Leveraging the CSF to Assess HIPAA Privacy
Nadia Fahim-Koster Director, IT Risk Management
Meditology Services
April 2016
Agenda

• Introduction
• HITRUST and Privacy Controls
• Privacy Rule core requirements and security intersections
• How to leverage MyCSF to assess your privacy function
• Questions
Introduction

Nadia Fahim-Koster, Director, Meditology Services

• 14+ years experience in healthcare IT security and privacy leadership
• Previously CISO and Chief Privacy Officer for several large health systems
• Certified CISSP, HCISPP, and HITRUST
• Advises healthcare clients coast to coast on privacy and security

Meditology is dedicated to delivering expertise and leadership in information privacy and security, compliance, and audit, specifically for healthcare
HITRUST CSF and Privacy Controls
HITRUST CSF and Privacy Controls

• CSF supports certification of any covered entity or business associate’s compliance with the HIPAA Privacy Rule
• Control category 13.0 Privacy Practices supports Texas certification of a covered entity’s compliance with the HIPAA Privacy Rule
• CSF also includes requirements specified in NIST SP 800-53 r4 Appendix J – Privacy Control Catalog (required for FISMA compliance or segments devoted to federal agencies and contractors)
Privacy Rule Core Requirements and Security Intersections
Overview of the Privacy Rule

• Uses and disclosures
• Patient rights
• Administrative requirements
Uses and Disclosures of PHI – General Rules

• Permitted uses and disclosures:
  o To the individual
  o Treatment, payment and healthcare operations
  o Business associates: only as required by BAA or by law

• Required uses and disclosures:
  o To the individual
  o As required by the secretary to investigate or determine compliance
  o Business associates: as required by secretary to investigate; to the CE, individual/designee to satisfy CE’s obligations with respect to a request for electronic copy of PHI
Uses and Disclosures of PHI – General Rules (Cont.)

- Prohibited uses and disclosures:
  - Sale of PHI
- Minimum necessary
- De-identified information
- Business associates
- Deceased individuals
- Personal representatives
- Whistleblowers
Uses and Disclosures of PHI – Authorization Required

- Psychotherapy notes
- Marketing
- Sale of PHI
Uses and Disclosures of PHI – Opportunity to Agree or Object

- Facility directories
- Involvement in the individual’s care and notification purposes
Uses and Disclosures of PHI – Authorization or Opportunity to Agree or Object is Not Required

- Required by law
- Public health activities
- Victims of abuse, neglect or domestic violence
- Health oversight activities
- Disclosures of judicial and administrative proceedings
- Law enforcement purposes
- Cadaveric organ, eye or tissue donation purposes
- Uses and disclosures for research purposes
- Avert a serious threat to health or safety
- Specialized government functions
- Disclosures for workers’ compensation
Uses and Disclosures of PHI – Other Requirements

• De-identification of PHI
• Minimum necessary
• Limited data set
• Fundraising
• Underwriting and related purposes
• Verification requirements
Individuals’ Rights

- Notice of Privacy Practices
- Rights to request privacy protection request
  - Restriction of uses and disclosures
  - Confidential communications
- Right to request access to PHI
- Right to request amendment of PHI
- Right to request an accounting of disclosures of PHI
Administrative Requirements

• Personnel designation
• Training
• Safeguards
• Complaints
• Sanctions
• Mitigation
• Refrain from intimidating or retaliatory acts
• Waiver of rights
• Policies and procedures
• Documentation
• Group Health Plans
Privacy and Security Rules – Intersection

• The HIPAA Privacy Rule requires that covered entities apply administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. See 45 CFR 164.530(c)

• The HIPAA Security Rule addresses the standards required to implement these safeguards

• The Administrative Safeguards require that covered entities implement:
  ○ Risk Analysis: “Conduct accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the organization”.
  ○ Risk Management: “Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level”.

MEDITOLOGY SERVICES

HITRUST 2016
Risk Assessment - Privacy

Leveraging HITRUST CSF to conduct comprehensive risk assessment to cover the HIPAA Privacy Rule requirements, including the administrative, physical and technical safeguards of the HIPAA Security Rule.
Developing the Privacy Risk Assessment - Leveraging MyCSF
Conducting the Assessment

Department of Health and Human Services (DHHS) guidance on risk assessment requirements:

• Scope the assessment to include all ePHI
• Identify & document all assets with ePHI
• Identify & document all reasonably anticipated threats to ePHI
• Assess all current security measures
• Determine the likelihood of threat occurrence
• Determine the potential impact of threat occurrence
• Determine the level of risk
• Document assigned risk levels and correction actions

Using the above guidance to conduct the Privacy Assessment by leveraging the HITRUST CSF
Scoping the Assessment

• Identify which controls/standards apply to your organization:
  o Covered entity
  o Business Associate
  o Hybrid entity
  o State specific requirements (i.e. Texas)
  o FISMA environment
Scoping the Assessment

![Screen capture of RSAM Home interface with HITRUST CSF Assessments page open, showing assessment details and options.](image)
Scoping the Assessment

![Administrative and Scoping Information](image-url)
## HIPAA Privacy Assessment - Applicable Controls

### 13.0 - Privacy Practices

<table>
<thead>
<tr>
<th>13.a Notice of Privacy Practices</th>
<th>TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.b Rights to Protection and Confidentiality</td>
<td>TX</td>
</tr>
<tr>
<td>13.c Authorization Required</td>
<td>TX</td>
</tr>
<tr>
<td>13.d Opportunity Required</td>
<td>TX</td>
</tr>
<tr>
<td>13.e Authorization or Opportunity Not Required</td>
<td>TX</td>
</tr>
<tr>
<td>13.f Access to Individual Information</td>
<td>TX</td>
</tr>
<tr>
<td>13.g Accounting of Disclosures</td>
<td>TX</td>
</tr>
<tr>
<td>13.h Correction of Records</td>
<td>TX</td>
</tr>
<tr>
<td>13.i Required Uses and Disclosures</td>
<td>TX</td>
</tr>
<tr>
<td>13.j Permitted Uses and Disclosures</td>
<td>TX</td>
</tr>
<tr>
<td>13.k Prohibited or Restricted Uses and Disclosures</td>
<td>TX</td>
</tr>
<tr>
<td>13.l Minimum Necessary Use</td>
<td>TX</td>
</tr>
<tr>
<td>13.m Confidential Communications</td>
<td>TX</td>
</tr>
<tr>
<td>13.n Organizational Requirements</td>
<td>GHP</td>
</tr>
</tbody>
</table>
Conduct the Assessment - Leveraging MyCSF
**HITRUST CSF Assessment**

The covered entity documents and maintains the designated record sets that are subject to access by individuals and the titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of seven years.

When authorization is required, the covered entity ensures the authorizations are valid. Note this addresses 506(b) [partially] and 508(c) [but both are contained in a single control, 13.c].

The covered entity provides for individual complaints concerning the covered entity's privacy policies and procedures or its compliance with such policies and procedures.

The covered entity only discloses PHI to law enforcement for valid law enforcement purposes when specifically defined criteria are met.
Leveraging Illustrative Procedures

- Policies
- Procedures
- Implemented
- Measured
- Managed
Illustrative Procedures—Policy

Policy

Maturity - Policy

2. Somewhat Compliant (25%)

Illustrative Procedure for Policy

Examine written policies and/or standards related to authorizations for the disclosure of PHI and ensure that the elements required for a valid authorization, as specified in HIPAA § 164.508(b)(1), (b)(2), (b)(6) and (c), are addressed. (The assessor is strongly encouraged to examine the HIPAA requirements in detail prior to assessing the organization’s compliance at any level for this requirement statement.) If no written policy or standard exists, interview key staff involved in the handling authorizations for the use and/or disclosure of PHI and determine if the requirements are understood. Evidence of ad hoc or informal policy may also be provided by reviewing any written procedures or examining documentation associated with formal or ad hoc processes to determine if the requirements are addressed consistently by the covered entity.

Process
Illustrative Procedures – Process

Process

Maturity - Process

3. Partially Compliant (50%)

Illustrative Procedure for Procedures

Determine if written procedures for the disclosure of PHI address the requirement for valid authorization, as specified in HIPAA § 164.508(b)(1), (b)(2), (b)(6) and (c). Determine whether or not the procedures address the specific elements required for valid authorization as specified in HIPAA § 164.508(b)(1), (b)(2), (b)(6) and (c). Interview a representative sample of personnel responsible for handling and disclosing PHI to determine if the procedures address the elements required for a valid authorization (whether or not a written policy or procedure exists). Ask them to describe the procedures and compare their description(s) to written procedures, if they exist, to determine if they are consistent.
Illustrative Procedures—Implementation

**Implemented**

Maturity - Implemented

3. Partially Compliant (50%)

Illustrative Procedure for Implementation

Obtain and review a sample of instances where authorization is required to determine if a valid authorization was obtained with respect to the elements specified in HIPAA § 164.508(b)(1), (b)(2), (b)(6) and (c). If the covered entity is a provider, obtain and review all patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any. Interview a representative sample of personnel responsible for handling patient/client information to determine if written or ad hoc procedures are followed consistently. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for unauthorized disclosure of PHI due to the lack of a valid authorization. Review complaints from an ethics and/or compliance hotline to determine if there were complaints about inappropriate or unauthorized disclosure due to the lack of a valid authorization have been made. Interview human resources personnel to determine if workforce members have been disciplined for unauthorized disclosure due to the lack of a valid authorization and whether or not the disclosures resulted in a violation of patient privacy. Examine related legal and HR documentation, if available.
Illustrative Procedures—Measured

Measured

Maturity - Measured

1. Non Compliant (0%)

Illustrative Procedure for Test

Examine metric(s) or other measure(s) that evaluate(s) the organizations compliance with the disclosure policy to determine if the requirements for authorization address the elements required for validity, as specified in HIPAA § 164.508(b)(1), (b)(2), (b)(6) and (c), are addressed by the metric. For example, the metric could indicate the number of invalid authorizations as a percentage of all authorizations based on a review of all authorizations or a representative sample of authorizations. Non-compliance with the policy requirements could also be part of a broader metric on unauthorized disclosures if unauthorized disclosures due to the lack of a valid authorization can be discerned. Note a measure could include regular or ad hoc reports or audits of authorizations if they considered the requirements for validity as specified. If a metric or measure adequately evaluates the elements required for a valid authorization, determine if the measure is tracked over time and if performance goals have been established.
Illustrative Procedures– Managed

**Managed**

Maturity - Managed

1. Non Compliant (0%)}

Illustrative Procedure for Integration

Determine if the individual or office that receives the measure or metric is able to correct issues with valid authorizations, as specified in HIPAA § 164.508(b)(1), (b)(2), (b)(6) and (c), without the need to routinely escalate the issues to the next level of management. Note the ability to escalate issues must also exist if the root cause of a specific incident cannot be addressed by the individual or office receiving and reviewing the metric or measurement. Examine related records to determine if deviations/incidents occurred and if appropriate action was taken to identify, investigate, correct and follow-up on deviations/incidents. If written records do not exist, interview personnel who receive and review the metric(s) to determine if ad hoc processes for investigation and resolution exist and if deviations/incidents occurred and were corrected.
Assessment Results
Compliance Level by Domain
GAPs Identified by Domain
Residual Risk Rating
### Assessment Results Exported

#### 19 Data Protection & Privacy - Nadia test

<table>
<thead>
<tr>
<th>Response Status</th>
<th>Type</th>
<th>Level</th>
<th>Related HITRUST CSF Control</th>
<th>Scope</th>
<th>Applicability</th>
<th>HITRUST CSF Requirement Statement</th>
<th>Maturity - Policy</th>
<th>Maturity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Started</td>
<td>Organizational</td>
<td>1</td>
<td>1.3.a Notice of Privacy Practices</td>
<td>In scope</td>
<td>Applicable</td>
<td>The covered entity uses and discloses PHI in a manner consistent with its privacy notice.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Organizational</td>
<td>1</td>
<td>1.3.a Notice of Privacy Practices</td>
<td>In scope</td>
<td>Applicable</td>
<td>The covered entity provides individuals with an appropriate, plain-language notice of the potential uses and disclosures of their PHI, that contains all required elements (e.g., header, description, dates, address, name) and at least one example, requirement is met.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complete</td>
<td>Organizational</td>
<td>1</td>
<td>1.3.a Notice of Privacy Practices</td>
<td>In scope</td>
<td>Applicable</td>
<td>The covered entity must provide appropriate notice to the individual (other than an inmate) no later than the compliance date or upon enrollment thereof, within 60 days of a material change that affects the notice.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Organizational</td>
<td>1</td>
<td>1.3.a Notice of Privacy Practices</td>
<td>In scope</td>
<td>Applicable</td>
<td>A covered entity may provide the notice of privacy practices to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Organizational</td>
<td>1</td>
<td>1.3.b Rights to Protection and Confidentiality</td>
<td>In scope</td>
<td>Applicable</td>
<td>A covered entity must permit an individual, or their legally-authorized representative, to request that the covered entity restrict uses or disclosures of the individual's PHI to carry out treatment, payment, or health care operations, but is not required to comply with such a request.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 18 Physical & Environmental Security

[Excel file]
Questions