MU Security & Privacy Risk Assessments: What It Is & How to Approach It

Dr. Bryan S. Cline, CISSP-ISSEP, CISM, CISA, CCSFP, HCISPP
Advisor, Health Information Trust Alliance
Introduction

• Healthcare providers across the country are conducting security and privacy risk assessments in support of the U.S. government’s initiative around the meaningful use of an EHR. However, there appears to be significant variation in the type and rigor of the assessments conducted by different providers and the consulting firms they engage. So what exactly is needed?

• This presentation drills down into the basic requirements specified under HIPAA and HITECH and provides a sound approach to efficiently and effectively conduct a meaningful use security and privacy risk assessment that will withstand regulatory review.
Outline

• Introduction

• Meaningful Use

• MU Risk Assessment
  – Demonstrate reasonable practices
  – Be efficient
  – Take remediation seriously

• Attestation
Meaningful Use
What is Meaningful Use?

• Meaningful use of an EHR:
  – Certified EHR [system/technology
  – Used in a meaningful way

• Stage 2 Requirements (thru 2016)
  – For eligible hospitals & critical access hospitals (25/15)
  – For eligible professionals (22/18/13+5)

• Stage 3 Requirements (beginning 2017)
  – Final rule with stage 3 requirements scheduled for mid-2015

https://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp
Why Pursue Meaningful Use?

- By [implementing] and meaningfully using an EHR, providers can:
  - Receive financial incentives prior to 2015
  - Avoid reductions in reimbursement beyond 2015
  - Reap benefits beyond financial incentives

https://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp
http://journal.ahima.org/2010/08/26/meaningful-use%E2%80%94incentive-payments-and-program-requirements
What are the Security & Privacy Requirements?

- **Stage 2 MU Measure**
  - Protect health information

- **Stage 2 MU Objective**
  - Manage risks to health information

- **Stage 2 MU Attestation**
  - Yes/No

- **Stage 2** – Adds req’t to add encryption/security of data at rest to original Stage 1 req’t for a HIPAA-compliant risk analysis!

http://www.cms.gov/EHRIncentivePrograms/Downloads/14HC-ProtectElectronicHealthInformation.pdf
What is a Security Risk Analysis?

• Per the HIPAA Security Rule
  – Accurate and thorough risk assessment
  – Reasonable and appropriate safeguards
  – Reasonably anticipated threats or hazards

• However the Security Rule does not prescribe a specific risk analysis methodology …

What are the Elements of a Risk Analysis?

- Scope the Analysis
- Collect Data
- Identify and Document Potential Threats and Vulnerabilities
- Assess Current Security Measures

Meaningful Use Risk Assessment
Guide to Meaningful Use Risk Assessments

- Demonstrate reasonable practices
- Be efficient
- Remediate deficiencies
Demonstrate Reasonable Practices
Select a Sound Risk Assessment Methodology (i)

1. Determine Scope
   - Applications, interfaces, infrastructure

2. Prepare for Assessment
   - Focus on high risk areas
   - Identify individuals responsible for key control areas
   - Conduct top down enterprise control analysis
   - Do not get stuck in the weeds

3. Report
   - Report on findings and remediation plan

4. Track and Measure Progress
   - Track progress against industry benchmarks
   - Focus on measures
Select a Sound Risk Assessment Methodology (ii)

1. Determine Scope
   - Applications, interfaces, infrastructure
   - HITRUST Scoping Template

2. Prepare for Assessment
   - Focus on high risk areas
   - Identify individuals responsible for key control areas
   - Conduct top down enterprise control analysis
   - Do not get stuck in the weeds
   - HITRUST High Risk List
   - HITRUST CHIP
   - HITRUST/NIST PRISMA

3. Report
   - Report on findings and remediation plan
   - HITRUST CSF Validated Report
   - Corrective Action Plan Template

4. Track and Measure Progress
   - Track progress against industry benchmarks
   - Focus on measures
   - HITRUST CSF Validated Report
Align Control Decisions w/ Industry Standards (i)

NIST

COSO

COBIT

ISO 9000

CMMI

ITIL & other standards

WHAT

HOW

SCOPE OF COVERAGE

(adapted from ITGI, 2007, p. 11)
Align Control Decisions w/ Industry Standards (ii)

- Understand how frameworks interrelate
- Adopt & manage a common set of controls
- Collect & store evidence
- Generate reports for each framework
Align Control Decisions w/ Industry Standards (iii)
Be Efficient
Focus on the Certified EHR System

- Determine what is within scope …

- … and what is potentially out of scope
Tailor the Assessment to the Organization (i)

- Two types of HITRUST CSF assessments
- Each tailored to the organization
- Focused on high risk areas
Tailor the Assessment to the Organization (ii)

- Common Healthcare Information Protection (CHIP) Questionnaire

<table>
<thead>
<tr>
<th>Security Capability Measures</th>
<th>INTRO.</th>
<th>SCOPE</th>
<th>PROFILE</th>
<th>PROP. METRICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Information Security Policies</td>
<td>Answer</td>
<td>Comments</td>
<td>Measure Validation</td>
<td></td>
</tr>
<tr>
<td>2 Laptop Security</td>
<td>Answer</td>
<td>Comments</td>
<td>Measure Validation</td>
<td></td>
</tr>
</tbody>
</table>

CSF Cross References (click + in left margin to view)

- Number of laptops with PHI lost or stolen in the past year?
- Percentage of laptops with desktop firewall installed and operating?
- Percentage of laptops with minimum cryptographic modules executed?
Use Sampling Techniques Where Appropriate

- HITRUST CSF Assurance supports sampling to improve efficiency
- Sampling should be random but other methods could be supported
- There must be a basis for concluding the practices/locations are similar
- HITRUST recommended sample sizes

<table>
<thead>
<tr>
<th>Number of Practices in Population/Group</th>
<th>Minimum Number of Practices at Which to Perform Security Risk Assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;50</td>
<td>10%, Maximum of 25 Practices</td>
</tr>
<tr>
<td>15-50</td>
<td>Minimum of 5/Use Judgment</td>
</tr>
<tr>
<td>&lt;15</td>
<td>Minimum of 3/All Practices</td>
</tr>
</tbody>
</table>

- Inconsistent results may imply sampling is inappropriate
Key Components of the CSF Assurance Program

• Standardized tools and processes

• Cost effective and rigorous assurance
  – Multiple assurance options
    • Self reporting
    • Remote testing
    • On-site assessment
  – Centralized quality control
Remediate Deficiencies
Develop a Sound Corrective Action Plan

- HIPAA/MU requires remediation / corrective action plans (CAPs)
- Develop a CAP methodology and train control owners / stakeholders
- HITRUST CSF assessment reports includes CAPs for high risk items

**Weakness Identifier**

Weaknesses represent any program or system-level information security vulnerability that poses an unacceptable risk of compromising confidentiality, integrity or availability of information.

Ex. SYSX_3_2009_1

**Related HITRUST CSF Control Specification for the Identified Weakness**

Ex. 01.b User Registration

**X-PDC** is the organization, department or title of the position within the organization that is directly responsible for mitigating the weakness.

Ex. System X Director of IT Security

**Resources Required** include the funding (denoted in dollars) or man-hours necessary for mitigating a weakness. The type of funding (current, new or reallocated) should be noted.

Ex. 120 hours, current staff

**Completion Dates** should be set based on a realistic estimate of amount of time it will take to collect the resources for the corrective action and implement/test the corrective action.

Ex. 2/15/2009

**Milestones with Completion Dates** outline the specific high-level steps to be executed in mitigating the weakness and the estimated completion date for each step.

Ex. Develop user registration procedures for granting, transferring, and terminating access.

Submit to System X Administrator for review and input, 2/15/2009

**Changes to Milestones** indicate the new estimated future date of a milestone’s completion if the original date is not met.

Ex. None noted to-date

<table>
<thead>
<tr>
<th>Weakness Identifier</th>
<th>Weakness Description</th>
<th>HITRUST CSF Control Specification</th>
<th>Organizational Point of Contact (PoC)</th>
<th>Resources Required</th>
<th>Scheduled Completion Date</th>
<th>Milestones with Completion Dates</th>
<th>Changes to Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSX_3_2009_1</td>
<td>Granting, transfer and termination procedures for user access are not established</td>
<td>01.b User Registration</td>
<td>System X Director of IT Security</td>
<td>120 hours, current staff</td>
<td>2/15/2009</td>
<td>Develop user registration procedures for granting, transferring, and terminating access.</td>
<td>None noted to-date</td>
</tr>
</tbody>
</table>

**HITRUST Common Security Framework**

CSF Assurance Toolkit 2010 / v1.0

Corrective Action Plan [TEMPLATE]
Actively Manage Remediation

Higher Priority CAPs

Lower Priority CAPs

- Information Security Policies
- Laptop
- Mobile Media
- Wireless
- Malware
- Vulnerability Management
- Secure Disposal
- External Data Protection
- PHI Transmission Protection
- Password Management
- Access Control and Authentication Control
- Training and Awareness
- Third Party Security Management
- Incident and Breach Response
- Business Continuity Management
- Auditing

© 2011-2014 HITRUST LLC, Frisco, TX. All Rights Reserved.
Attestation
Attestation Requirement

• Medicare hospitals’ that they have “satisfied the required objectives and associated measures” of 42 CFR §495.6

• Medicaid providers must attest:

“This is to certify that the foregoing information is true, accurate, and complete. I understand that Medicaid EHR incentive payments submitted under this provider number will be from Federal funds, and that any falsification, or concealment of a material fact may be prosecuted under Federal and State laws.” (42 CFR § 495.368)
Attestation Risks

• Government is very concerned about fraud under the program
  – CMS is developing an audit strategy to ameliorate and address risk (Federal Register Vol. 75, No. 144, p. 44324)
  – CMS may “review … demonstration(s) of meaningful use.” (42 CFR § 495.8)
  – States required to “annually … verify information regarding … meaningful use of said technology before making any payments to providers.” (42 CFR § 495.366)
  – States required to ensure the qualification of the providers who request Medicaid EHR incentive payments ((42 CFR § 495.368)

• Other methods to deter, detect and correct fraud
  – HITECH incentive audits
  – HIPAA compliance and security breach investigations
  – Federal/state false claims act penalties
  – Whistleblower (qui tam) lawsuits
  – Federal/state program disqualification
  – Criminal/civil fraud actions
Due Diligence and Due Care

• Leverage HIPAA’s inherent flexibility when performing due diligence

• Exercise due care

• Ensure attesting officer is properly informed

• Show your work!
Summary of CSF Assurance Risk Assessments

- Approach referenced by Office of Civil Rights

- Designed to be cost-effective and efficient

- Leverages defined, **reasonable controls**

- Streamlines risk determination

- Provides formal and credible reporting

- Utilizes benchmarking data

- Provides recommendations for remediation
Questions?

- Dr. Bryan Cline, HITRUST, bryan.cline@hitrustalliance.net

For more information on the CSF Assurance Program visit: www.HITRUSTAlliance.net/assurance

For a list of HITRUST CSF Assessors visit: www.HITRUSTAlliance.net/Assessors_List.pdf

For customer support (Professional Subscribers only) write: support@HITRUSTalliance.net