Presentation

ACCE / ECRI Information for Biomedical Technology:
A HIPAA Compliance Guide ©

November 22, 2004

CD-ROM Based
ACCE / ECRI
Information Security for Biomedical Technology:
A HIPAA Compliance Guide™

- Details compliance process
  - Security Management
  - Risk Analysis & Management
- Provides variety of compliance tools, including
  - Matrix of security standards & implementation specifications
  - Biomedical Equipment Survey Form & Questionnaire
  - Risk Mitigation Worksheet
  - Security Assessment Survey Questionnaire
  - Sample policies/procedures
  - Security incident report
  - Business associate agreement with security provisions
  - Management templates for project planning and budgeting
  - Bibliography, Definitions, and relevant On-line Resources
**HIPAA’s Final Security Rule**

"Standards & Implementation Specifications"

**Key elements/tools**

Standards & Implementation Specifications laid out in Matrix

<table>
<thead>
<tr>
<th>Sections</th>
<th>Standards</th>
<th>Implementation Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.308(a)(1)</td>
<td>(i) Security management process: Implement policies and procedures to prevent, detect, contain, and correct security violations...</td>
<td>(i)(A) Risk analysis <em>(REQUIRED)</em>. 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>
</tr>
<tr>
<td></td>
<td></td>
<td>(ii)(D) Risk management <em>(REQUIRED)</em>. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section §164.306(a).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(ii)(C) Sanction policy <em>(REQUIRED)</em>. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(ii)(D) Information system activity review <em>(REQUIRED)</em>. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.</td>
</tr>
<tr>
<td>§164.308(a)(2)</td>
<td>(i) Assigned security responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity...</td>
<td><em>(REQUIRED)</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>(REQUIRED)</em></td>
</tr>
<tr>
<td>§164.308(a)(3)</td>
<td>(i) Workforce security: Implement policies and procedures to ensure that all members of its workforce have appropriate access...</td>
<td><em>(ADDRESSABLE)</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>(ADDRESSABLE)</em></td>
</tr>
</tbody>
</table>

November 22, 2004 © ACCE/ECRI ~ 3 of 15
Key elements/tools

- Biomedical Equipment Survey Form to identify systems with ePHI, system vulnerabilities, and system security measures available
Key elements/tools

- Security Assessment Survey Questionnaire addressing level of compliance on *Standards* and *Implementation Specifications* for Administrative, Physical & Technical Safeguards

---

### 9.2.4 ACCE/ECRI Security Assessment Survey Questionnaire

<table>
<thead>
<tr>
<th>I. Administrative Safeguards [§164.308]</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Security management process [§164.308(a)(1)(i)]</td>
</tr>
<tr>
<td>Implement policies and procedures to prevent, detect, contain and correct security violations...</td>
</tr>
<tr>
<td>Risk analysis [§164.308(a)(1)(ii)(A)] (Required). 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>
</tr>
<tr>
<td>1. Has an inventory been conducted of all biomedical devices and systems, and have those devices/systems maintaining or transmitting ePHI been identified?</td>
</tr>
<tr>
<td>Policy</td>
</tr>
<tr>
<td>[ ] Yes [ ] No</td>
</tr>
<tr>
<td>Date/Source:</td>
</tr>
<tr>
<td>Comments:</td>
</tr>
<tr>
<td>2. For each inventoried biomedical device/system maintaining or transmitting ePHI, has a description of that ePHI been documented?</td>
</tr>
<tr>
<td>Policy</td>
</tr>
<tr>
<td>[ ] Yes [ ] No</td>
</tr>
<tr>
<td>Date/Source:</td>
</tr>
<tr>
<td>Comments:</td>
</tr>
</tbody>
</table>
Information Security for Biomedical Technology: A HIPAA Compliance Guide™

Key elements/tools

- Management templates for project scheduling and budgeting

Table 6.2: Project Budget (Time Estimates)

<table>
<thead>
<tr>
<th>Project Activities</th>
<th>Project Resources</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time Estimate</td>
<td>Cost</td>
</tr>
<tr>
<td>1. Preparation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Schedule/Budget Preparation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Orientation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Survey Policies/Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Interviews</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Document Review</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Physical Inspection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Analytical &amp; Microphysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Report &amp; Presentations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Other Activities</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project Personnel</th>
<th>Time Estimate</th>
<th>Cost</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Manager</td>
<td>(10)</td>
<td>(50)</td>
<td>(60)</td>
</tr>
<tr>
<td>Clinical Consultant</td>
<td>(10)</td>
<td>(50)</td>
<td>(60)</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

November 22, 2004
**Information Security for Biomedical Technology: A HIPAA Compliance Guide™**

**Key elements/tools**
- Risk Mitigation Worksheet for Medical Devices/Systems

### Risk Mitigation Worksheet for Medical Devices/Systems

<table>
<thead>
<tr>
<th>Device</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>
</table>
| Physiologic Monitor
  - ECG Waveform
  - Blood pressure
  - Heart Rate
  - Temp
  - O₂-Saturation | Integrity        | - Device "out of calibration"
  - Electromagnetic Interference (EMI) or other environmental factors
  - Data modified by unauthorized personnel or equipment tampering | - Misdiagnosis (i.e., diagnostic device and interpretation of bad data can lead to misdiagnosis)
  - Inappropriate or delayed treatment (due to misdiagnosis) | 1                 | 2                 | 6                    | - Device to be included in program that ensures adequate scheduled maintenance & calibration
  - Policy/ procedure restricting or controlling use of EMI generating devices in areas where this device is operated
  - Incorporate network firewall, VPN as necessary where device to be used                      |

**Steps**

1. **Identify ePHI**
2. **Identify & Assess Risks**
3. **Establish Priorities**
4. **Determine Gap**
5. **Formulate & Implement Plan**
6. **Test & Measure Effectiveness of Plan**
Information Security for Biomedical Technology: A HIPAA Compliance Guide™

Key elements/tools

- Policies & Procedures, Incident Reporting Form, and Business Associate Agreements
ACCE / ECRI Security Process

Manufacturer-supplied MDS² Forms

Biomedical Equipment Survey Forms (sources of ePHI)

Information Security Officer & Committee (risk assessment)

Risk Mitigation Worksheets (plan & priorities)

Security Assessment Survey Questionnaire (process analysis)

Criteria & Guidelines

Security Management Schedule & Budget

Administrative Safeguards
- Incident Reports & Audits
- Policies & Procedures; Contingency Plans

Business Associate Agreements

Training

Physical Safeguards
- Lock & Key
- Data Backup
- Intrusion & Environmental Alarms

Technical Safeguards
- Encryption
- Business Associate Agreements
- Biometrics
- Tokens
- Error Correction
- Firewalls

November 22, 2004
© ACCE/ECRI ~ 9 of 15
HIMSS Manufacturer Disclosure Statement for Medical Device Security (MDS²)

- Facilitates the providers’ review & analysis of the large volume of security-related information supplied by manufacturers for devices on the providers’ inventories
The MDS\textsuperscript{2} provides the Manufacturer’s Model-specific Description of

- Device ability to maintain/transmit ePHI
  - ✓ Is the device capable of maintaining or transmitting ePHI?
  - ✓ For those devices capable of maintaining/transmitting ePHI, a description of
    - • type of ePHI (e.g., demographic info, diagnostic/therapeutic info, etc.)
    - • device mechanisms for maintaining ePHI
    - • device mechanisms for transmitting ePHI

- Security features associated with the device
  - ✓ Safeguards provided with or incorporated in the device, including
    - □ Administrative
    - □ Physical
    - □ Technical
  - ✓ A list of any manufacturer-optional recommended safety practices
MDS² supplies key data to the ACCE / ECRI Biomedical Equipment Survey Form

MDS² Developed by HIMSS Medical Device Security Workgroup
ACCE / ECRI on Medical Device Security

CD-ROM based

Information Security for Biomedical Technology:
A HIPAA Compliance Guide™

Product Description
http://www.ecri.org/Products_and_Services/Products/HIPAA_Compliance_Guide/Default.aspx

Table of Contents
http://www.ecri.org/Marketingdocs/HIPAAATOCwithCover.pdf

Brochure and Order Form

Press Release

Discount for Members
HIMSS on Medical Device Security

- Web Site for HIMSS Medical Device Security Workgroup
  with Bibliography of relevant source material
  http://www.himss.org/ASP/topics_medicalDevice.asp

- HIMSS November 8, 2004 Press Release on MDS²

- Manufacturer's Disclosure Statement for Medical Device Security (MDS2) Form & Instructions
  http://www.himss.org/content/files/MDS2FormInstructions.pdf

- Manufacturers obtain free UMDNS (nomenclature) listing of their products by e-mailing ECRI at himss-mds@ecri.org
Questions?

Stephen L. Grimes, FACCE
slgrimes@nycap.rr.com

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