CSF Support for HIPAA and NIST Implementation and Compliance
Why does HITRUST exist?

• Multitude of challenges
  – Significant government oversight
  – Evolving requirements
  – Complex business relationships
  – Uncertain standard of care
    • Reasonable and appropriate?
    • Adequate protection?
Principle driver ...
“Overarching” requirement

• 45 CFR § 164.308(a)(1)
  – *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 or business associate.

• 45 CFR § 164.306(a)
  – (1) Ensure the [CIA] of all [ePHI] the covered entity or business associate creates, receives, maintains or transmits.
  – (2) *Protect against any reasonably anticipated threats* or hazards to the security or integrity of such information.
What exactly is a risk assessment?

• Risk assessment
  – “The process of identifying, estimating, and prioritizing risks … resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.”
    NIST SP 800-39, Managing Information Security Risk

• Risk analysis
  – “Examination of information to identify the risk to an information asset. Synonymous with risk assessment”
    CNSSI No. 4009, National IA Glossary

• “Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule”
  HHS Guidance on Risk Analysis Requirements under the HIPAA Security Rule
Risk management lifecycle

Step 1: Identify risks and define protection requirements

Step 2: Specify controls

Step 3: Implement and manage controls

Step 4: Assess and report
Risk analysis process

1. Classify Information Assets
2. Inventory and Categorize Assets
3. Identify Threats
4. Assess Vulnerabilities
5. Determine Impact
6. Assess and Rank Risks
7. Develop Risk Strategies/Plan
HHS interpretation

- HHS Guidance on RA Requirements under the Security Rule
  - Scope the assessment to include all ePHI
  - ID & document all assets with ePHI
  - ID & document all reasonably anticipated threats to ePHI
  - Assess all current security measures
  - Determine the likelihood of threat occurrence
  - Determine the potential impact of a threat occurrence
  - Determine the level of risk
  - Document assigned risk levels and corrective actions
  - Rinse & repeat
Traditional approach

• Conduct comprehensive risk analysis
  – Threat & vulnerability assessment
  – Information asset valuation
  – Information protection control selection

• Comprehensive risk analysis difficult for most
  – Lack of skilled resources, funding, time
  – Limited information available
Framework Approach

• Modify general baseline control standard
  – Threat modeling / control selection performed by capable, third-party for general threats, vulnerabilities
  – Baseline controls assigned based on confidentiality, and/or criticality

• Baseline control approach most widely used
  – ISO/IEC 27001/27002, part of the ISO/IEC 27000-series RMF
  – NIST SP 800-53, part of the NIST SP 800-series RMF
  – HITRUST CSF, part of the HITRUST RMF
    • Based on ISO/IEC 27001 and integrates a significant portion of NIST SP800-53 requirements
HITRUST Risk Analysis

• Modified Guidance on RA Requirements for the Security Rule
  – Scope the assessment to include all ePHI
  – ID & document all assets with ePHI (inventory and categorization)
  – Select a control baseline for given categorization (risk factors)
  – Assess all current security measures (gap analysis)
  – Determine the likelihood of a control failure
  – Determine the potential impact of a control failure
  – Determine the level of residual risk
  – Document assigned risk levels and corrective actions
  – Rinse & repeat

Note: A threat catalog is being developed as part of a HITRUST C3 initiative to map threats to specific controls, which will support the requirement to enumerate and address all reasonably anticipated threats.
Justification for the approach

• All federal agencies use the NIST RMF
  – NIST SP 800-30 r1, Guide for Conducting Risk Assessments, addresses traditional RA
    • Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition
  – BUT ... NIST SP 800-37 r1, Guide to Applying the [RMF] to Federal Information Systems, doesn’t address threat identification
    • Categorize information system
    • Select security controls
    • Implement security controls ...
  – Hardly seems fair, does it?
    • Traditional approach likely used due to lack of federally recognized healthcare security framework ... including NIST
But what about everything else in HIPAA?

• RA requirement is one of 42 stds & specifications
• Like RA, other requirements lack prescription
  – What safeguards are reasonable and appropriate?
  – What is adequate protection?
• Simple HIPAA requirement-based approaches to risk analysis lack depth, breadth and rigor
• OCR will not accept a risk analysis based on the old OCR Audit Protocol developed by KPMG
  (Linda Sanchez, 2014 HCCA conference)
  – Implies controls reviewed do not sufficiently address all reasonably anticipated threats
  – Implies similar approaches based on HIPAA standards and specifications are also flawed
Defining reasonable and appropriate for healthcare

- HITRUST CSF
  - Built on international framework, ISO 27001
  - Additional prescription provided by:
    - ISO 27002 & 27799
    - NIST SP 800-53
    - CMS IS ARS (High-level baseline)
    - PCI-DSS
    - Others
  - CSF controls mapped to HIPAA
    - E.g., 164.308(a)(5)(ii)(C), Log-in Monitoring (Addressable)
    - 8 controls provide direct support: 01.b., 01.c, 01.e, 02.i, 09.aa, 09.ab, 09.ad, 09.af
    - 7 controls provide indirect support: 01.q, 01.s, 01.t, 01.u, 06.e, 06.i, 11.a
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>07.b Ownership of Assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07.c Acceptable Use of Assets?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07.d Classification Guidelines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>07.e Information Labeling and Handling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08.a Physical Security Perimeter</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>08.b Physical Entry Controls?</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>08.c Securing Offices, Rooms, and Facilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>08.d Protecting Against External and Env. Threats?</td>
<td>X</td>
<td></td>
<td>O</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>08.e Working in Secure Areas</td>
<td></td>
<td></td>
<td></td>
<td>O</td>
<td></td>
<td>O</td>
<td>X</td>
</tr>
<tr>
<td>08.f Public Access, Delivery, and Loading Areas</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>08.g Equipment Siting and Protection</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>08.h Supporting Utilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08.i Cabling Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08.j Equipment Maintenance?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>08.k Security of Equipment Off-Premises</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>08.l Secure Disposal or Re-Use of Equipment?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

https://www.hitrustcentral.net/news_repository/blog/comparingthecsfisoiec27001andnistsp80053~1
But what about NIST?

- **NIST SP 800-53 r4 moderate-level baseline**
  - All controls
  - All enhancements
- **Requirements tailored/harmonized for healthcare**
  - Reasonable and appropriate
  - Adequate protection
- **Mappings are similar to HIPAA**
  - Direct mappings with relevant language
  - Indirect or supportive mappings with relevant language
- **Mappings are consistent with NIST mappings to ISO/IEC 2001:2005**
Prego ... it’s in there!

<table>
<thead>
<tr>
<th>Item</th>
<th>CSF</th>
<th>CA-9</th>
<th>CM-1</th>
<th>CM-2</th>
<th>CM-3</th>
<th>CM-4</th>
<th>CM-5</th>
<th>CM-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>09.a. Documented Operations Procedures</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.b. Change Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>09.c. Segregation of Duties*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.d. Separation of Development, Test, and Operational Environments</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.e. Service Delivery*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.f. Monitoring and Review of Third-Party Services*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.g. Managing Changes to Third-Party Services*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.h. Capacity Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 09.i. System Acceptance | | | | | | | | 0
| 08.j. Controls Against Malicious Code* | | | | | | | | |
| 08.k. Controls Against Mobile Code | | | | | | | | |
| 08.l. Backup | | | | | | | | |
| 08.m. Network Controls* | | | | | | | | |
| 08.n. Security of Network Services | | | | | | | | |
| 08.o. Management of Removable Media* | | | | | | | | |

https://www.hitrustcentral.net/news_repository/blog/comparingthecsfisoiec27001andnistsp80053~1
But what about the “other” NIST?

- The NIST Cybersecurity Framework provides structure for sector-level cybersecurity frameworks and organizational-level programs.
- HITRUST provides a healthcare-specific implementation of the NIST framework that addresses a broad spectrum of information security risk (not just cybersecurity).
- CSF controls mapped to 100% of the NIST cybersecurity subcategories (w/ language updates) – 2014 CSF v6.1.
Dr. Bryan S. Cline, CISSP-ISSEP, CISM, CISA, CCSFP, HCISPP
HITRUST Advisor
Bryan.Cline@HITRUSTAlliance.net