Overview of Medical Devices and HIPAA Security Compliance

Wednesday, March 9, 2005

Stephen L. Grimes, FACCE
Chair, Medical Device Security Workgroup
Healthcare Information and Management Systems Society (HIMSS)
Chair, HIPAA Task Force
American College of Clinical Engineering (ACCE)
Senior Consultant & Analyst
Strategic Health Care Technology Associates
Medical Device Security: Is this just a HIPAA issue?

NO! …. Even if HIPAA were thrown out, Medical Device Security is a necessity … not just a regulation

- Medical device security … particularly data integrity & data availability … is critical to healthcare quality, timeliness, and cost-effectiveness

- Today, a reasonable standard of care cannot be maintained without an effective an Information Security Management Program in place that includes biomedical technology
HIPAA’s Security Rule

Implications for Biomedical Devices & Systems
Security Risks to Healthcare Technology

Make sure you are addressing more than the tip of the risk!

The inventory of biomedical devices & systems in a typical hospital is 3-4 times larger than the IT inventory.
Significant Medical Device Industry Trends

- Medical devices and systems are being designed and operated as special purpose computers … more features are being automated, increasing amounts of medical data are being collected, analyzed and stored in these devices.

- There has been a rapidly growing integration and interconnection of disparate medical (and information) technology devices and systems where medical data is being increasingly exchanged.
Information Technology Systems

**Mission Critical**
Activities, processing, etc., that are deemed vital to the organization's business success or existence. If a *Mission Critical* application fails, crashes, or is otherwise unavailable to the organization, it will have a significant negative impact upon the business.

Examples of *Mission Critical* applications include accounts/billing, customer balances, ADT processes, JIT ordering, and delivery scheduling.
Biomedical Technology Systems

**Life Critical**

Devices, systems and processes that are deemed vital to the patient’s health and quality of care. If a *Life Critical* system fails or is otherwise compromised, it will have a significant negative impact on the patient's health, quality of care or safety.

Examples of *Life Critical* systems include physiologic monitoring, imaging, radiation therapy, and clinical laboratory systems.
HIPAA Security requires Risk Analysis: 
*Risks Associated with IT vs Biomedical Systems*
HIPAA’s Security Rule

*Implications for Biomedical Technology*

Why is security an issue for biomedical technology?
Because compromise in ePHI can affect

- **Integrity or Availability** … can result in improper diagnosis or therapy of patient resulting in harm (even death) because of delayed or inappropriate treatment

- **Confidentiality** … can result in loss of patient privacy … and, as a consequence, may result in financial loss to patient and/or provider organization
HIPAA’s Security Rule

Implications for Biomedical Technology

Standalone with ePHI
HIPAA’s Security Rule

Implications for Biomedical Technology

Both Standalone

and

Networked Systems with ePHI
HIPAA’s Security Rule

Overview of Compliance Process
HIPAA’s Security Rule

Compliance Overview

Information Security Management (ISM) Program

Risk Analysis & Management Plan (RAMP)
HIPAA’s Security Rule
Compliance Overview

Establish effective **Info Security Management (ISM)** program:

1) **Assign** security official & establish information security committee

2) **Develop necessary policies** as per security **standards**

3) **Develop necessary procedures**, physical/technical safeguards as per **implementation specifications**

4) **Implement** Policies/procedures, Business associate agreements, Educate workforce & Install/Configure security “tools”

5) **Test** implementation

6) **Integrate** security measures into organization-wide program

**GOAL:** HIPAA Compliance & an Effective Info Security Program
HIPAA’s Security Rule Compliance Overview

Information Security Committee

- Clinical Engineering
- Information Security Official
- Information Services / Information Technology
- Facilities Engineering
- Materials Management / Purchasing
- Quality Assurance
- Risk Management
- Compliance Officer
- Privacy Officer
- Human Resources
- Staff Education / Inservice
- Administration
- Core Members
- Ad Hoc Members
- Representatives of device users (i.e., clinical staff)
HIPAA’s Security Rule

Compliance Overview

Establish Risk Analysis/Management Plan (RAMP):

1) Conduct inventory (identify sources of ePHI) and survey current security practices & resources
2) Identify and Assess Security Risks
3) Establish Priorities
4) Determine Security Gap (i.e., need for additional safeguards) following “best practices” and Security Rule’s Standards and Implementation Specifications
5) Formulate/Implement Plan for Risk Mitigation Process incorporating Risk-based Priorities
6) Test & Measure Effectiveness of Risk Mitigation Process (Improving as Necessary)
Compliance Overview
Risk Analysis/Management

1) Conduct Inventory

- Identify biomedical devices & systems that maintain and/or transmit ePHI
- For each affected device/system, determine:
  - Types of ePHI
  - Who has access & who needs access
  - Description of any connections with other devices
  - Types of security measures currently employed

New!
HIMSS Manufacturers Disclosure Statement for Medical Device Security (MDS²)

© HIMSS / ACCE / ECRI ~ 17

March 9, 2005
Nov 8, 2004
Compliance Overview
Risk Analysis/Management

1) and Survey current security practices & resources ... to analyze existing processes

- Policies & procedures
- Training programs
- Tools & security measures

<table>
<thead>
<tr>
<th>9.2.4</th>
<th>ACCE/ECRI Security Assessment Survey Questionnaire</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I. Administrative Safeguards [§164.308]</strong></td>
<td></td>
</tr>
<tr>
<td><strong>A. Security management process [§164.308(a)(1)(i)]</strong></td>
<td>Implement policies and procedures to prevent, detect, contain and correct security violations...</td>
</tr>
<tr>
<td><strong>Risk analysis [§164.308(8)(1)(ii)(A)] (REQUIRED).</strong> 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>1. Has an inventory been conducted of all biomedical devices and systems, and have those devices/systems maintaining or transmitting ePHI been identified?</strong></td>
</tr>
<tr>
<td></td>
<td><strong>2. For each inventoried biomedical device/system maintaining or transmitting ePHI, has a description of that ePHI been documented?</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Policy</th>
<th>Procedures</th>
<th>Implemented</th>
<th>Tested</th>
<th>Integrated</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Source:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comments:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date/Source:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

March 9, 2005 © HIMSS / ACCE / ECRI ~ 18
Create/Input ePHI

- Keyboard
- Scanning - bar code - magnetic - OCR
- Imaging - photo - medical image
- Biometrics
- Voice Recognition

Maintain ePHI

Component, Device, or System

- Hard Disk
- Memory (e.g., RAM)
- Disk
- Tape
- Digital Memory Card
- Optical disk, CD-ROM, DVD

Transmit/Receive ePHI

- Disk
- Tape
- Digital Memory Card
- Optical disk, CD-ROM, DVD
- Wired Networks Private or Public, Leased or Dial-up lines, Internet
- Wireless Networks

March 9, 2005
Physiologic Monitor

where ePHI may consist of patient identifying information and the following data:

- ECG waveform
- Blood pressure
- Heart rate
- Temp
- $O_2$ Saturation
- Respiration
- Alarms
Compliance Overview

Inventory of Devices/Systems

Infusion pump

where ePHI may consist of

patient identifying information

and the following data:

- Flow Rate
- Volume delivered
- Alarms
Compliance Overview

Inventory of Devices/Systems

- **Ventilator**
  
  where ePHI may consist of patient identifying information and the following data:
  
  - Flow Rate
  - Volume Delivered
  - Respiration (Breaths Per Minute)
  - O\textsubscript{2} Saturation
  - Alarms
Compliance Overview

Inventory of Devices/Systems

- Laboratory analyzer
  where ePHI may consist of
  patient identifying information and the
  following data:
    - Blood related
      - Hemoglobin
      - Glucose
      - Gas
      - pH
      - Electrolyte
    - Urine related
      - Albumin
      - Creatinine
      - Bilirubin
Compliance Overview

Inventory of Devices/Systems

MRI, CT Scanner, Diagnostic Ultrasound

where ePHI may consist of patient identifying information and the following data:

- Image
2) Assess risk with respect to confidentiality, integrity, availability:

- **Criticality**
  Categorize level of risk/vulnerability (e.g., high, medium, low) to CIA

- **Probability**
  Categorize the likelihood of risk (e.g., frequent, occasional, rare) to CIA

- **Composite Score** for Criticality/Probability
Taking into account **Criticality**: Assess Risk associated with compromises to **Integrity** of ePHI

<table>
<thead>
<tr>
<th>Data</th>
<th>Actual</th>
<th>Maintained/Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient ID</td>
<td>7813244</td>
<td>7813254</td>
</tr>
<tr>
<td>Heart Rate</td>
<td>60 bpm</td>
<td>35 bpm</td>
</tr>
<tr>
<td>Blood Pressure</td>
<td>120/80 mmHg</td>
<td>90/50 mmHg</td>
</tr>
<tr>
<td>Temp</td>
<td>98.6º F</td>
<td>89.6º F</td>
</tr>
<tr>
<td>SpO2</td>
<td>92%</td>
<td>92%</td>
</tr>
</tbody>
</table>
Taking into account **Criticality**: Assess Risk associated with compromises to **Availability** of ePHI

### Data

<table>
<thead>
<tr>
<th>Data</th>
<th>Actual</th>
<th>Maintained/Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient ID</td>
<td>7813244</td>
<td>XXXXXXX</td>
</tr>
<tr>
<td>Heart Rate</td>
<td>60 bpm</td>
<td>XX bpm</td>
</tr>
<tr>
<td>Blood Pressure</td>
<td>120/80 mmHg</td>
<td>XXX/XX mmHg</td>
</tr>
<tr>
<td>Temp</td>
<td>98.6º F</td>
<td>XX.Xº F</td>
</tr>
<tr>
<td>SpO2</td>
<td>92%</td>
<td>XX%</td>
</tr>
</tbody>
</table>
Taking into account **Criticality**: Assess Risk associated with compromises to **Confidentiality** of ePHI

<table>
<thead>
<tr>
<th>Data</th>
<th>Actual</th>
<th>Maintained/Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient ID</td>
<td>7813244</td>
<td>7813244</td>
</tr>
<tr>
<td>Heart Rate</td>
<td>60 bpm</td>
<td>60 bpm</td>
</tr>
<tr>
<td>Blood Pressure</td>
<td>120/80 mmHg</td>
<td>120/80 mmHg</td>
</tr>
<tr>
<td>Temp</td>
<td>98.6°F</td>
<td>98.6°F</td>
</tr>
<tr>
<td>SpO2</td>
<td>92%</td>
<td>92%</td>
</tr>
</tbody>
</table>

Central Station

Clinician with Authorized Access

UnAuthorized Access

Patient Monitor

Physiologic Monitor

Patient ID: 7813244

Heart Rate: 60 bpm

Blood Pressure: 120/80 mmHg

Temp: 98.6°F

SpO2: 92%
## Assessing **Criticality** of Risk Associated with Biomedical Devices/Systems with ePHI

<table>
<thead>
<tr>
<th>RISK LEVEL</th>
<th>Impact on Patient</th>
<th>Impact on Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>Potential degree to which health care would be adversely impacted by compromise of availability or integrity of ePHI</td>
<td>Potential degree to which privacy would be adversely impacted by compromise of confidentiality of ePHI</td>
</tr>
</tbody>
</table>
|            | Serious impact to patient's health (including loss of life) due to:  
  - misdiagnosis,  
  - delayed diagnosis or  
  - improper, inadequate or delayed treatment | Could identify patient and their diagnosis | Extremely grave damage to organization's interests |
|            | Serious damage | Major $1,000K | Imprisonment and/or large fines |
| **Medium** | Minor impact to patient's health due to:  
  - misdiagnosis,  
  - delayed diagnosis or  
  - improper, inadequate or delayed treatment | Could identify patient and their health information (but from which a diagnosis could not be derived) | Serious damage |
|            | Minor damage | Moderate $100K | Moderate Fines |
| **Low**    | Minor Impact | Could identify patient | Minor damage |
|            | Minor damage | Minor $10K | None |

March 9, 2005 © HIMSS / ACCE / ECRI ~ 29
Assessing *Probability* of Risks Associated with Biomedical Devices/Systems with ePHI

- **Frequent**
  Likely to occur (e.g., once a month)

- **Occasional**
  Probably will occur (e.g., once a year)

- **Rare**
  Possible to occur (e.g., once every 5-10 years)
Assessing **Criticality** & **Probability** of Risks associated with Biomedical Devices/Systems with ePHI

Determining the Criticality/Probability Composite Score

<table>
<thead>
<tr>
<th>Criticality</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rare</td>
</tr>
<tr>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
</tr>
</tbody>
</table>
Compliance Overview

Risk Analysis/Management

3) Establish priorities

- Use Criticality/Probability composite score to prioritize risk mitigation efforts
- Conduct mitigation process giving priority to devices/systems with highest scores (i.e., devices/systems that represent the most significant risks)
4) **Determine security gap**

- Determine what measures are necessary to safeguard data
- Compare list of necessary measures with existing measures identified during biomedical device/system inventory process
- Prepare gap analysis for devices/systems detailing additional security measures necessary to mitigate recognized risks (addressing devices/systems according to priority)
Compliance Overview
Risk Analysis/Management

5) Formulate & implement mitigation plan

- Formulate written mitigation plan incorporating
  - additional security measures required (i.e., policies, procedures, technical & physical safeguards)
  - priority assessment, and
  - schedule for implementation

- Implement plan & document process
Compliance Overview

Risk Analysis/Management

6) Monitor process

- Establish on-going monitoring system (including a security incident reporting system) to insure mitigation efforts are effective

- Document results of regular audits of security processes
Compliance Overview
Risk Analysis/Management

Prepare a Risk Mitigation Worksheet

<table>
<thead>
<tr>
<th>Device Type of Data</th>
<th>Security Element</th>
<th>Possible Sources of Risk to Data</th>
<th>Consequences of Data Compromise</th>
<th>Criticality Score</th>
<th>Probability Score</th>
<th>Composite Score (Priority)</th>
<th>Mitigation plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physiologic Monitor</td>
<td>Integrity</td>
<td>- Device “out of calibration”</td>
<td>- Misdiagnosis (i.e., diagnostic device and interpretation of bad data can lead to misdiagnosis)</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>- Device to be included in program that ensures adequate scheduled maintenance &amp; calibration</td>
</tr>
<tr>
<td>ECG Waveform</td>
<td></td>
<td>- Electromagnetic Interference (EMI) or other environmental factors</td>
<td>- Inappropriate or delayed treatment (due to misdiagnosis)</td>
<td></td>
<td></td>
<td></td>
<td>- Policy/procedure restricting or controlling use of EMI generating devices in areas where this device is operated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Data modified by unauthorized personnel or processes (accessing locally or remotely...this includes computer viruses, worms)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Incorporate network firewall, VPN as necessary where these devices are networked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Erroneous data input (by processes or personnel)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Locate operating devices in areas only accessible to authorized personnel and patients</td>
</tr>
</tbody>
</table>

1 Identify ePHI
2 Identify & Assess Risks
3 Establish Priorities
4 Determine Gap
5 Formulate & Implement Plan
6 Test & Measure Effectiveness of Plan
HIPAA’s Security Rule
Overview of Compliance Process

Security Management

Document

Security Plan
0. Acquire working knowledge of HIPAA and appoint a Security Official.
1. Develop security policies.
2. Develop security procedures and technical/physical safeguards.
3. Implement safeguards
   > Policies/procedures
   > Business associate agreements
   > Educational programs
   > Security tools/measures
4. Test implemented safeguards
5. Integrate security program elements.

Document

Risk Analysis and Management

Document

Risk Assessment
1. Inventory, identify, and survey devices/systems containing ePHI.
2. Assess security policies, procedures, and safeguards.
3. Identify what, if any, security precautions have been taken.
4. Determine risk levels associated with data criticality and probability.

Document

Planning and Mitigation
1. Prioritize mitigation efforts according to assessed risk levels.
2. Apply security measures, including:
   > Administrative safeguards
   > Physical safeguards
   > Technical safeguards where risks have been identified.
3. Conduct staff education and training.

Document

Monitoring
Evaluate effectiveness of security measures through:
1. Periodic audits
2. Incident reporting

Feedback and Review Process

March 9, 2005
© HIMSS / ACCE / ECRI ~ 37
Questions?

Stephen L. Grimes, FACCE
slgrimes@shcta.com
Strategic Health Care Technology Associates
www.SHCTA.com

Health Information and Management Systems Society
www.himms.org
American College of Clinical Engineering (ACCE)
www.accenet.org
ECRI
www.ecri.org