Enforcement
Privacy & Security Rule Complaint Process

**Complaint**
- Possible Criminal Violation

**Intake & Review**

**Possible HIPAA Privacy or Security Rule Violation**

**Investigation**

**Resolution**
- The violation did not occur after April 14, 2003
- Entity is not covered by the HIPAA Privacy Rule
- Complaint not filed within 180 days and an extension was not granted
- The incident described in the complaint does not violate the HIPAA Privacy Rule

**Resolution**
- OCR finds no violation
- OCR obtains voluntary compliance, corrective action, or other agreement
- OCR issues formal finding of violation

HIPAA Enforcement
How Breaches lead to OCR Investigations

- If an impermissible use of disclosure of PHI is determined to be a Breach, CEs must provide notification of the Breach to affected individuals, the Secretary of HHS (The Secretary), state entities (under applicable state law) and, in certain circumstances, to the media

<table>
<thead>
<tr>
<th>Breach Notification Timeline Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach Type</td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td>If Breach affects &lt; 500 individuals</td>
</tr>
<tr>
<td>If Breach affects &gt; 500 individuals</td>
</tr>
</tbody>
</table>

Sources:
45 CFR §§ 164.400-414
http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
Resolution of Complaints / Investigations

If the evidence indicates that the CE was not in compliance, OCR will attempt to resolve the case by obtaining one or more of the following:

– Voluntary Compliance
– Corrective Action
– Resolution Agreement
– Civil Money Penalties (CMPs)

Sources:
45 CFR §§ 160.300 – 160.426
OCR Enforcement Results

• OCR has received over **128,937** complaints
  
  – **75,705** were deemed ineligible for OCR investigation
  – **24,126** led to OCR investigations which resulted in corrective actions
  – **12,505** resulted in OCR intervention and the provision of technical assistance, without the need for an investigation
  – **10,955** investigations found no violations
  – ~**866** led to OCR compliance reviews
  
  – **31** resulted in the application of corrective measures that included payment of a resolution amount in lieu of civil money penalties
    • **$32,164,200**
  – **2** resulted in the assessment of CMPs
    • **$4,539,800**

Sources:
http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html
## Resolution Agreements / CMPs

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity</th>
<th>Resolution Amount</th>
<th>CMPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/17/2016</td>
<td>Feinstein Institute for Medical Research</td>
<td>$3,900,000</td>
<td></td>
</tr>
<tr>
<td>3/16/2016</td>
<td>North Memorial Health Care</td>
<td>$1,550,000</td>
<td></td>
</tr>
<tr>
<td>2/16/2016</td>
<td>P.T., Pool &amp; Land Physical Therapy, Inc.</td>
<td>$25,000</td>
<td></td>
</tr>
<tr>
<td>2/3/2016</td>
<td>Lincare, Inc.</td>
<td></td>
<td>$239,800</td>
</tr>
<tr>
<td>12/14/2015</td>
<td>The University of Washington Medicine</td>
<td>$750,000</td>
<td></td>
</tr>
<tr>
<td>11/30/2015</td>
<td>Triple-S Management Corporation</td>
<td>$3,500,000</td>
<td></td>
</tr>
<tr>
<td>11/24/2015</td>
<td>Lahey Hospital and Medical Center</td>
<td>$850,000</td>
<td></td>
</tr>
<tr>
<td>8/31/2015</td>
<td>Cancer Care Group, P.C.</td>
<td>$750,000</td>
<td></td>
</tr>
<tr>
<td>6/10/2015</td>
<td>St. Elizabeth’s Medical Center</td>
<td>$218,400</td>
<td></td>
</tr>
<tr>
<td>4/22/2015</td>
<td>Cornell Prescription Pharmacy</td>
<td>$125,000</td>
<td></td>
</tr>
<tr>
<td>12/2/2014</td>
<td>Anchorage Community Mental Health Services</td>
<td>$150,000</td>
<td></td>
</tr>
<tr>
<td>6/23/2014</td>
<td>Parkview Health System, Inc.</td>
<td>$800,000</td>
<td></td>
</tr>
<tr>
<td>5/7/2014</td>
<td>New York and Presbyterian Hospital and Columbia University</td>
<td>$4,800,000</td>
<td></td>
</tr>
<tr>
<td>4/22/2014</td>
<td>Concentra Health Services</td>
<td>$1,725,220</td>
<td></td>
</tr>
<tr>
<td>4/22/2014</td>
<td>QCA Health Plan, Inc.</td>
<td>$250,000</td>
<td></td>
</tr>
<tr>
<td>3/7/2014</td>
<td>Skagit County, Washington</td>
<td>$215,000</td>
<td></td>
</tr>
<tr>
<td>12/20/2013</td>
<td>Adult &amp; Pediatric Dermatology, P.C.</td>
<td>$150,000</td>
<td></td>
</tr>
<tr>
<td>8/14/2013</td>
<td>Affinity Health Plan, Inc.</td>
<td>$1,215,780</td>
<td></td>
</tr>
<tr>
<td>7/11/2013</td>
<td>WellPoint</td>
<td>$1,700,000</td>
<td></td>
</tr>
<tr>
<td>6/13/2013</td>
<td>Shasta Regional Medical Center</td>
<td>$275,000</td>
<td></td>
</tr>
<tr>
<td>5/23/2013</td>
<td>Idaho State University</td>
<td>$400,000</td>
<td></td>
</tr>
<tr>
<td>12/31/2012</td>
<td>Hospice of Northern Idaho</td>
<td>$50,000</td>
<td></td>
</tr>
<tr>
<td>9/17/2012</td>
<td>Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc.</td>
<td>$1,500,000</td>
<td></td>
</tr>
<tr>
<td>6/26/2012</td>
<td>Alaska DHSS</td>
<td>$1,700,000</td>
<td></td>
</tr>
<tr>
<td>4/13/2012</td>
<td>Phoenix Cardiac Surgery</td>
<td>$100,000</td>
<td></td>
</tr>
<tr>
<td>3/13/2012</td>
<td>BCBST</td>
<td>$1,500,000</td>
<td></td>
</tr>
<tr>
<td>7/6/2011</td>
<td>UCLA Health System</td>
<td>$865,500</td>
<td></td>
</tr>
<tr>
<td>2/14/2011</td>
<td>General Hospital Corporation and Massachusetts General Physicians Organization, Inc.</td>
<td>$1,000,000</td>
<td></td>
</tr>
<tr>
<td>2/4/2011</td>
<td>Cignent Health of Prince George’s County</td>
<td></td>
<td>$4,300,000</td>
</tr>
<tr>
<td>12/3/2010</td>
<td>Management Services Organization Washington, Inc.</td>
<td>$35,000</td>
<td></td>
</tr>
<tr>
<td>7/27/2010</td>
<td>Rite Aid Corporation</td>
<td>$1,000,000</td>
<td></td>
</tr>
<tr>
<td>1/16/2009</td>
<td>CVS Pharmacy, Inc.</td>
<td>$2,250,000</td>
<td></td>
</tr>
<tr>
<td>7/16/2008</td>
<td>Providence Health &amp; Services</td>
<td>$100,000</td>
<td></td>
</tr>
</tbody>
</table>

Breaking News …

- April 20, 2016
  - $750,000 Resolution Payment
  - Raleigh Orthopedic Clinic
    - April 2013 – Breach of impermissible disclosure of x-ray films for over 17,300 patients to a third party pursuant to an oral arrangement for the vendor to harvest the silver from the films in exchange for transferring the x-rays to electronic media
    - No BAA in place with third party
Resolution Agreements / CMPs

How did these come about?

- Breach Reports
- Complaints
- Media Reports
- Referrals from other Government Agencies
Top HIPAA Privacy and Security Rule Compliance Issues

1. Impermissible uses and disclosures of PHI,
2. Lack of physical and technical safeguards of PHI,
3. Use or disclosure of more than the “minimum necessary” PHI, and
4. Lack of administrative safeguards of electronic PHI (ePHI)
4. Lack of Administrative Safeguards of ePHI
Administrative Safeguards – 45 CFR §164.308

• Administrative actions, policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the CE's or BA's workforce in relation to the protection of that information.

• There are 13 administrative safeguards
  – comprise over half of the HIPAA Security requirements

<table>
<thead>
<tr>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Management Process</strong></td>
</tr>
<tr>
<td>45 CFR § 164.308(a)(1)(ii)(A)</td>
</tr>
<tr>
<td><strong>Security Awareness and Training</strong></td>
</tr>
<tr>
<td>45 CFR § 164.308(a)(5)(i)</td>
</tr>
<tr>
<td><strong>Evaluation</strong></td>
</tr>
<tr>
<td>45 CFR § 164.308(a)(8)</td>
</tr>
<tr>
<td><strong>Risk Analysis</strong></td>
</tr>
<tr>
<td>Conduct 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.</td>
</tr>
<tr>
<td><strong>Access Authorization</strong></td>
</tr>
<tr>
<td>Implement P&amp;Ps for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism</td>
</tr>
<tr>
<td><strong>Evaluation</strong></td>
</tr>
<tr>
<td>Perform a periodic technical and nontechnical evaluation, based initially upon the standards listed in the Security Rule, in response to environmental or operations changes affecting the security of ePHI, that establishes the extent to which an entity’s security policies and procedures meet the requirements of the Security Rule.</td>
</tr>
</tbody>
</table>
Example of Where CE did not have the Proper Administrative Safeguards in Place

Feinstein Institute for Medical Research (3/17/16)

- Breach report filed with the Secretary indicated that a laptop computer containing the ePHI of approximately 13,000 patients and research participants was stolen from an employee’s car.
- OCR launched and investigation and determined that the CE failed to:
  - Conduct an accurate and thorough risk analysis of its ePHI § 164.308(a)(1)(ii)(A)
  - Implement P&Ps for granting access to ePHI by its workforce members § 164.308(a)(4)(ii)(B)

Resolution Amount Paid: $3,900,000

Of the 33 Resolution Agreements/CMPs, more than 10 CEs were cited for not conducting a proper risk analysis.

Lesson Learned:
Having Administrative Safeguards in Place can Help to Prevent a Breach

Conduct a Risk Analysis … and follow it up with Risk Management

Risk Analysis
1. The scope of the Risk Analysis is key
2. Document *where* ePHI is stored, received, maintained or transmitted
3. Identify and document potential threats and vulnerabilities
4. Document how well your current security measures address the potential threats and vulnerabilities
5. Determine the likelihood of threat occurrence, the threat’s level of risk, and the potential impact of such an occurrence
6. Identify next steps that need to be taken to mitigate risk

Risk Management
The actual implementation of security measures to sufficiently reduce an organization’s risk of losing or compromising its ePHI and to meet the general security standards
Lesson Learned:
Having Administrative Safeguards in Place can Help to Prevent a Breach

• Helpful Tools:


    • Updated tools is due out any day now!

3. Use or Disclosure of More than the “Minimum Necessary” PHI
The “Minimum Necessary Rule”
45 CFR §§ 164.502(b), 164.514(d)

• CEs and BAs must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use of disclosure
  – Example: a CE may not use or disclose the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose
Example of Where CE did not follow the “Minimum Necessary Rule”

Triple-S Management Corporation
(3/17/16)

• Breach report filed with the Secretary stated that former employees had accessed restricted database containing ePHI because their access rights had not been terminated

• OCR launched and investigation and determined that the CE (among other things):
  – Disclosed more PHI than was necessary to accomplish the purpose for which it had hired the outside vendor § 164.514(d)

Resolution Amount Paid: $3,500,000

Violating the “Minimum Necessary Rule” can have serious implications for CEs and BAs beyond OCR Enforcement Actions!

Lesson Learned:
Following the “Minimum Necessary Rule” is Crucial to Preventing a Breach

• Better management of Release of Information (ROI) processes is essential:
  – Consider working with a provider of disclosure management services If ROI is conducted in-house, proper training for employees is critical

• Consider conducting “Minimum Necessary Rule” Audits
  – Audit of Role-Based Access to PHI
    • Identify workforce members who need PHI access
    • Identify what information can be accessed
    • Limit access
  – Audit of User Access
    • Same last name search
    • Staff accessing their own records
    • Staff accessing records of VIPs, Facility Executives

• Helpful Tool: HHS Guidance on the Minimum Necessary Requirement:
2. Lack of Physical and Technical Safeguards of PHI
<table>
<thead>
<tr>
<th>Physical Safeguards 45 CFR § 164.310</th>
<th>Technical Safeguards 45 CFR § 164.312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical measures and P&amp;Ps to protect a CE’s or BA's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion</td>
<td>Technology and the policy and procedures for its use that protect ePHI and control access to it.</td>
</tr>
</tbody>
</table>

**Physical Safeguards 45 CFR § 164.310**
- Facility Access Controls 164.310(a)(1)
  - Contingency Operations
  - Facility Security Plan
  - Access Control and Validation Procedures
  - Maintenance Records
- Workstation Use 164.310(b)
- Workstation Security 164.310(c)
- Device and Media Controls 164.310(d)(1)
  - Disposal
  - Media Re-Use
  - Accountability
  - Data Backup and Storage

**Technical Safeguards 45 CFR § 164.312**
- Access Control 164.312(a)(1)
  - Unique User Identification
  - Emergency Access Procedure
  - Automatic Logoff
  - Encryption and Decryption
- Audit Controls 164.312(b)
- Integrity 164.312(c)(1)
  - Mechanism to Authenticate ePHI
- Person or Entity Authentication 164.312(d)
- Transmission Security 164.312(e)(1)
  - Integrity Controls
  - Encryption
Examples of Where CEs did not have the Proper Physical and Technical Safeguards in Place

<table>
<thead>
<tr>
<th>Company</th>
<th>Date</th>
<th>Violation Details</th>
<th>CMP</th>
<th>Resolution Payment</th>
</tr>
</thead>
</table>
| Lincare, Inc.                  | (2/3/16)      | • Employee left behind documents containing PHI of 278 patients after moving  
• CE had inadequate P&Ps in place to safeguard patient information that was taken offsite                                                                                       | $239,800 | $750,000           |
| Cancer Care Group, P.C.        | (8/31/15)     | • Laptop bag stolen from an employee’s car contained a computer and unencrypted backup media, which contained PHI of ~55,000 current and former patients  
• No written policy specific to the removal of hardware and electronic media containing ePHI into and out of its facilities, even though this was common practice |       |                    |
| BCBST                          | (3/13/12)     | • 57 unencrypted computer hard drives were stolen from a leased facility that contained PHI of over 1 million individuals  
• CE failed to implement appropriate physical safeguards by not having adequate facility access controls                                                                 | $1,500,000 |                    |
| Anchorage Community Mental Health Services | (12/2/2014) | • Breach of unsecured ePHI affecting 2,743 individuals due to malware  
• CE failed to implement technical security measures to guard against unauthorized access to ePHI that is transmitted electronically by failing to ensure that firewalls were in place with threat identification monitoring of inbound and outbound traffic and that information technology resources were both supported and regularly updated with available patches |     | $150,000           |

Lesson Learned:
Having Physical and Technical Safeguards in Place is Key to Preventing a Breach

• Use the HIPAA Administrative Simplification Table of Contents as your guide to ensuring that your HIPAA P&Ps address all of the appropriate safeguards
  – Not only is this helpful for creating/updating the P&Ps, it makes conducting risk analyses and potential audits easier because you can crosswalk your P&Ps to the regulations

• Don’t just create the P&Ps, educate your workforce and enforce them
  – Training of workforce members who use or disclose PHI should be provided on an on-going basis

• Make sure that your privacy and security folks are working hand-in-hand to create and implement P&Ps

• Helpful Tools:
1. Impermissible Uses and Disclosures of PHI
# HIPAA: Use and Disclosure of PHI

<table>
<thead>
<tr>
<th>Required Disclosures</th>
<th>Permitted Disclosures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>45 CFR 164.502(a)(2)(i)-(ii)</strong></td>
<td><strong>45 CFR 164.512(a)-(l)</strong></td>
</tr>
<tr>
<td>CEs are required to disclose PHI to:</td>
<td>A CE is permitted to use or disclose PHI as follows:</td>
</tr>
<tr>
<td>1. Individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI; and</td>
<td>1. Treatment, payment, and health care operations</td>
</tr>
<tr>
<td>1. To HHS when it is undertaking a compliance investigation or review, or enforcement action</td>
<td>2. For facility directories (with an opportunity to agree/object)</td>
</tr>
<tr>
<td></td>
<td>3. For notification and other purposes (with an opportunity to agree/object)</td>
</tr>
<tr>
<td></td>
<td>4. Incident to an otherwise permitted use and disclosure</td>
</tr>
<tr>
<td></td>
<td>5. Public interest and benefit activities</td>
</tr>
<tr>
<td></td>
<td>• Required by law</td>
</tr>
<tr>
<td></td>
<td>• Public health activities</td>
</tr>
<tr>
<td></td>
<td>• Victims of abuse, neglect or domestic violence</td>
</tr>
<tr>
<td></td>
<td>• Health oversight activities</td>
</tr>
<tr>
<td></td>
<td>• Judicial and administrative proceedings</td>
</tr>
<tr>
<td></td>
<td>• Law enforcement purposes</td>
</tr>
<tr>
<td></td>
<td>6. Decedents;</td>
</tr>
<tr>
<td></td>
<td>7. Limited data set for the purposes of research, public health or health care operations</td>
</tr>
</tbody>
</table>

**Breach - 45 CFR §164.402**

An impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of PHI
Examples of Where CEs Used or Disclosed PHI Improperly

<table>
<thead>
<tr>
<th>Company</th>
<th>Date</th>
<th>Explanation</th>
<th>Resolution Payment</th>
</tr>
</thead>
<tbody>
<tr>
<td>P.T., Pool &amp; Land Physical Therapy, Inc.</td>
<td>2/16/16</td>
<td>CE impermissibly disclosed numerous individuals’ PHI when it posted patient testimonials, including full names and photos, to its website without obtaining valid, HIPAA-compliant authorizations</td>
<td>$25,000</td>
</tr>
<tr>
<td>Shasta Regional Medical Center</td>
<td>6/13/13</td>
<td>In response to a California Watch investigation into CE’s billing practices, which reported that the CE had billed for treating a patient for a severe form of malnutrition (even though the patient was overweight and indicated she received no such treatment), CE executives released the patient’s PHI to several media outlets, claiming that the patient “waived” her privacy rights when she discussed her care with the media.</td>
<td>$275,000</td>
</tr>
<tr>
<td>Management Services Organization Washington, Inc.</td>
<td>12/13/10</td>
<td>CE impermissibly disclosed ePHI for marketing purposes without patient authorizations</td>
<td>$35,000</td>
</tr>
<tr>
<td>UCLA</td>
<td>7/6/2011</td>
<td>Workforce members impermissibly examined the ePHI of celebrity patients. CE did not provide nor document the provision of necessary and appropriate Privacy and/or Security Rule training for all workforce members. CE failed to apply appropriate sanctions on workforce members who impermissibly examined ePHI. CEs failed to implement security measures sufficient to reduce the risks of impermissible access to ePHI by unauthorized users.</td>
<td>$865,500</td>
</tr>
</tbody>
</table>

Lesson Learned:
Implementing P&Ps, Training, and Technical Safeguards can Prevent Breaches

- Better management of Release of Information (ROI) processes is essential:
  - Consider working with a provider of disclosure management services
    - Cutting edge vendors are using Optical Character Recognition (OCR) software to prevent the disclosure of the wrong PHI
  - If ROI is conducted in-house, proper training for employees is critical

- Access Audits should be conducted regularly
  - Technology is available that monitors access and can notify you of improper access

- If you plan on using PHI for marketing, make sure you follow the rules:
  - 45 CFR § 164.508(a)(3)
    - CE must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:
      - a face-to-face communication made by a CE to an individual; or
      - a promotional gift of nominal value provided by the CE.
    - If the marketing involves financial remuneration, to the CE from a third party, the authorization must state that such remuneration is involved
Problems on the Horizon

• Malware/ Ransomware
  – “Hot topic” in the news
  – Training and procedures need to be put in place for workforce members
    • Examples:
      – The University of Washington Medicine (12/14/15)
      – Anchorage Community Mental Health Services (12/2/2014)

• BA Compliance with HIPAA
  – Due diligence is needed to ensure that BAs are compliant with HIPAA
    • Examples:
      – North Memorial Health Care (3/16/16)
      – Triple-S Management Corporation (11/30/15)

• The Cloud, Mobile Devices and Applications
  – Risk analysis should include details about where ePHI is being stored
  – Asset inventory should be conducted for mobile devices
    • Examples:
      – St. Elizabeth’s Medical Center (6/10/15) – New York and Presbyterian Hospital / Columbia University (5/7/14)
      – Adult & Pediatric Dermatology, P.C. (12/20/13) – Alaska DHSS (6/26/12) – QCA Health Plan, Inc. (4/22/14)
      – Hospice of Northern Idaho (12/31/12)
Closing Remarks

• Implement the Right Technologies
  – Encryption
    • “Safe Harbor” for encrypted PHI
  – Access Tracking Software
  – OCR Software

• Document how you implement your Compliance Program
  – P&Ps
  – Sanctions
  – Business Associate Agreements (BAAs)

• Train and Educate Your Workforce
  – More than 40% of Breaches are due to “unintentional employee negligence” which can be attributed to inconsistent organizational policies, processes not being followed, and uncertainty by staff with different levels of training and experience
Questions?

Sara M. Goldstein, Esq.
General Counsel
(P): 610-994-7500 x 472 | sgoldstein@mrocorp.com
https://www.linkedin.com/in/saragoldsteinesq