After the Breach:
Using the HITRUST CSF to Support the Massachusetts Eye and Ear Resolution Agreement and Corrective Action Plan

Heather Fowles, CISSP, CISA
Director of Information Security
Mass. Eye and Ear
Mass. Eye and Ear

- Small, independent nonprofit specialty hospital located in Boston focused on treatment of eye, ear, nose and throat conditions
- Principally ambulatory – over 90% of surgical cases performed on an outpatient basis
- Close clinical affiliation with Massachusetts General Hospital
- Harvard Medical School teaching affiliate for Ophthalmology and Otolaryngology
The Breach

- February 2010: unencrypted laptop stolen in from physician travelling overseas
- Contained database with Protected Health Information for approximately 3500 patients and research subjects
- April 2010: Mass. Eye and Ear reported the theft under the HITECH breach reporting rules
Investigation

- October 2010: US Dept. of Health and Human Services’ Office for Civil Rights (OCR) initiated investigation of Mass. Eye and Ear’s compliance with HIPAA Privacy, Security and Breach Notification rules
- Comprehensive data request
  - Facts related to investigation and mitigation of incident
  - Information reflective of HIPAA compliance generally
Resolution Agreement

- September 2012: Mass. Eye and Ear and OCR sign Resolution Agreement (RA)
  - No admission / No concession
  - 3-year Corrective Action Plan (CAP)
  - Six areas of “Covered Conduct”
  - $1.5M to OCR

**Covered Conduct**

- Risk Assessment
- Security Measures for Portable Devices
- Incident Identification & Response
- Access Control - Portable Devices
- Inventory - Portable Devices (Incl. BYOD)
- Encryption of Portable Devices
CAP Requirements

- Revise information security policies and procedures (subject to OCR approval)
  - 10 minimum content requirements
- Re-train workforce
- Engage independent monitor to oversee compliance for three years
- Implement additional controls particularly around portable devices
RA/CAP Lessons

- Stolen laptop prompted the OCR’s investigation, but broader concerns drove the RA and CAP
  - Policies and procedures
  - Risk assessment
  - Long view – from compliance date of HIPAA Security Rule until 2009-2010
HITRUST CSF

- Adopted by Mass. Eye and Ear in March 2013
  - Referenced by OCR (along with other frameworks) as resource for risk assessment*
  - Acceptable to Mass. Eye and Ear’s Monitor, PwC
  - Comprehensive
  - Healthcare / HIPAA focus
  - Benchmarking

- Basis for HIPAA Risk Assessment
- Basis for Monitor’s “Monitor Plan”

Risk Assessment

- Annual process per Mass. Eye and Ear policy
- First cycle just completed
  - Questionnaire Q2 2013
  - HITRUST Report Q3 2013
  - Risk Acceptance or Remediation
    Recommendations Q4 2013
  - VP acceptance Q1 2014
  - Quarterly status updates
Monitor Plan

- Audit plan for scheduled and unannounced visits
  - Developed by Monitor, PwC, in collaboration with Mass. Eye and Ear
  - Subject to OCR approval
  - Intended to validate Mass. Eye and Ear compliance with CAP
  - Procedures to test specific obligations regarding policies and training
  - CSF controls leveraged to define and test Workforce Compliance with Mass. Eye and Ear policies and procedures

- One “yardstick” - CSF shared standard for internal and Monitor assessment
Monitor Plan Development

- Mapping exercise – CAP “Minimum Content” requirements to one or more CSF controls

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>01: Access Control Policy</td>
<td>An access control policy shall be established, documented, and reviewed based on business and security requirements for access.</td>
<td>Yes</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>01.1 Review of User Access Rights</td>
<td>All access rights shall be regularly reviewed by management via a formal documented process.</td>
<td>Yes</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>01.1 Password Use</td>
<td>Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the selection and use of passwords and security of equipment.</td>
<td>Yes</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>01.1 Unattended User Equipment</td>
<td>Users shall ensure that unattended equipment has appropriate protection.</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Monitor Plan Development

Twenty-five key CSF controls selected

Test procedures defined for each
Monitor Plan Development – Example

From CAP Minimum Content requirement #6

“Procedures that specify ...the physical attributes of the surroundings of a specific workstation or class of workstations that can access ePHI.”

Mass. Eye and Ear policy (from Acceptable Use of Portable Devices)

“While the Workforce member is present ...the Portable Device must be kept in the physical presence of the Workforce member, or when left unattended, stored in a locked office, locked drawer or locked closet, or physically secured via means such as a locking housing or cable.”

CSF control

Access Control - Unattended User Equipment: “Users shall ensure that unattended equipment has appropriate protection.”

Test Plan

Validate policy, currency and dissemination. Onsite inspections and interviews.
Conclusions

- Active HIPAA enforcement continues
  - OCR – investigation of complaints, reported breaches, audits
  - State Attorneys General now also in the mix
  - Small number of cases but significant fines

- Investigation may go beyond immediate circumstances of reported breach or complaint

- Adopting/implementing comprehensive risk framework
  - Identifies risks, may prevent issues
  - Satisfies regulatory requirements for risk assessment
  - Provides support for investigation response
Lessons Learned from OCR Audits, Mock Audits & Enforcements – 5 Things Every Health Care Company Needs to Know Now (and How the HITRUST Common Security Framework Can Help)

April 23, 2014 - HITRUST 2014
Introduction
# Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now
   i. Know the Rules and Areas of Non-Compliance
   ii. Know the Risks Specific to Your Organization
   iii. Know the Data and the Flows – Internal and External
   iv. Know Your Audit Process and Prepare
   v. Know the Roadmap Ahead and Be Self-Aware
Background

- **Statutory Basis.** HITECH Section 13411 requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards.

- **Audit Program.** To implement this mandate, OCR piloted a program and performed 115 audits of covered entities in 2012.

- **Goal and Objectives.** To improve covered entity and business associate compliance with the HIPAA standards
  
  - Examine mechanisms for compliance,
  - Identify best practices
  - Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
  - Encourage attention to compliance with HIPAA
Audit Protocols – 11 Modules

- The audit protocol is organized around 11 different modules.
- Provides established criteria, audit testing procedures, work paper reference and applicability.

1. Breach Notification

2. Administrative Safeguards
3. Physical Safeguards
4. Technical Safeguards

Privacy

5. Notice of Privacy Practices
6. Rights to Request Privacy
   Protection of PHI
7. Access of Individuals to PHI
8. Administrative Requirements
9. Uses and Disclosures of PHI
10. Amendment of PHI
11. Accounting of Disclosures
Enforcement - Over $30 Million in Resolution Agreements & Fines for Variety of Issues an Entities – Focus on Risk

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Amount</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concentra Health Services</td>
<td>$1,975,220</td>
<td>22-Apr-14</td>
</tr>
<tr>
<td>QCA Health Plan</td>
<td>$250,000</td>
<td>22-Apr-14</td>
</tr>
<tr>
<td>Skagit County Public Health Department</td>
<td>$215,000</td>
<td>7-Mar-14</td>
</tr>
<tr>
<td>Adult &amp; Pediatric Dermatology, P.C. of Massachusetts</td>
<td>$150,000</td>
<td>20-Dec-13</td>
</tr>
<tr>
<td>Affinity Health Plan</td>
<td>$1,215,780</td>
<td>14-Aug-13</td>
</tr>
<tr>
<td>WellPoint</td>
<td>$1,700,000</td>
<td>11-Jul-13</td>
</tr>
<tr>
<td>Shasta Regional Medical Center</td>
<td>$275,000</td>
<td>13-Jun-13</td>
</tr>
<tr>
<td>Idaho State University</td>
<td>$400,000</td>
<td>21-May-13</td>
</tr>
<tr>
<td>Hospice of North Idaho</td>
<td>$50,000</td>
<td>28-Dec-12</td>
</tr>
<tr>
<td>Massachusetts Eye and Ear Institute</td>
<td>$1,500,000</td>
<td>17-Sep-12</td>
</tr>
<tr>
<td>Alaska DHSS</td>
<td>$1,700,000</td>
<td>26-Jun-12</td>
</tr>
<tr>
<td>Phoenix Cardiac Surgery</td>
<td>$100,000</td>
<td>13-Apr-12</td>
</tr>
<tr>
<td>BCBS Tennessee</td>
<td>$1,500,000</td>
<td>13-Mar-12</td>
</tr>
<tr>
<td>UCLA Health System</td>
<td>$865,500</td>
<td>6-Jul-11</td>
</tr>
<tr>
<td>Massachusetts General Hospital</td>
<td>$1,000,000</td>
<td>14-Feb-11</td>
</tr>
<tr>
<td>Cignet Health</td>
<td>$4.3 Million</td>
<td>4-Feb-11</td>
</tr>
<tr>
<td>Management Services Organization of Washington</td>
<td>$35,000</td>
<td>13-Dec-10</td>
</tr>
<tr>
<td>Rite Aid Corporation</td>
<td>$1,000,000</td>
<td>27-Jul-10</td>
</tr>
<tr>
<td>CVS Pharmacy, Inc.</td>
<td>$2,250,000</td>
<td>16-Jan-09</td>
</tr>
</tbody>
</table>
What Has Been in the Sites of the OCR

Case Examples Organized by Covered Entity
- General Hospitals
- Health Care Providers
- Health Plans / HMOs
- Outpatient Facilities
- Pharmacies
- Private Practices

Case Examples Organized by Issue
- Access
- Authorizations
- Business Associates
- Conditioning Compliance with the Privacy Rule
- Confidential Communications
- Disclosures to Avert a Serious Threat to Health or Safety
- Impermissible Uses and Disclosures
- Minimum Necessary
- Notice
- Safeguards
Fortune Telling – What You Might See

- **Results of Audits.** Provide further insight into risks and vulnerabilities, non-compliance areas and best practices.

- **Revised Protocols.** Updated compliance protocols to be released. Likely updated for Omnibus Rule, revised risk areas, size and type of organization and risk-based approach.

- **Risk-Based Approach.** Prior audits were done on a strict compliance approach. Guidance as to how more of a risk-based approach will be utilized – different than existing healthcare use of “risk base.”

- **Potentially More Audits.** A new process and to be announced scale, emphasis and approach.

- **Continued Enforcement Emphasizing Risk Assessment.** To improve covered entity and business associate compliance with the HIPAA standards

- **New Round of Audits Announced:** The new audits will look little like the old. OCR conducting the audits itself; focusing on more high-risk areas; doing away with on-site visits (at least for the moment); and potentially integrating the audits into OCR's formal enforcement program.
Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now
   i. Know the Rules and Areas of Non-Compliance
   ii. Know the Risks Specific to Your Organization
   iii. Know the Data and the Flows – Internal and External
   iv. Know Your Audit Process and Prepare
   v. Know the Roadmap Ahead and Be Self-Aware
Preliminary Analysis Discussed by OCR

- **Common Privacy areas:**
  - Notice of Privacy Practices
  - Access of Individuals
  - Minimum Necessary
  - Authorizations

- **Common Security areas:**
  - Risk Analysis
  - Media movement and disposal
  - Audit controls and monitoring

- Policies and Procedures exist but are outdated or not implemented
- HIPAA compliance programs are not a priority
- Small providers are not in compliance
- Larger entities demonstrate security challenges
- Entities are not conducting Risk Assessments
- Entities are not managing third party risks
- Privacy challenges are widely dispersed throughout the protocol - no clear trends by entity type or size

- Common finding of lacking audit controls and monitoring (as well as other areas) can be addressed by HITRUST CSF.
Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now

   i. Know the Rules and Areas of Non-Compliance

   ii. Know the Risks Specific to Your Organization

   iii. Know the Data and the Flows – Internal and External

   iv. Know Your Audit Process and Prepare

   v. Know the Roadmap Ahead and Be Self-Aware
The Risk Landscape

Breach Data Composite for 2012 and 2013

- **Electronic 73%**
  - 185 Incidents
  - 7,796,953 individuals affected

- **Paper 20%**
  - 50 Incidents
  - 452,537 individuals affected

- **Other/Unknown 7%**
  - 18 Incidents
  - 324,516 individuals affected

Source: US Department of Health and Human Services Office for Civil Rights
Number of Individuals Impacted vs. Number of Breaches

- Number of Breaches Consistent
- Number of People Impacted Up

<table>
<thead>
<tr>
<th>Year</th>
<th>Breaches</th>
<th>Records Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-2011</td>
<td>374</td>
<td>11,090,462</td>
</tr>
<tr>
<td>2012-2013</td>
<td>350 (-6%)</td>
<td>6,865,379</td>
</tr>
</tbody>
</table>

Note: 57,000+ reports of breaches of under 500 individuals for September 2009 through May 31, 2012

Source: US Department of Health and Human Services Office for Civil Rights
## What Is The Greatest Risk to PHI & Other Regulated Data?

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile devices</td>
<td>69%</td>
</tr>
<tr>
<td>Cloud computing infrastructure</td>
<td>45%</td>
</tr>
<tr>
<td>Applications</td>
<td>33%</td>
</tr>
<tr>
<td>Network infrastructure</td>
<td>23%</td>
</tr>
<tr>
<td>Virtual computing environments</td>
<td>16%</td>
</tr>
<tr>
<td>Archives and backups</td>
<td>8%</td>
</tr>
<tr>
<td>Data center environment</td>
<td>5%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>

**Source:** Ponemon The Risk of Regulated Data ion Mobile Devices and in the Cloud (2014)
What Is Your Greatest Risk – How Do You Measure?

Source: US Department of Health and Human Services Office for Civil Rights
Portable Devices Over the Last 4 Years – Decreasing Risk?

Source: US Department of Health and Human Services Office for Civil Rights
Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now
   i. Know the Rules and Areas of Non-Compliance
   ii. Know the Risks Specific to Your Organization
   iii. Know the Data and the Flows – Internal and External
   iv. Know Your Audit Process and Prepare
   v. Know the Roadmap Ahead and Be Self-Aware
Revolution in HIT and New Healthcare Delivery Models

- **Health Information, IT and Sharing Revolutions.** Stimulus Bill provided funds driving healthcare information and analytics, but healthcare organizations go from 0 to 11 in IT maturity.

- **Care without Walls.** Healthcare using new channels and new technologies to deliver treatments – i.e. telemedicine, social media, care without walls.

- **New, but Vulnerable, Healthcare Ecosystem.** All the new data sharing and movement of data creates new capabilities and a broad set of new data privacy/security vulnerabilities.

- **More Vendors and Business Associates Needed to Enable and Support.** New business partners, business associates and independent contracts needed to deliver and host new healthcare delivery methods and new technologies.

- **New Cyber Threats Attacking Healthcare.** Many providers, payors, pharma, medical device and business associates have been the target of cyber attacks and incidents.
What Others Are Doing

- Assessing against CSF, certifying and/or requiring business associates to do so
- Data mapping, internal and external flows
- Data use and data element inventories
- Enhancing BAs with minimum security provisions, pre-contract assessments and post-contract audits
- Updating Incident response plans
- Enhancing access controls and access monitoring
- Building cyber capabilities
Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now
   i. Know the Rules and Areas of Non-Compliance
   ii. Know the Risks Specific to Your Organization
   iii. Know the Data and the Flows – Internal and External
   iv. Know Your Audit Process and Prepare
   v. Know the Risks Specific to Your Organization
So You Got a Letter . . . A Few Tips for Audit Success

Process

- **Prepare.** Many organizations conduct mock audits or other exercises to prepare and practice.

Documentation

- **Omnibus Rule Update.** Ensure that the documentation for Programs is reviewed and updated, as necessary, to comply with the new Omnibus Rule requirements. Continue to monitor communications from OCR for revisions to the Protocol based on Omnibus.

- **Mapping of Documentation.** Map policy documents to the specific areas of the document request list from OCR. This can be a cross walk to the CSF materials. The mapping document furnished along with Program documentation is helpful.

- **Include a Log of Revisions/Updates.** The policies and procedures can include a revision history at the end of each document that provides a log of each revision/update that was made over time.
So You Got a Letter . . . A Few Tips for Audit Success (cont.)

Interviews

- **Prepare Responses for 10 Key Topics.** We suggest focusing preparations and responses for, at a minimum, each topic below. CSF can be used to support each. Note, this is not an OCR list.

  1. Business Associates
  2. Training
  3. Sanctions
  4. Minimum Necessary Use
  5. Accounting for Disclosures
  6. Authorizations
  7. Incident Response
  8. Breach Tracking/Analysis/Notification
  9. Notice of Privacy Practices
  10. Physical Security

- **Pay Attention to Trends.** Watch (i) OCR trends and compliance protocol changes, (ii) common areas of non-compliance and (iii) areas of enforcements and breaches.
So You Got a Letter . . . A Few Tips for Audit Success (cont.)

Interviews

- **Tell the Story - Emphasize Strengths of the Plan Programs.** Identify in advance and stress a number of strengths and tools to promote culture of compliance and maturity to the OCR auditor -- (i) training, (ii) assessments for BAs; (iii) data sharing/governance programs; (iv) processes for obtaining authorizations and delivering NPPs; and (v) incident response.
  - Provide prepared responses and emphasize strengths early in discussion.
  - Use questions to discuss program approach, not limited confirmations.

- **Interview Responses Should Be Truthful, Direct, and Concise.** All questions from the OCR auditors should be answered truthfully, directly, and concisely. Interviewees should be cautious of over-answering.

- **Know the Audience and Avoid Acronyms.** OCR auditors will have varying levels of experience with respect to health industry business operations and regulatory compliance requirements and programs.
  - Interviewees should be prepared to provide simple, brief backgrounds of industry and operations if necessary.
  - The use of acronyms and industry jargon should be avoided.
Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now
   i. Know the Rules and Areas of Non-Compliance
   ii. Know the Risks Specific to Your Organization
   iii. Know the Data and the Flows – Internal and External
   iv. Know Your Audit Process and Prepare
   v. Know the Roadmap Ahead and Be Self-Aware
Being Self-Aware and Having a Plan - The Secret Sauce

- **Ingredient 1 - Risk Assessment Process.** Ensure that a current risk analysis is in place and that the risk analysis actually identifies and categorizes risks (e.g., low, medium, high) rather than merely documenting that controls are in place or documenting the gaps in compliance with the Security Rule.
  - See OCR Guidance on Risk Analysis and HHS' recently released Security Risk Assessment Tool. Jives nicely with CSF, but one size does not fit all.

- **Ingredient 2 - Business Associate Included.** Going forward, BAs to be included. Ensure to know who is has access to your systems and data and to whom you entrust sensitive personal information.

- **Ingredient 3 - Integrated Privacy & Security Program Initiative Roadmap - The Secret Ingredient.** A simple Gantt chart roadmap illustrating how planned remediation measures are typically coordinated/timed and the related key dependencies is often overlooked.
  - Organizations have an 18 month to 3 year horizon (some longer).
Contact for Inquiries

Jim Koenig JD
Global Leader, Commercial Privacy Practice and Cybersecurity for Health Principal
Booz Allen Hamilton Inc.
1818 Market Street 27th Floor
Philadelphia, PA 19103
+1 610-246-4426
Koenig_James@bah.com
Questions?