MONITORING AND DOCUMENTING HIPAA PRIVACY AND SECURITY IMPLEMENTATION USING METRICS

Mr. Sam Jenkins
TMA Privacy Office
Department of Defense
Agenda

- Background
- Where were we last year?
- What have we done?
- What we are doing: Metrics
  - Background
  - Development
  - Use
What is the MHS? TMA?

MHS: Military Health System
TMA: TRICARE Management Activity
The MHS includes Provider, Payor, Government, and Life Sciences
A Combat-Ready Healthcare System
MISSION
To enhance the Department of Defense and our nation’s security by providing health support for the full range of military operations and sustaining the health of all those entrusted to our care.

WHAT IS TRICARE
A health care plan using military health care as the main delivery system.
- Augmented by a civilian network of providers and facilities.
- Serving our uniformed services, their families, retired military, and their families worldwide.

BASIC FACTS OF TRICARE

9.2 MILLION
TRICARE Eligible Beneficiaries
- 5.0 million TRICARE Prime Enrollees
- 1.62 million TRICARE for Life
- 170,000 TRICARE Plus
- 93,000 US Family Health Plan
- 24,000 TRICARE Reserve Select
- 2.29 million Non-enrolled Users

18,300
Inpatient Admissions
- 5,300 Direct Care
- 13,000 Purchased Care

1.8 MILLION
Outpatient Visits
- 640,000 Direct Care
- 1.17 million Purchased Care

132,500
MHS Personnel
- 88,400 Military
- 44,100 Civilian

2200
Births
- 1,000 Direct Care
- 1,200 Purchased Care

A WEEK IN THE LIFE
Where We Were Last Year
From last year...

- The key to compliance is risk management. To correctly implement the security standards and establish compliance, each covered entity must:
  - Assess potential risks and vulnerabilities to ePHI
  - Develop, implement, and maintain appropriate security measures given those risks
  - Document those measures and keep them current
How Do We Know If We Are Compliant?

- Policy?
- Procedure?
- Process?
How Do We Know If We Are Compliant?

- No standard policy, procedure, or methodology can guarantee compliance for all covered entities.
- Compliance is different for each organization and no single strategy will serve all covered entities.
- …Compliance is not a one-time goal, it must be maintained. Compliance with the Evaluation Standard at § 164.308(a)(8) will allow covered entities to maintain compliance.

Source: HHS FAQ
Executing the Plan
(from last year...)

- Development and selection of Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE$^{SM}$) as risk assessment methodology
- DoD and Service level policy gap analysis
- Integrated Process Team and Medical Interdisciplinary Readiness Team (MIRT) formation
- Initial training in HIPAA and OCTAVE$^{SM}$
Executing the Plan
(from last year...)

- Development of HIPAA Security Program and Strategy
  - Program Management Plan
  - Training and Awareness Program
  - Policy development (Directive, Regulation and Implementation Guides)
  - Oversight and Compliance (Compliance Assurance Framework, Compliance and reporting tools)
  - Incident Response
What We Planned  
(conceptual from last year...)

Oversight and Compliance (1 of 2)

Compliance is established and maintained by implementing business practices including measurement against metrics and periodic reports through an appropriate reporting structure

- Measuring success
- Completion percentages
- Identifying areas for improvement
- Preparations and contingencies
- Communication of issues
What We Are Doing – HIPAA Metrics
To Keep Up the Good Work...

- A lot of things going on in your day-to-day activities
  - Sanctions
  - Complaints and Incidents
  - Access Management
  - Training and Awareness
  - Risk Management
  - Accounting of Disclosures
  - Evaluation
  - Workstation Security
To sustain and improve how we implement HIPAA, we must identify for each requirement:

- **Goal**: what we hope to achieve
- **Objective**: what we specifically seek to do
- **Evidence of Implementation**: proof we do it
- **Level of Effectiveness**: how well we do it
...And Identify Key Roles and Needs

- HIPAA Security Official
- HIPAA Privacy Officer
- Medical interdisciplinary readiness team (MIRT)
- Senior Executive Staff
- Covered entity workforce
- Self-assessment tool
- Risk analysis / management
- Training and Awareness
Example: Risk Analysis

- **GOAL**
  - Technical and organizational policies, procedures, and processes address the potential risks to PHI

- **OBJECTIVE**
  - A MIRT assesses and documents risks to PHI on a regular basis and as a result of system, operational, or other changes
Example: Risk Analysis

EVIDENCE OF IMPLEMENTATION

1. Updated and disseminated **policy** for conducting information security risk assessments
2. Updated and disseminated **procedures** for conducting information security risk assessments
3. Procedures for conducting information security risk assessments are **implemented** and reinforced in a consistent manner
4. Policies and procedures are routinely **evaluated** for adequacy and effectiveness, including
5. The consideration of HIPAA requirements is **institutionalized**
Going Forward

- Ongoing cycle of risk management and improvement
- Self-assessment tool: initial compliance assessment
- Prioritized mitigation based on risk analysis
- Metrics Program guides, measures and reports effectiveness of HIPAA implementation
- Institutionalizes activities of risk management
Developing Measures
Analyzed Privacy and Security Rules, Determined Goals and Objectives

- Adapted metrics approaches from NIST and Federal CIO Council
- Designed metrics that guide, measure, and report implementation
  - Measures management process
  - Identifies evidence of compliance that emerges as a natural consequence of doing the work
Identified Indicators of Effectiveness

- **Evidence** in the form of products and processes that suggest progress toward meeting the **Goal** (target) with indicated **Objective** (approach)

- Objective, obvious actions and products needed to ESTABLISH compliance

- What is being done to MANAGE and IMPROVE implementation
Indicators of Effectiveness: 5 Levels

- Each level represents a more complete and effective state of a requirement
  - Level 1: Policies
  - Level 2: Procedures
  - Level 3: Implementation = initial compliance
  - Level 4: Test and validate
  - Level 5: Institutionalize

- Each level includes product and process evidence of compliance and management
Two Kinds of Measures

- Management: effectiveness of managing HIPAA implementation
- Statistical: completion percentages and trending
What are some compliance and management products and processes for risk analysis?

Please refer to your handout titled “Risk Analysis Metric”
<table>
<thead>
<tr>
<th>Performance Goal</th>
<th>Technical and organizational policies, procedures, and processes address the potential risks to PHI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Objective</td>
<td>The MIRT assesses and documents risks to PHI on a regular basis and as a result of system, operational, or other changes.</td>
</tr>
<tr>
<td>Purpose</td>
<td>To guide, measure, and communicate that the risk to PHI has been assessed across the organization.</td>
</tr>
<tr>
<td>Indicators of Effectiveness</td>
<td>Up-to-date, signed, and disseminated policy for conducting information security risk assessments that includes:</td>
</tr>
<tr>
<td>LEVEL 1</td>
<td>1. A Purpose and Scope that states expected goals and boundaries;</td>
</tr>
<tr>
<td></td>
<td>2. Responsibilities; and</td>
</tr>
<tr>
<td></td>
<td>3. Criteria for meeting the requirements.</td>
</tr>
<tr>
<td>LEVEL 2</td>
<td>Up-to-date, signed, and disseminated procedures for conducting information security risk assessments that include:</td>
</tr>
<tr>
<td></td>
<td>1. Clarification on where, how, when, about what, and to whom a particular procedure applies;</td>
</tr>
<tr>
<td></td>
<td>2. Clearly defined roles and responsibilities; and</td>
</tr>
<tr>
<td></td>
<td>3. Appropriate points of contact.</td>
</tr>
<tr>
<td>LEVEL 3</td>
<td>Implemented and reinforced procedures for conducting information security risk assessments in a consistent manner through:</td>
</tr>
<tr>
<td></td>
<td>1. Distribution to, and periodic acknowledgment from MIRT members of their awareness and acceptance of responsibility;</td>
</tr>
<tr>
<td></td>
<td>2. Management of compliance throughout the life of the PHI; including creation, reception, use, edit, transfer, disclosure, deletion, and tracking;</td>
</tr>
<tr>
<td></td>
<td>3. Updated MIRT position descriptions that accurately identify and reflect skill needs and responsibilities;</td>
</tr>
<tr>
<td></td>
<td>4. Planning, implementing, and maintaining a training and awareness program tailored for MIRT;</td>
</tr>
<tr>
<td></td>
<td>5. Scheduling a risk assessment;</td>
</tr>
<tr>
<td></td>
<td>6. Conducting a risk assessment;</td>
</tr>
<tr>
<td></td>
<td>7. Drafting a risk assessment report;</td>
</tr>
<tr>
<td></td>
<td>8. Presenting a risk assessment report to senior executive staff; and</td>
</tr>
<tr>
<td></td>
<td>9. Review and approval by senior executive staff of the risk assessment (OCTAVE$^{SM}$) conducted within the last 3 years?</td>
</tr>
<tr>
<td>Example Metric: Risk Analysis</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>LEVEL 4</strong></td>
<td></td>
</tr>
<tr>
<td>MTF routinely evaluates policies and procedures for adequacy and effectiveness. Activities include:</td>
<td></td>
</tr>
<tr>
<td>1. A documented and implemented plan of action to progress through Level 4;</td>
<td></td>
</tr>
<tr>
<td>2. Senior executive staff establishes quality requirements for OCTAVE℠;</td>
<td></td>
</tr>
<tr>
<td>3. Senior executive staff reviews, documents, and communicates recommendations for improvement of each completed OCTAVE℠;</td>
<td></td>
</tr>
<tr>
<td>4. Senior executive staff properly constitutes, ensures training, and monitors meeting attendance of the MISRT;</td>
<td></td>
</tr>
<tr>
<td>5. Regular risk assessments by MISRT in response to system, operational, and other changes;</td>
<td></td>
</tr>
<tr>
<td>6. Date of last risk assessment: ____________________; and</td>
<td></td>
</tr>
<tr>
<td>7. Routine preparation and transmittal of reports relating to risk assessments from MISRT to senior executive staff.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEVEL 5</th>
<th>The consideration of HIPAA requirements is pervasive in the culture of the MTF. Evidence includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A documented and implemented plan of action to progress through Level 5;</td>
<td></td>
</tr>
<tr>
<td>2. An implemented and enforced formal methodology, and an ongoing program to identify and institutionalize best practices;</td>
<td></td>
</tr>
<tr>
<td>3. The Service Surgeon General formally adopts and enforces the use of OCTAVE℠ for MTF information security risk assessment;</td>
<td></td>
</tr>
<tr>
<td>4. The MTF shares lessons learned and best practices in executing OCTAVE℠;</td>
<td></td>
</tr>
<tr>
<td>5. Documented evidence that senior management ensures effective remedial action is taken on issues, the prioritization of significant issues, and the development of action plans; and</td>
<td></td>
</tr>
<tr>
<td>6. Local Program Objective Memorandum (POM) and allocation of needed resources are based on the identified costs and benefits of managing and sustaining health information assurance through information security risk assessment.</td>
<td></td>
</tr>
</tbody>
</table>

| Data Source | OCTAVE℠ reports; Risk Information Management Resource (RIMR), archives of reports to senior executive staff on risk assessment |

<table>
<thead>
<tr>
<th>Levels of Effectiveness</th>
<th>LEVEL 1</th>
<th>LEVEL 2</th>
<th>LEVEL 3</th>
<th>LEVEL 4</th>
<th>LEVEL 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Training and Awareness Example

- \textit{THAT} your workforce has completed training is important...
- \textit{WHAT} your workforce does after training is as important

- Do you test and validate that training is working?
Training and Awareness Metrics

- Management and statistical metrics have the same goal, different approach and evidence.
- Management metric focuses on processes and products to gauge compliance.
- Statistical metric relies on percentage completion of training per job description.
Comparing the Two Types of Metrics

- **Goal**: All workforce members understand responsibilities for appropriate use and protection of PHI

Management:
- **Objective**: Develop and implement a local HIPAA awareness and training program for all members of the workforce

Statistical:
- **Objective**: Train all workforce members on use and protection of PHI
Evidence of Implementation

- **Management:** The HIPAA Compliance Officer reports to senior management monthly on the status of the local training and awareness program.

- **Statistical:** Documented pass percentages for job positions.

### Pass Percentage for Job Positions

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Students:</td>
<td>15720</td>
</tr>
<tr>
<td>No. of Students Complete:</td>
<td>13730</td>
</tr>
<tr>
<td>No. of Students Incomplete:</td>
<td>1990</td>
</tr>
<tr>
<td>Percentage of Students Complete:</td>
<td>87.34%</td>
</tr>
<tr>
<td>Students 31-60 Days Delinquent:</td>
<td>133</td>
</tr>
<tr>
<td>Students 61-90 Days Delinquent:</td>
<td>163</td>
</tr>
<tr>
<td>Students 90+ Days Delinquent:</td>
<td>1057</td>
</tr>
</tbody>
</table>
Management and Statistical Metrics

- Handling these separately and keeping them distinct allows for meaningful comparison and trending without bias.
- For example:
  - A statistical level of effectiveness score of 5, but a management level of effectiveness score of 2 may suggest difficulty in sustaining the Pass Percentages.
  - Conversely, a low statistical score and a high management score may indicate positive trends in the near future.
Accounting of Disclosure Example
Common Goal

- Applies to both Management and Statistical metrics

- **Goal**: To protect and enhance rights of beneficiaries by allowing them control of inappropriate use and disclosure of their PHI
Objectives

- **Management**: The MTF implements a process for authorizing and accounting all disclosures, and provides accountings to patients upon request in a timely manner.

- **Statistical**: The MTF accurately authorizes, tracks, and accounts for disclosures.
Evidence of Implementation

- **Management**: The HIPAA Privacy Officer regularly reports to senior executive staff on issues pertaining to accounting of disclosures, and mitigation progress.

- **Statistical**: Comparison of recorded disclosures in PHIMT versus Release of Information records (ROI).
Level of Effectiveness

- **Management**: Based on policies, procedures, implementation, evaluation, and extent to which it has been institutionalized

- **Statistical**: Number of disclosures recorded in the PHIMT against the number based on ROI
  - Level 1 → 0% - 25%
  - Level 2 → 26% - 74%
  - Level 3 → 75% - 84.9%
  - Level 4 → 85% - 94.9%
  - Level 5 → 95% - 100%
Using a Metric
Metrics Provide Multiple Benefits

- **Guide** development and refinement of existing HIPAA program
- **Measure** effectiveness of implementation with enterprise-wide framework
- **Communicate** progress and issues to senior executive staff and higher levels
Guide and Measure Implementation

- Initially achieve core compliance but seek to improve over time
- One metric for each HIPAA requirement
- Suitable for internal and external review
Framework of Effectiveness

- Level 1: Do you have a local policy?
- Level 2: Are your procedures sent to your workforce?
- Level 3: Are local procedures implemented?
- Level 4: Do you test and validate the procedures?
- Level 5: Do senior executive staff fully support the program with funding and resource needs?
Using the Framework of Effectiveness

- Levels of Effectiveness
  - Represent stages of institutional development
  - Requirements for each Level guide steps to take
  - Determining Level: Exhaustive and Cumulative

<table>
<thead>
<tr>
<th>Level of Effectiveness</th>
<th>LEVEL 1</th>
<th>LEVEL 2</th>
<th>LEVEL 3</th>
<th>LEVEL 4</th>
<th>LEVEL 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Responsibilities

- HIPAA Security Official / Privacy Officer
  - Jointly coordinate activities of the MIRT
  - Ensure implementation of requirements
  - Measure effectiveness
  - Report results to senior executive staff
Responsibilities

- MIRT manages all related activities
  - Completes self-assessment
  - Conducts risk assessment
  - Executes metrics
  - Brief results to management

- Senior Executive Staff
  - Staffs, funds, and oversees MIRT
  - Reviews and authorizes self-assessment reports, risk assessment methodology, metrics
  - Regularly reviews health information protection program
You’ve measured aspects of your program, and have a lot of information. Now what?

<table>
<thead>
<tr>
<th>Requirement</th>
<th>LEVEL 1</th>
<th>LEVEL 2</th>
<th>LEVEL 3</th>
<th>LEVEL 4</th>
<th>LEVEL 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Analysis</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Management</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Statistical</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Improving Your Program

- Enhance your program by through trending, analysis, and information sharing
  - Trending enables you to detect possible problems
  - Analysis determines the details of problems
  - Information sharing promotes awareness to prevent negative impact
Reporting on Effectiveness

- Overdue Requirements
  Reported Monthly
  - *What has not been done.* All requirements that have not been addressed within predetermined threshold (*delinquent*) as determined by risk analysis

- Active Requirements
  Reported Quarterly
  - *What is being done.* The vulnerabilities whose mitigation is in progress. Requirements whose mitigation fall outside of acceptable thresholds are reported as Overdue
Reporting on Effectiveness

- Resolved Requirements
  Reported Quarterly
  - What has been done. Successfully addressed vulnerabilities, as of the current quarter, whose mitigation has been verified and validated

- Compliant Requirements
  Reported Annually
  - What does not require action. The requirements that are not applicable, whose risk has been accepted, or have been successfully resolved
Improving the Enterprise

- Reporting effectiveness enables enterprise-wide trending, analysis, and higher level oversight
  - Identify and mitigate local issues efficiently
  - Unify improvements across the enterprise
  - Promote cross-organization collaboration that establishes basis for cost-effective solutions
Keys to Success

- Involvement of HIPAA Security Officials, HIPAA Privacy Officers, and cross-discipline personnel
- Senior leadership buy-in
- Beta testing with diverse site selection
- Receptive to issues, comments, suggestions
- Remember: this is good business
Our Commitment

The TRICARE Management Activity (TMA) Privacy Office is committed to ensuring the Privacy and Security of patient information at every level as we deliver the best medical care possible to those we serve.

Confidentiality ---- Integrity ---- Availability
Resources

- TMA Privacy Web Site: www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- Contact us at the TMA Privacy Office: privacymail@tma.osd.mil

Questions?
Accomplishments
HIPAA Application Suite

- Learning Management System
  - Delivers online customized HIPAA Privacy and Security courses to 160,000+ Military Health System (MHS) personnel
  - Captures the MHS organizational hierarchy and tracks student learning activities

- Protected Health Information Management Tool
  - Simplifies/automates manual processes such as disclosure accounting, PHI access, and alternative communication requests
  - Patient demographics pre-populated (over 9 million records)

- HIPAA BASICS™
  - Online tool for conducting baseline assessment of HIPAA Privacy compliance
  - Reporting capabilities at various levels of the organizational hierarchy
Communications

- Help Desk (email and outbound phone support)
  - Assists tool users with subject matter and technical issues.
  - Assist beneficiaries with concerns

- TMA Privacy Office Website
  - Information Papers
  - Policy and Procedures
  - Forms/Templates
  - Workforce Training Announcements
  - Customizable presentations for special interest groups

- Listserv
  - Periodic updates on new postings to website and related industry news
  - Training announcements
  - Tool modification and downtime bulletins
Training and Awareness

- Learning Management System
  - Online role specific training courses
- WebEx (just in time training)
  - Interactive online training
  - Includes presentations, live demonstrations, open discussions/Q&A
  - Attendance and credit tracked through student’s LMS account
- 2005 U. S. Distance Learning Association 21st Century Best Practices Award

- Annual Training Conferences
  - Attended by Military Treatment Facility HIPAA Privacy and Security Officers
  - Four identical sessions held each year in various geographic locations
  - Topics include: Privacy and Security Essentials, War gaming exercises, Uses and Disclosures, Tool training, Risk Management, Metrics, Complaint Process