

New Tools & Initiatives for Addressing Medical Device Security

***Information Security for Biomedical Technology:
A HIPAA Compliance Guide™***

January 2005

The HIMSS logo is a white, multi-pointed starburst shape. Inside the starburst, the word "HIMSS" is written in a bold, sans-serif font. The "i" is lowercase and blue, while the "H", "M", "S", "S" are uppercase and black. A small registered trademark symbol (®) is located to the upper right of the "S".

HIMSS®

Stephen L. Grimes FACCE
Chair, Medical Device Security Workgroup
Health Information and Management Systems (HIMSS)
Principal Associate
Strategic Health Care Technology Associates (SHCTA)

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

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

9.1 HIPAA Security Standards and Implementation Specifications Matrix*

Administrative Safeguards

SECTIONS	STANDARDS	IMPLEMENTATION SPECIFICATIONS	Policies	Procedures
§164.308(a)(1)	(i) Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations ...	(ii)(A) Risk analysis (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.		
		(ii)(B) Risk management (REQUIRED). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section §164.306(a).		
		(ii)(C) Sanction policy (REQUIRED). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	X	X
		(ii)(D) Information system activity review (REQUIRED). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.		X
§164.308(a)(2)	(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	(REQUIRED)	X	X
§164.308(a)(3)	(i) Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access	(ii)(A) Authorization and/or supervision (ADDRESSABLE). Implement procedures for the authorization and/or supervision of workforce members who work with electronic		X

ACCE / ECRI

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

Key elements/tools

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

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

9.2.3 ACCE/ECRI Biomedical Equipment Survey Form

Instructions

- Question 1 answers to questions 4, 5, and 6 will help determine whether question 7 should be answered "Yes" or "No."
- Questions 8-12 indicate whether a mitigating measure is present or not applicable (N/A). However, determination of applicability may require further investigation and review after setting priorities for developing mitigating strategies.

ID #	Description	Serial #	Manufacturer
Model		Location	
Dept	Owner		

Mfg or Rep Contact Info	Name	Title	Dept
Company Name	Tel #	email	

1. Is this device capable of maintaining or transmitting electronic Protected Health Information (ePHI)? Yes No
Contact manufacturer if necessary to answer this or other device-specific questions. If yes, then complete the remainder of this form.

2. Data element(s) that qualifies health information as ePHI (check all that apply)

<input type="checkbox"/> Name	<input type="checkbox"/> Device ID #	<input type="checkbox"/> Unique Identifying #, Characteristic, or Code
<input type="checkbox"/> Treatment Date	<input type="checkbox"/> Biometric ID	<input type="checkbox"/> Other
<input type="checkbox"/> Med Record #	<input type="checkbox"/> Location or Address	
<input type="checkbox"/> Account #	<input type="checkbox"/> Image (e.g., photo, video, radiograph with identifying characteristics)	

3. Input source of ePHI (check all that apply)

<input type="checkbox"/> Keyboard, Keypad	<input type="checkbox"/> Voice Recognition	<input type="checkbox"/> Interconnect Cable
<input type="checkbox"/> Scanning (bar code, magnetic, OCR)	<input type="checkbox"/> Diskette, Removable Disk	<input type="checkbox"/> Telephone Line
<input type="checkbox"/> Image/Taking (optical, radiologic camera)	<input type="checkbox"/> Optical Disk, CD, DVD	<input type="checkbox"/> Wired or Wireless LAN, WAN, VPN, Intranet, Internet*
<input type="checkbox"/> Biometric (retina, finger/handprint, face, voice)	<input type="checkbox"/> Data Tape, Digital or Analog	

4. Is this device capable of maintaining ePHI? Yes No (if yes, check all that apply)

<input type="checkbox"/> Hard Disk	<input type="checkbox"/> Diskette, Removable Disk	<input type="checkbox"/> Data Tape, Digital or Analog
<input type="checkbox"/> Memory	<input type="checkbox"/> Optical Disk, CD, DVD	<input type="checkbox"/> PC Card or Memory Stick

5. Is this device capable of transmitting ePHI? Yes No (if yes, check all that apply)

<input type="checkbox"/> Diskette, Removable Disk	<input type="checkbox"/> PC Card or Memory Stick	<input type="checkbox"/> Wired or Wireless LAN, WAN, VPN, Intranet, Internet*
<input type="checkbox"/> Optical Disk, CD, DVD	<input type="checkbox"/> Interconnect Cable	
<input type="checkbox"/> Data Tape, Digital or Analog	<input type="checkbox"/> Telephone Line	

6. Output destination of ePHI (check all that apply)

<input type="checkbox"/> Displayed (e.g., onscreen)	<input type="checkbox"/> Optical Disk, CD, DVD	<input type="checkbox"/> Interconnect Cable
<input type="checkbox"/> Printed	<input type="checkbox"/> Data Tape, Digital or Analog	<input type="checkbox"/> Telephone Line
<input type="checkbox"/> Diskette, Removable Disk	<input type="checkbox"/> PC Card or Memory Stick	<input type="checkbox"/> Wired or Wireless LAN, WAN, VPN, Intranet, Internet*

7. Who is authorized to access ePHI associated with this device? (check all that apply)

<input type="checkbox"/> Medical Staff (i.e., physicians)	<input type="checkbox"/> Treatment/(diagnosis/therapy)	<input type="checkbox"/> Payment	<input type="checkbox"/> Operations*	<input type="checkbox"/> Other
<input type="checkbox"/> Clinical Staff (i.e., nursing, therapists)	<input type="checkbox"/> Treatment/(diagnosis/therapy)	<input type="checkbox"/> Payment	<input type="checkbox"/> Operations*	<input type="checkbox"/> Other
<input type="checkbox"/> Support Staff (i.e., laboratory, radiology)	<input type="checkbox"/> Treatment/(diagnosis/therapy)	<input type="checkbox"/> Payment	<input type="checkbox"/> Operations*	<input type="checkbox"/> Other
<input type="checkbox"/> Office Staff (i.e., medical records, billing)	<input type="checkbox"/> Treatment/(diagnosis/therapy)	<input type="checkbox"/> Payment	<input type="checkbox"/> Operations*	<input type="checkbox"/> Other
<input type="checkbox"/> Risk Management, Quality Management	<input type="checkbox"/> Treatment/(diagnosis/therapy)	<input type="checkbox"/> Payment	<input type="checkbox"/> Operations*	<input type="checkbox"/> Other
<input type="checkbox"/> Tech Staff (i.e., IT, clinical engineering)	<input type="checkbox"/> Treatment/(diagnosis/therapy)	<input type="checkbox"/> Payment	<input type="checkbox"/> Operations*	<input type="checkbox"/> Other
<input type="checkbox"/> Outside Organizations	<input type="checkbox"/> Treatment/(diagnosis/therapy)	<input type="checkbox"/> Payment	<input type="checkbox"/> Operations*	<input type="checkbox"/> Other
<input type="checkbox"/> Other	<input type="checkbox"/> Treatment/(diagnosis/therapy)	<input type="checkbox"/> Payment	<input type="checkbox"/> Operations*	<input type="checkbox"/> Other

*Attach network diagrams showing interconnections.
*Examples of Operations include maintenance, repair, quality assurance, safety, and risk management.

HIPAA Security Compliance Guide, V. 1.0 Appendix ©2004, ACCE/ECRI All Rights Reserved
Page A 28

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

9.2.3 ACCE/ECRI Biomedical Equipment Survey Form

8. Is this device on an inventory of devices/systems covered by the security program? Yes No N/A

9. What administrative safeguards are currently in place?

a. Are there security policies/procedures associated with this device that cover

i. Appropriate user?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
ii. Authorized users?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

b. Are users and service staff educated regarding security issues/procedures associated with this device? Yes No N/A

c. Is this device ever operated or serviced by a manufacturer, vendor, third party service, or other?

i. If the answer to 9c is yes, are there business associate agreements with this/these organization(s)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
ii. If the answer to 9c is yes, are records of access and/or removal maintained?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

d. Do contingency and emergency operations plans include provisions to access ePHI provided by this device? Yes No N/A

e. If ePHI data is backed up to ensure availability,

i. Are backups regular?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
ii. Are backup media rotated?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
iii. Are backups secured and stored in a safe location?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
iv. Does backup storage include off-site locations?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
v. Are backups clearly labeled?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

f. Are there redundant devices available to ensure ePHI availability? Yes No N/A

10. What physical safeguards are currently in place?

a. To ensure that the device is physically secure,

i. Is the device and any components containing ePHI physically secured (i.e., not removable), or is the device kept in a secure location accessible only to authorized users and support staff?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
ii. Are any removable media containing ePHI kept secured so as to be accessible only to authorized staff?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
iii. Are device displays containing ePHI physically observable only by authorized staff?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

b. Is ePHI access restricted by

i. Unique ID and password (properly formatted and periodically updated)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
ii. Lock and/or key, combination, PIN	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
iii. Biometric	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
iv. Token	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

c. Is access tracked (i.e., login monitoring)? Yes No N/A

d. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logout)? Yes No N/A

e. When media (containing ePHI) are no longer needed, are they

i. Physically altered, destroyed, or sanitized (i.e., erased and overwritten)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
ii. Deposited in a locked "destruction bin" for disposal by a bonded service?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

f. Is the device supplied with power during service interruptions by: battery/UPS, emergency generator? Yes No N/A

11. What technical safeguards are currently in place?

a. When exchanging ePHI with other devices (i.e., connected via cable, network, Internet, wireless), is ePHI

i. Transmitted via secured cable (i.e., no access possible via "unsecured" intermediate connections)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
ii. Encrypted prior to transmission over Internet, public network, or wireless?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
iii. Located on a device that is behind a firewall?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

b. Is ePHI data checked to verify it is authentic, uncorrupted, and free from unauthorized modification? Yes No N/A

c. Is the device computer based (e.g., PC based)? Yes No N/A

i. Does the device utilize virus protection and/or intrusion detection? Yes No N/A

ii. Are virus definitions updated regularly? Yes No N/A

iii. Does the device prevent boot-up from an unauthorized boot disk? Yes No N/A

d. Can the device be accessed remotely?

i. Does the system security restrict remote access to specific devices or locations?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
ii. Does the device log and provide an audit trail of remote-access activity?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

12. What is device criticality rating for ePHI confidentiality, integrity, and availability where	Confidentiality	Integrity	Availability
Low = 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Medium = 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
High = 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

13. What is device probability rating for ePHI confidentiality, integrity, and availability where	Confidentiality	Integrity	Availability
Rare	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Occasional = 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Frequent = 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

14. What is device composite criticality/probability score for ePHI confidentiality, integrity, and availability where criticality rating x probability rating = composite score	Confidentiality	Integrity	Availability
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Review Date: _____ Reviewer: _____

HIPAA Security Compliance Guide, V. 1.0 Appendix ©2004, ACCE/ECRI All Rights Reserved
Page A 29

ACCE / ECRI

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

Key elements/tools

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

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

9.2.4 ACCE/ECRI Security Assessment Survey Questionnaire													
I. Administrative Safeguards [§164.308]													
A. Security management process [§164.308(a)(1)(i)] Implement policies and procedures to prevent, detect, contain and correct security violations...													
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.													
1. Has an inventory been conducted of all biomedical devices and systems, and have those devices/systems maintaining or transmitting ePHI been identified?	<table border="1"><thead><tr><th>Policy</th><th>Procedures</th><th>Implemented</th><th>Tested</th><th>Integrated</th><th>N/A</th></tr></thead><tbody><tr><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td></td></tr></tbody></table> <p>Date/Source: _____</p> <p>Comments: _____</p>	Policy	Procedures	Implemented	Tested	Integrated	N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Policy	Procedures	Implemented	Tested	Integrated	N/A								
<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No									
2. For each inventoried biomedical device/system maintaining or transmitting ePHI, has a description of that ePHI been documented?	<table border="1"><thead><tr><th>Policy</th><th>Procedures</th><th>Implemented</th><th>Tested</th><th>Integrated</th><th>N/A</th></tr></thead><tbody><tr><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td><input type="checkbox"/> Yes <input type="checkbox"/> No</td><td></td></tr></tbody></table> <p>Date/Source: _____</p> <p>Comments: _____</p>	Policy	Procedures	Implemented	Tested	Integrated	N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Policy	Procedures	Implemented	Tested	Integrated	N/A								
<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No									

ACCE / ECRI

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

Key elements/tools

- Management templates for project scheduling and budgeting

Information Security for Biomedical Technology:
A HIPAA Compliance Guide™

Also see **Appendices 9.2.1, ACCE/ECRI Information Security Management Program Preliminary Project Schedule Worksheet, and 9.2.2, ACCE/ECRI Information Security Management Program Preliminary Project Budget Worksheet.**

Table 6.1: Project Schedule (time estimates)

Activity		Week Number (Units of Time)														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Initialization	1. Preparation	(24)	(12)													
	2. Schedule/Budget Preparation		(12)	(24)	(18)											
	3. Orientation					(16)										
RAMP	4. Survey Equipment						(40)	(40)	(40)							
	5. Survey Policies and Procedures															
	a. Interviews								(24)	(20)	(20)					
	b. Document Review									(20)	(20)	(20)				
	c. Physical Inspection									(40)	(40)	(40)				
	6. Analysis and Planning Preparation												(40)	(40)	(40)	
	7. Report & Presentation															(16)
Total Week Hours		(24)	(24)	(24)	(16)	(16)	(40)	(40)	(64)	(80)	(80)	(60)	(40)	(40)	(14)	
Project Manager Hours		(12)	(12)	(18)	(8)	(8)			(24)	(24)	(24)	(12)	(16)	(16)	(8)	
Clinical Engineering Consultant Hours		(12)	(12)	(6)	(8)	(8)	(8)	(8)	(8)	(24)	(24)	(16)	(24)	(16)	(8)	
Technical Analyst Hours							(32)	(32)	(32)	(32)	(32)	(32)				

HIPAA Security Compliance Guide, V. 1.0 © 2004, ACCE/ECRI All Rights Reserved

Information Security for Biomedical Technology:
A HIPAA Compliance Guide™

Table 6.2: Project Budget (time estimates)

Project Activities:	Project Resources			Total	
	Project Manager	Clinical Engineering Consultant	Technical Analyst	Hrs	Cost
1. PreparationHours	(24)	(12)		(36)	
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
2. Schedule & Budget PrepHours	(26)	(26)		(52)	
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
3. OrientationHours	(8)	(8)		(16)	
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
4. Survey EquipmentHours		(24)	(96)	(120)	
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
5. Survey Policies and Procedures					
a. Interviews.....Hours	(48)	(16)		(64)	
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
b. Document Review.....Hours	(36)	(24)		(60)	
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
c. Physical Inspection.....Hours		(24)	(96)	(120)	
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
6. Analysis & Plan PrepHours	(56)	(64)		(120)	
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
7. Report & PresentationHours	(8)	(8)		(16)	
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
8. Other (e.g., education)Hours					
.....Labor Cost					
.....Travel Expense					
.....Misc. Expense					
Total				(604)	

HIPAA Security Compliance Guide, V. 1.0 © 2004, ACCE/ECRI All Rights Reserved

ACCE / ECRI

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									
Device • Type of Data	Security Element	Possible Sources of Risk to Data	Consequences of Data Compromise	Criticality Score	Probability Score	Composite Score (Priority)	Mitigation plan	Responsible Party	Target Date for Mitigation
Physiologic Monitor • ECG Waveform • Blood pressure • Heart Rate • Temp • O ₂ Saturation	Integrity	- Device "out of calibration" - Electromagnetic Interference (EMI) or other environmental factors - Data modified by unauthorized personnel or processes (accessing locally	- 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 insures 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 these devices are networked	Dir. Clinical Engr.	
<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 2px solid blue; padding: 10px; text-align: center; width: 15%;"> <h1 style="margin: 0;">1</h1> <p style="margin: 0;">Identify ePHI</p> </div> <div style="border: 2px solid blue; padding: 10px; text-align: center; width: 25%;"> <h1 style="margin: 0;">2</h1> <p style="margin: 0;">Identify & Assess Risks</p> </div> <div style="border: 2px solid blue; padding: 10px; text-align: center; width: 15%;"> <h1 style="margin: 0;">3</h1> <p style="margin: 0;">Establish Priorities</p> </div> <div style="border: 2px solid blue; padding: 10px; text-align: center; width: 15%;"> <h1 style="margin: 0;">4</h1> <p style="margin: 0;">Determine Gap</p> </div> <div style="border: 2px solid blue; padding: 10px; text-align: center; width: 15%;"> <h1 style="margin: 0;">5</h1> <p style="margin: 0;">Formulate & Implement Plan</p> </div> </div> <div style="border: 2px solid blue; padding: 10px; text-align: center; margin-top: 10px;"> <h1 style="margin: 0;">6</h1> <p style="margin: 0;">Test & Measure Effectiveness of Plan</p> </div>									
Temp		- Physical assault (e.g., fire,					- Employ physical safeguards & alarms		

ACCE / ECRI

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

Key elements/tools

■ Policies & Procedures, Incident Reporting Form, and Business Associate Agreements

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

9.3.4 Sample Policies and Procedures

SUBJECT:	Security of Electronic Protected Health Information (ePHI): Intent and Definitions	No.:	
Prepared by:		Date:	
Approved by:		Date:	
		Effective Date:	
		Review/Renewal Date:	
Supersedes:	N/A	Old No.:	N/A
Related		No(s):	

Policies regarding Privacy and Security of electronic Protected Health Information (ePHI)

Intent: Ensure privacy and security of electronic Protected Health Information (ePHI) in a manner consistent with the provisions of the:

- Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191)
- Privacy and Security Rules (45 CFR Parts 160, 162, and 164)

Definitions:

- **Availability** is the property wherein data is accessible and usable on demand by an authorized person.
- **Business associate** is an individual or organization that is not a member of the workforce and performs or assists in the performance of an activity involving ePHI on behalf of <organization>. A **business associate contract** is an agreement between the business associate and <organization> wherein the business associate assures <organization> that it will take appropriate measures to ensure the privacy and security of any ePHI it may encounter, that it will permit <organization> to monitor these measures, and that failure of the business associate to employ these measures shall be sufficient grounds for <organization> to terminate the contract.
- **Chain-of-Custody Log** is a document listing the name, date(s) of custody, description of ePHI, and ePHI disposition on termination of custody for each staff member who takes responsibility for ePHI.
- **Confidentiality** is the property wherein data is not made available or disclosed to any unauthorized persons.
- **Integrity** is the property wherein data is accurate and has not been altered or destroyed in an unauthorized manner.
- **Protected Health Information (PHI)** (also known as **Individually Identifiable Health Information (IIHI)**) is defined as information that is a subset of health information, including demographic information collected from an individual, and that:
 - (a) is created or received by a healthcare provider
 - (b) relates to the past, present, or future health or condition of an individual, the provision of care to an individual, and
 - (c) identifies the individual.
- **Electronic Protected Health Information (ePHI)** is defined as PHI maintained or transmitted in electronic media.
- **Electronic Media** are defined as storage media or transmission media.
- **Sanctions** are either disciplinary measures applied to staff or penalties applied to third parties. When used, sanctions are applied commensurate with the degree to which <organization's> policies are violated. Sanctions may range up to dismissal for staff and up to termination of contracts or agreements with third parties.
- **Security** consists of the administrative, physical, and technical processes and systems put in place to safeguard the integrity, availability, and confidentiality of data.

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

9.3.3 Sample Information Security Incident Report and Procedure Outline

INFORMATION SECURITY INCIDENT REPORT	
Date/Time of Report:	Name and Contact Information of Individual Making Report:
Date/Time of Incident:	Location of Incident:
Description of Device/System Involved:	
Description of Media Involved:	
Storage Media: <ul style="list-style-type: none"><input type="checkbox"/> Hard Disk<input type="checkbox"/> Memory	Combination Storage and Transmission Media: <ul style="list-style-type: none"><input type="checkbox"/> Diskette or Other Removable Magnetic Disk<input type="checkbox"/> Optical Disk, CD, or DVD<input type="checkbox"/> Data Tape, Analog or Digital<input type="checkbox"/> PC Card or Memory Stick
Transmission Media: <ul style="list-style-type: none"><input type="checkbox"/> Interconnecting Cable<input type="checkbox"/> Telephone Line<input type="checkbox"/> Wired or Wireless LAN, WAN, VPN, Internet, Intranet	
Detailed Description of Incident:	
Check any applicable: <ul style="list-style-type: none"><input type="checkbox"/> Documentation Missing<input type="checkbox"/> Patient Information Abused/Disclosed	<ul style="list-style-type: none"><input type="checkbox"/> Login Failure<input type="checkbox"/> Data or Workstation Left Unattended<input type="checkbox"/> System Generated Message<input type="checkbox"/> Incremental Update Late<input type="checkbox"/> Emergency Service
Nature/Type of Security Incident: <ul style="list-style-type: none"><input type="checkbox"/> Small scale<input type="checkbox"/> Widespread	Confidentiality: <ul style="list-style-type: none"><input type="checkbox"/> Disclosure of Information<input type="checkbox"/> Unauthorized Access to Information<input type="checkbox"/> Description of Affected Information
Integrity: <ul style="list-style-type: none"><input type="checkbox"/> Modification or Corruption of Information<input type="checkbox"/> Loss or Destruction of Information<input type="checkbox"/> Diagnostic<input type="checkbox"/> Therapeutic<input type="checkbox"/> Billing<input type="checkbox"/> Other	Availability: <ul style="list-style-type: none"><input type="checkbox"/> Denial of Access to Information<input type="checkbox"/> Information Missing or Not Usable
Description of Actions Taken Immediately Following Incident:	
Witness Name(s) and Contact Information:	
Organization's Security Policy/Policies Violated: <ul style="list-style-type: none"><input type="checkbox"/> Yes<input type="checkbox"/> No	If Yes, What Aspects?
Description of Available Documentation (e.g., Extracts of Audit Reports) and Other Evidence:	
Remainder of Report to be Completed by Security Officer:	
Date Completed by Information Security Officer:	Date Reviewed by Security Committee:
Seriousness of Incident: <ul style="list-style-type: none">Potential for DamageActual Damage	<ul style="list-style-type: none">HighMediumLow
Analysis of Incident:	
Recommendations to Prevent Future Incidents:	
Administrative: <ul style="list-style-type: none"><input type="checkbox"/> Policies/Procedures<input type="checkbox"/> Education/Training<input type="checkbox"/> Modification to or Additional BA Agreements<input type="checkbox"/> Other	Physical: <ul style="list-style-type: none"><input type="checkbox"/> Relocation/Reposition Device or Media<input type="checkbox"/> Securing Device, Components, or Media<input type="checkbox"/> Data Backup<input type="checkbox"/> Other
Technical: <ul style="list-style-type: none"><input type="checkbox"/> Data Encryption<input type="checkbox"/> Access Controls (e.g., Password, Biometric)<input type="checkbox"/> Intrusion Detection, Audit Controls, Firewall<input type="checkbox"/> Other	
Action(s) Taken:	
Report Submitted to Authorities? <input type="checkbox"/> Yes <input type="checkbox"/> No	Type of Authority:
Date Submitted:	

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

9.3.2 Sample Business Associate Contract with Security Provisions

THIS AGREEMENT, made and entered into this [day] day of [month], [year], by and between the [healthcare provider's name] ("Covered Entity"), an organization with a mailing address of [healthcare provider's address], and [Business Associate's name] ("Business Associate"), an individual/organization with a mailing address of [Business Associate's address] (individually a "Party" and collectively the "Parties").

1. Purpose

- The purpose of this Agreement is to
- comply with the Privacy Rule and Security Rule provisions of the Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191) and
 - provide for the privacy of Protected Health Information (PHI) and the security of electronic Protected Health Information (ePHI) that is received, accessed, created, or maintained by or transmitted from the Business Associate in the performance of a function or activity on behalf of the Covered Entity.

2. Definitions

- Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule and the Security Rule.
- Business Associate. "Business Associate" shall mean [insert name of Business Associate].
 - Covered Entity. "Covered Entity" shall mean [insert name of Covered Entity].
 - Electronic Protected Health Information (ePHI). "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103.
 - Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
 - Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164.
 - Protected Health Information (PHI). "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of the Covered Entity.
 - Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.
 - Secretary. "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his designee.
 - Security Rule. "Security Rule" shall mean Health Insurance Reform: Security Standards at 45 CFR Parts 160, 162, and 164.

3. Obligations and Activities of the Parties with Respect to PHI/ePHI

3.1 Obligations of the Business Associate

- With respect to use and/or disclosure of PHI, the Business Associate agrees to
- not use or disclose PHI other than as permitted or required by the Agreement or as Required By Law;
 - use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement;
 - mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement;
 - report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which

ACCE / ECRI Security Process



MDS² supplies key data to the ACCE / ECRI Biomedical Equipment Survey Form

Manufacturer Disclosure Statement for Medical Device Security - MDS²

RECOMMENDED SECURITY PRACTICES

Document ID: _____ Document Release Date: _____
 Software Release Date: _____ Department: _____

Device Category: _____ Manufacturer: _____ Telephone #: _____ Yes/No/N/A/Note: _____
 Device Model: _____ Software Revision: _____ Title: _____ Email: _____
 Manufacturer or Representative Contact Information: _____ Company Name: _____

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) (As defined by HIPAA Security Rule, 45 CFR Part 164)

1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?
 2. Types of ePHI data elements that can be maintained by the device:
 a. Demographic (e.g., name, address, location, unique identification number)?
 b. Medical record (e.g., medical record #, accession #, test or treatment data with identifying characteristics)?
 c. Diagnostic/therapeutic (e.g., photos/radiograph, test results, or physiologic data with identifying characteristics)?
 d. Other unstructured text entered by device user/operator?
 3. Maintaining ePHI: Can the device
 a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?
 b. Import/export ePHI with other systems?
 c. Import/export ePHI for the transmitting, importing/exporting of ePHI? Can the device
 a. Display ePHI (e.g., video display)?
 b. Generate hardcopy reports or images containing ePHI?
 c. Retrieve ePHI from or import/export ePHI via dedicated cable connection (e.g., IEEE 1394, serial)?
 d. Transmit/receive ePHI via a network wireless connection (e.g., LAN, WAN, VPN, Intranet, Internet)?
 e. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)?
 f. Other _____ Yes/No/N/A/Note: _____

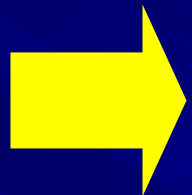
ADMINISTRATIVE SAFEGUARDS
 5. Does manufacturer offer operator and technical support training or documentation on device security features?
 6. What underlying operating system(s) (including version number) are used by the device? Yes/No/N/A/Note: _____

PHYSICAL SAFEGUARDS
 7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove or tamper with)?
 8. Does the device have an integral data backup capability (i.e., backup onto removable media (i.e., a storage device) or an internal drive (i.e., a storage device) or other device)?
 9. Can the device boot from uncontrolled media (i.e., a storage device or other device)? Yes/No/N/A/Note: _____

TECHNICAL SAFEGUARDS
 10. Can the device be serviced remotely (i.e., via a network or other device)?
 11. Can the device be serviced remotely (i.e., via a network or other device)?
 12. Level of encryption used to protect ePHI:
 a. None
 b. Inadequate (i.e., does not meet NIST 1973, FIPS 197, or other cryptographic standard)
 c. Adequate (i.e., meets NIST 1973, FIPS 197, or other cryptographic standard)
 13. Does the device have a secure boot process?
 14. Can the device be serviced remotely (i.e., via a network or other device)?
 15. Does the device have a secure boot process?
 16. Does the device have a secure boot process?
 17. Can the device be serviced remotely (i.e., via a network or other device)?
 18. Does the device have a secure boot process?
 19. Does the device have a secure boot process?

Adapted from Information Security for Biomedical Technology: A HIPAA Compliance Guide*
 ACCE - the American College of Clinical Engineering
 MDS² v 1.0 (2004-11-01)

© 2004, HIMSS. All rights reserved.



MDS² Developed by HIMSS Medical Device Security Workgroup

Information Security for Biomedical Technology: A HIPAA Compliance Guide*

9.2.3 ACCE/ECRI Biomedical Equipment Survey Form

9. Is this device on an inventory of devices/systems covered by the security program? Yes No N/A

9.2.3 ACCE/ECRI Biomedical Equipment Survey Form

Instructions:
 • Questions 1-12 indicate whether a mitigating measure is present or not applicable (N/A). However, determination of applicability may require further investigation and review after setting priorities for developing mitigating strategies.

1. Is this device capable of maintaining or transmitting electronic Protected Health Information (ePHI)?
 a. Name _____ Title _____ Manufacturer _____
 b. Treatment Date _____ Location _____
 c. Account # _____ Med Record # _____ Dept _____
 d. Other _____
 e. Identifying #, Characteristic, or Code _____

2. Data element(s) that qualifies health information as ePHI (check all that apply):
 Device ID #
 Biometric ID
 Location or Address
 Image (e.g., photo, video, radiograph with identifying characteristics)
 Keyboard, Keypad
 Scanning (bar code, magnetic, OCR)
 Image-Taking (optical, radiologic, etc.)
 Biometric (retina, finger/thumbprint)

3. Input source of ePHI:
 Hard Disk
 Memory
 Other _____

4. Is this device capable of:
 Hard Disk
 Memory
 Other _____

5. Is this device capable of:
 Hard Disk
 Memory
 Other _____

6. Other _____

7. Who is authorized to access ePHI?
 Medical Staff
 Clinical Staff
 Support Staff
 Office Staff (i.e., Administrative, Billing, etc.)
 Tech Staff (i.e., IT, Biomedical, etc.)
 Outside Organization
 Other _____

8. Attach network diagrams showing examples of operations including:
 LAN, WAN, VPN, Intranet, Internet
 Digital or Analog Memory Stick
 Other _____

9. Other _____

10. Other _____

11. Other _____

12. Other _____

13. Other _____

14. Other _____

15. Other _____

16. Other _____

17. Other _____

18. Other _____

19. Other _____

20. Other _____

21. Other _____

22. Other _____

23. Other _____

24. Other _____

25. Other _____

26. Other _____

27. Other _____

28. Other _____

29. Other _____

30. Other _____

31. Other _____

32. Other _____

33. Other _____

34. Other _____

35. Other _____

36. Other _____

37. Other _____

38. Other _____

39. Other _____

40. Other _____

41. Other _____

42. Other _____

43. Other _____

44. Other _____

45. Other _____

46. Other _____

47. Other _____

48. Other _____

49. Other _____

50. Other _____

51. Other _____

52. Other _____

53. Other _____

54. Other _____

55. Other _____

56. Other _____

57. Other _____

58. Other _____

59. Other _____

60. Other _____

61. Other _____

62. Other _____

63. Other _____

64. Other _____

65. Other _____

66. Other _____

67. Other _____

68. Other _____

69. Other _____

70. Other _____

71. Other _____

72. Other _____

73. Other _____

74. Other _____

75. Other _____

76. Other _____

77. Other _____

78. Other _____

79. Other _____

80. Other _____

81. Other _____

82. Other _____

83. Other _____

84. Other _____

85. Other _____

86. Other _____

87. Other _____

88. Other _____

89. Other _____

90. Other _____

91. Other _____

92. Other _____

93. Other _____

94. Other _____

95. Other _____

96. Other _____

97. Other _____

98. Other _____

99. Other _____

100. Other _____

101. Other _____

102. Other _____

103. Other _____

104. Other _____

105. Other _____

106. Other _____

107. Other _____

108. Other _____

109. Other _____

110. Other _____

111. Other _____

112. Other _____

113. Other _____

114. Other _____

115. Other _____

116. Other _____

117. Other _____

118. Other _____

119. Other _____

120. Other _____

121. Other _____

122. Other _____

123. Other _____

124. Other _____

125. Other _____

126. Other _____

127. Other _____

128. Other _____

129. Other _____

130. Other _____

131. Other _____

132. Other _____

133. Other _____

134. Other _____

135. Other _____

136. Other _____

137. Other _____

138. Other _____

139. Other _____

140. Other _____

141. Other _____

142. Other _____

143. Other _____

144. Other _____

145. Other _____

146. Other _____

147. Other _____

148. Other _____

149. Other _____

150. Other _____

151. Other _____

152. Other _____

153. Other _____

154. Other _____

155. Other _____

156. Other _____

157. Other _____

158. Other _____

159. Other _____

160. Other _____

161. Other _____

162. Other _____

163. Other _____

164. Other _____

165. Other _____

166. Other _____

167. Other _____

168. Other _____

169. Other _____

170. Other _____

171. Other _____

172. Other _____

173. Other _____

174. Other _____

175. Other _____

176. Other _____

177. Other _____

178. Other _____

179. Other _____

180. Other _____

181. Other _____

182. Other _____

183. Other _____

184. Other _____

185. Other _____

186. Other _____

187. Other _____

188. Other _____

189. Other _____

190. Other _____

191. Other _____

192. Other _____

193. Other _____

194. Other _____

195. Other _____

196. Other _____

197. Other _____

198. Other _____

199. Other _____

200. Other _____

201. Other _____

202. Other _____

203. Other _____

204. Other _____

205. Other _____

206. Other _____

207. Other _____

208. Other _____

209. Other _____

210. Other _____

211. Other _____

212. Other _____

213. Other _____

214. Other _____

215. Other _____

216. Other _____

217. Other _____

218. Other _____

219. Other _____

220. Other _____

221. Other _____

222. Other _____

223. Other _____

224. Other _____

225. Other _____

226. Other _____

227. Other _____

228. Other _____

229. Other _____

230. Other _____

231. Other _____

232. Other _____

233. Other _____

234. Other _____

235. Other _____

236. Other _____

237. Other _____

238. Other _____

239. Other _____

240. Other _____

241. Other _____

242. Other _____

243. Other _____

244. Other _____

245. Other _____

246. Other _____

247. Other _____

248. Other _____

249. Other _____

250. Other _____

251. Other _____

252. Other _____

253. Other _____

254. Other _____

255. Other _____

256. Other _____

257. Other _____

258. Other _____

259. Other _____

260. Other _____

261. Other _____

262. Other _____

263. Other _____

264. Other _____

265. Other _____

266. Other _____

267. Other _____

268. Other _____

269. Other _____

270. Other _____

271. Other _____

272. Other _____

273. Other _____

274. Other _____

275. Other _____

276. Other _____

277. Other _____

278. Other _____

279. Other _____

280. Other _____

281. Other _____

282. Other _____

283. Other _____

284. Other _____

285. Other _____

286. Other _____

287. Other _____

288. Other _____

289. Other _____

290. Other _____

291. Other _____

292. Other _____

293. Other _____

294. Other _____

295. Other _____

296. Other _____

297. Other _____

298. Other _____

299. Other _____

300. Other _____

301. Other _____

302. Other _____

303. Other _____

304. Other _____

305. Other _____

306. Other _____

307. Other _____

308. Other _____

309. Other _____

310. Other _____

311. Other _____

312. Other _____

313. Other _____

314. Other _____

315. Other _____

316. Other _____

317. Other _____

318. Other _____

319. Other _____

320. Other _____

321. Other _____

322. Other _____

323. Other _____

324. Other _____

325. Other _____

326. Other _____

327. Other _____

328. Other _____

329. Other _____

330. Other _____

331. Other _____

332. Other _____

333. Other _____

334. Other _____

335. Other _____

336. Other _____

337. Other _____

338. Other _____

339. Other _____

340. Other _____

341. Other _____

342. Other _____

343. Other _____

344. Other _____

345. Other _____

346. Other _____

347. Other _____

348. Other _____

349. Other _____

350. Other _____

351. Other _____

352. Other _____

353. Other _____

354. Other _____

355. Other _____

356. Other _____

357. Other _____

358. Other _____

359. Other _____

360. Other _____

361. Other _____

362. Other _____

363. Other _____

364. Other _____

365. Other _____

366. Other _____

367. Other _____

368. Other _____

369. Other _____

370. Other _____

371. Other _____

372. Other _____

373. Other _____

374. Other _____

375. Other _____

376. Other _____

377. Other _____

378. Other _____

379. Other _____

380. Other _____

381. Other _____

382. Other _____

383. Other _____

384. Other _____

385. Other _____

386. Other _____

387. Other _____

388. Other _____

389. Other _____

390. Other _____

391. Other _____

392. Other _____

393. Other _____

394. Other _____

395. Other _____

396. Other _____

397. Other _____

398. Other _____

399. Other _____

400. Other _____

401. Other _____

402. Other _____

403. Other _____

404. Other _____

405. Other _____

406. Other _____

407. Other _____

408. Other _____

409. Other _____

410. Other _____

411. Other _____

412. Other _____

413. Other _____

414. Other _____

415. Other _____

416. Other _____

417. Other _____

418. Other _____

419. Other _____

420. Other _____

421. Other _____

422. Other _____

423. Other _____

424. Other _____

425. Other _____

426. Other _____

427. Other _____

428. Other _____

429. Other _____

430. Other _____

431. Other _____

432. Other _____

433. Other _____

434. Other _____

435. Other _____

436. Other _____

437. Other _____

438. Other _____

439. Other _____

440. Other _____

441. Other _____

442. Other _____

443. Other _____

444. Other _____

445. Other _____

446. Other _____

447. Other _____

448. Other _____

449. Other _____

450. Other _____

451. Other _____

452. Other _____

453. Other _____

454. Other _____

455. Other _____

456. Other _____

457. Other _____

458. Other _____

459. Other _____

460. Other _____

461. Other _____

462. Other _____

463. Other _____

464. Other _____

465. Other _____

466. Other _____

467. Other _____

468. Other _____

469. Other _____

470. Other _____

471. Other _____

472. Other _____

473. Other _____

474. Other _____

475. Other _____

476. Other _____

477. Other _____

478. Other _____

479. Other _____

480. Other _____

481. Other _____

482. Other _____

483. Other _____

484. Other _____

485. Other _____

486. Other _____

487. Other _____

488. Other _____

489. Other _____

490. Other _____

491. Other _____

492. Other _____

493. Other _____

494. Other _____

495. Other _____

496. Other _____

497. Other _____

498. Other _____

499. Other _____

500. Other _____

501. Other _____

502. Other _____

503. Other _____

504. Other _____

505. Other _____

506. Other _____

507. Other _____

508. Other _____

509. Other _____

510. Other _____

511. Other _____

512. Other _____

513. Other _____

514. Other _____

515. Other _____

516. Other _____

517. Other _____

518. Other _____

519. Other _____

520. Other _____

521. Other _____

522. Other _____

523. Other _____

524. Other _____

525. Other _____

526. Other _____

527. Other _____

528. Other _____

529. Other _____

530. Other _____

531. Other _____

532. Other _____

533. Other _____

534. Other _____

535. Other _____

536. Other _____

537. Other _____

538. Other _____

539. Other _____

540. Other _____

541. Other _____

542. Other _____

543. Other _____

544. Other _____

545. Other _____

546. Other _____

547. Other _____

548. Other _____

549. Other _____

550. Other _____

551. Other _____

552. Other _____

553. Other _____

554. Other _____

555. Other _____

556. Other _____

557. Other _____

558. Other _____

559. Other _____

560. Other _____

561. Other _____

562. Other _____

563. Other _____

564. Other _____

565. Other _____

566. Other _____

567. Other _____

568. Other _____

569. Other _____

570. Other _____

571. Other _____

572. Other _____

573. Other _____

574. Other _____

575. Other _____

576. Other _____

577. Other _____

578. Other _____

579. Other _____

580. Other _____

581. Other _____

582. Other _____

583. Other _____

584. Other _____

585. Other _____

586. Other _____

587. Other _____

588. Other _____

589. Other _____

590. Other _____

591. Other _____

592. Other _____

593. Other _____

594. Other _____

595. Other _____

596. Other _____

597. Other _____

598. Other _____

599. Other _____

600. Other _____

601. Other _____

602. Other _____

603. Other _____

604. Other _____

605. Other _____

606. Other _____

607. Other _____

608. Other _____

609. Other _____

610. Other _____

611. Other _____

612. Other _____

613. Other _____

614. Other _____

615. Other _____

616. Other _____

617. Other _____

618. Other _____

619. Other _____

620. Other _____

621. Other _____

622. Other _____

623. Other _____

624. Other _____

625. Other _____

626. Other _____

627. Other _____

628. Other _____

629. Other _____

630. Other _____

631. Other _____

632. Other _____

633. Other _____

634. Other _____

635. Other _____

636. Other _____

637. Other _____

638. Other _____

639. Other _____

640. Other _____

641. Other _____

642. Other _____

643. Other _____

644. Other _____

645. Other _____

646. Other _____

647. Other _____

648. Other _____

649. Other _____

650. Other _____

651. Other _____

652. Other _____

653. Other _____

654. Other _____

655. Other _____

656. Other _____

657. Other _____

658. Other _____

659. Other _____

660. Other _____

661. Other _____

662. Other _____

663. Other _____

664. Other _____

665. Other _____

666. Other _____

667. Other _____

668. Other _____

669. Other _____

670. Other _____

671. Other _____

672. Other _____

673. Other _____

674. Other _____

675. Other _____

676. Other _____

677. Other _____

678. Other _____

679. Other _____

680. Other _____

681. Other _____

682. Other _____

683. Other _____

684. Other _____

685. Other _____

686. Other _____

687. Other _____

688. Other _____

689. Other _____

690. Other _____

691. Other _____

692. Other _____

693. Other _____

694. Other _____

695. Other _____

696. Other _____

697. Other _____

698. Other _____

699. Other _____

700. Other _____

701. Other _____

702. Other _____

703. Other _____

704. Other _____

705. Other _____

706. Other _____

707. Other _____

708. Other _____

709. Other _____

710. Other _____

711. Other _____

712. Other _____

713. Other _____

714. Other _____

715. Other _____

716. Other _____

717. Other _____

718. Other _____

719. Other _____

720. Other _____

721. Other _____

722. Other _____

723. Other _____

724. Other _____

725. Other _____

726. Other _____

727. Other _____

728. Other _____

729. Other _____

730. Other _____

731. Other _____

732. Other _____

733. Other _____

734. Other _____

735. Other _____

736. Other _____

737. Other _____

738. Other _____

739. Other _____

740. Other _____

741. Other _____

742. Other _____

743. Other _____

744. Other _____

745. Other _____

746. Other _____

747. Other _____

748. Other _____

749. Other _____

750. Other _____

751. Other _____

752. Other _____

753. Other _____

754. Other _____

755. Other _____

756. Other _____

757. Other _____

758. Other _____

759. Other _____

760. Other _____

761. Other _____

762. Other _____

763. Other _____

764. Other _____

765. Other _____

766. Other _____

767. Other _____

768. Other _____

769. Other _____

770. Other _____

771. Other _____

772. Other _____

773. Other _____

774. Other _____

775. Other _____

776. Other _____

777. Other _____

778. Other _____

779. Other _____

780. Other _____

781. Other _____

782. Other _____

783. Other _____

784. Other _____

785. Other _____

786. Other _____

787. Other _____

788. Other _____

789. Other _____

790. Other _____

791. Other _____

792. Other _____

793. Other _____

794. Other _____

795. Other _____

796. Other _____

797. Other _____

798. Other _____

799. Other _____

800. Other _____

801. Other _____

802. Other _____

803. Other _____

804. Other _____

805. Other _____

806. Other _____

807. Other _____

808. Other _____

809. Other _____

810. Other _____

811. Other _____

812. Other _____

813. Other _____

814. Other _____

815. Other _____

816. Other _____

817. Other _____

818. Other _____

819. Other _____

820. Other _____

821. Other _____

822. Other _____

823. Other _____

824. Other _____

825. Other _____

826. Other _____

827. Other _____

828. Other _____

829. Other _____

830. Other _____

831. Other _____

832. Other _____

833. Other _____

834. Other _____

835. Other _____

836. Other _____

837. Other _____

838. Other _____

839. Other _____

840. Other _____

841. Other _____

842. Other _____

843. Other _____

844. Other _____

845. Other _____

846. Other _____

847. Other _____

848. Other _____

849. Other _____

850. Other _____

851. Other _____

852. Other _____

853. Other _____

854. Other _____

855. Other _____

856. Other _____

857. Other _____

858. Other _____

859. Other _____

860. Other _____

861. Other _____

862. Other _____

863. Other _____

864. Other _____

865. Other _____

866. Other _____

867. Other _____

868. Other _____

869. Other _____

870. Other _____

871. Other _____

872. Other _____

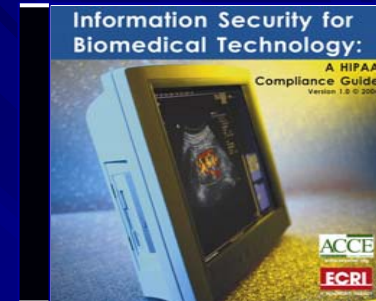
873

The screenshot shows the HIMSS website interface. At the top left is the HIMSS logo. To the right is a search bar with a 'SEARCH' button and a 'Powered by Google' logo. Below the logo is a navigation menu with links for Home, About HIMSS, Contact Us, and Member Login. A secondary menu contains links for News & Research, Topics & Tools, Professional Development, Conferences & Events, Membership, and HIMSS Store. The main content area features a sidebar on the left with a 'HIMSS Store' section containing various categories like Books & CDs, Ordering and Shipping Information, All, Ambulatory Care, Auto ID & Bar Coding, Clinical Decision Support, Clinical Informatics, Conference Proceedings and E-Sessions, Electronic Health Record, Financial Management and ROI, HIPAA, Privacy and Security, Integration & Interoperability, Management and Strategy, National Preparedness & Response, Patient Safety and Process Improvement, and Professional Certification. The main content area displays a product advertisement for 'Information Security for Biomedical Technology: A HIPAA Compliance Guide CD-ROM Just Released!' by ECRI. The advertisement includes a price list (\$495 for members, \$695 for non-members) and a 'BUY IT NOW >>' button. A yellow starburst graphic on the right side of the advertisement says 'Discount for Members'. Below the product title is a detailed description of the CD-ROM's content, including its purpose for meeting HIPAA's 2005 Security Rule deadline, the types of resources it provides (worksheets, policies, checklists, etc.), and its production by ECRI and the American College of Clinical Engineering. At the bottom of the page is a copyright notice for 2005 Healthcare Information and Management Systems Society, along with contact information for HIMSS in Chicago, IL.



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

<http://www.ecri.org/Marketingdocs/HIPAAcdromBROpdf.pdf>

<http://www.himss.org/asp/book.asp?ContentID=59138>

■ Press Release

http://www.ecri.org/Newsroom/Document_Detail.aspx?docid=20040604_125

Discount for
Members