New Tools & Initiatives for Addressing Medical Device Security

Information Security for Biomedical Technology: A HIPAA Compliance Guide™

January 2005

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* ™

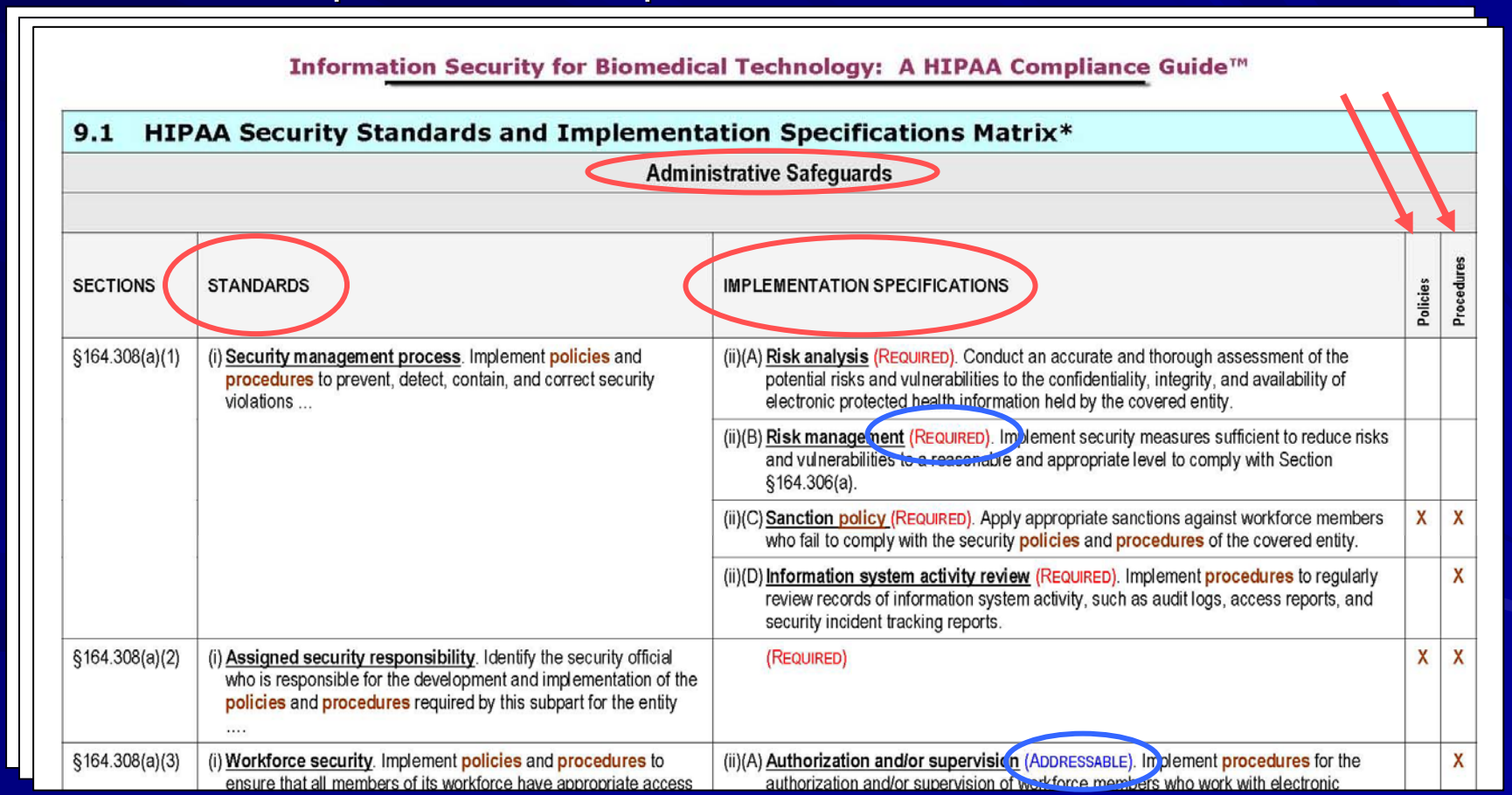
- Details compliance process
  - ✓ Security Management
  - ✓ Risk Analysis & Management
- Provides variety of compliance tools, including
  - ✓ Matrix of security standards & implementation specifications
  - ✓ Biomedical Equipment Survey Form & Questionnaire
  - ✓ Risk Mitigation Worksheet
  - ✓ Security 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 1 should be answered "Yes" or "No."
- Questions 9-12: 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		Manufacturer
Model		Serial #	Location
Dept		Owner	
Mfg or Rep Contact Info:	Name	Title	Dept
	Company Name	Tel #	e-mail

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)*
   ▫ Name ▫ Device ID # ▫ Unique Identifying #, Characteristic, or Code
   ▫ Treatment Date ▫ Biometric ID ▫ Other _____
   ▫ Med Record # ▫ Location or Address ▫ _____
   ▫ Account # ▫ Image (*e.g., photo, video, radiograph with identifying characteristics*) ▫ _____

3. Input source of ePHI *(check all that apply)*
   ▫ Keyboard, Keypad ▫ Voice Recognition ▫ Interconnect Cable
   ▫ Scanning (bar code, magnetic, OCR) ▫ Diskette, Removable Disk ▫ Telephone Line
   ▫ Image-Taking (optical, radiologic camera) ▫ Optical Disk, CD, DVD ▫ Wired or Wireless LAN, WAN, VPN, Intranet, Internet*
   ▫ Biometric (retina, finger-/handprint, face, voice) ▫ Data Tape, Digital or Analog

4. Is this device *capable of maintaining* ePHI? ▫ Yes ▫ No *(if yes, check all that apply)*
   ▫ Hard Disk ▫ Diskette, Removable Disk ▫ Data Tape, Digital or Analog
   ▫ Memory ▫ Optical Disk, CD, DVD ▫ PC Card or Memory Stick

5. Is this device *capable of transmitting* ePHI? ▫ Yes ▫ No *(if yes, check all that apply)*
   ▫ Diskette, Removable Disk ▫ PC Card or Memory Stick ▫ Wired or Wireless LAN, WAN, VPN, Intranet, Internet*
   ▫ Optical Disk, CD, DVD ▫ Interconnect Cable
   ▫ Data Tape, Digital or Analog ▫ Telephone Line

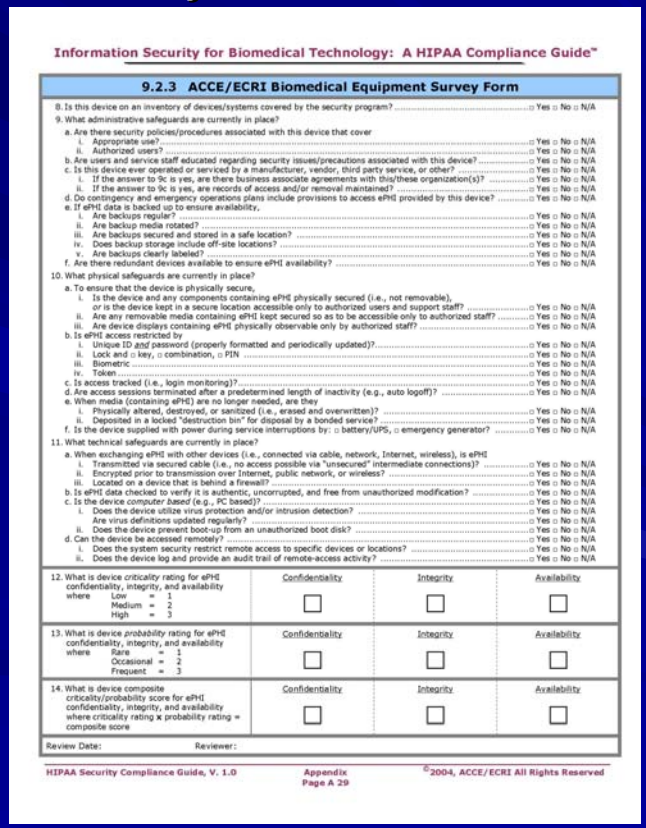
6. Output destination of ePHI *(check all that apply)*
   ▫ Displayed (e.g., onscreen) ▫ Optical Disk, CD, DVD ▫ Interconnect Cable
   ▫ Printed ▫ Data Tape, Digital or Analog ▫ Telephone Line
   ▫ Diskette, Removable Disk ▫ PC Card or Memory Stick ▫ Wired or Wireless LAN, WAN, VPN, Intranet, Internet*

7. Who is authorized to access ePHI associated with this device? *(check all that apply)*
   ▫ Medical Staff (i.e., physicians) ..... ▫ Treatment/(diagnosis/therapy) ▫ Payment ▫ Operations* ▫ Other _____
   ▫ Clinical Staff (i.e., nursing, therapists) ..... ▫ Treatment/(diagnosis/therapy) ▫ Payment ▫ Operations* ▫ Other _____
   ▫ Support Staff (i.e., laboratory, radiology) ..... ▫ Treatment/(diagnosis/therapy) ▫ Payment ▫ Operations* ▫ Other _____
   ▫ Office Staff (i.e., medical records, billing) ..... ▫ Treatment/(diagnosis/therapy) ▫ Payment ▫ Operations* ▫ Other _____
   ▫ Risk Management, Quality Management ..... ▫ Operations* ▫ Other _____
   ▫ Tech Staff (i.e., IT, clinical engineering) ..... ▫ Operations* ▫ Other _____
   ▫ Outside Organizations _____ ▫ Treatment/(diagnosis/therapy) ▫ Payment ▫ Operations* ▫ Other _____
   ▫ Other _____ ▫ Treatment/(diagnosis/therapy) ▫ Payment ▫ Operations* ▫ 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 Page A 28 ©2004, ACCE/ECRI All Rights Reserved



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 use? ..... ▫ Yes ▫ No ▫ N/A
      ii. Authorized users? ..... ▫ Yes ▫ No ▫ N/A
   b. Are users and service staff educated regarding security issues/precautions 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? ..... ▫ Yes ▫ No ▫ N/A
      i. If the answer to 9c is yes, are there business associate agreements with this/these organization(s)? ..... ▫ Yes ▫ No ▫ N/A
      ii. If the answer to 9c is yes, are records of access and/or removal maintained? ..... ▫ Yes ▫ No ▫ 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? ..... ▫ Yes ▫ No ▫ N/A
      ii. Are backup media rotated? ..... ▫ Yes ▫ No ▫ N/A
      iii. Are backups secured and stored in a safe location? ..... ▫ Yes ▫ No ▫ N/A
      iv. Does backup storage include off-site locations? ..... ▫ Yes ▫ No ▫ N/A
      v. Are backups clearly labeled? ..... ▫ Yes ▫ No ▫ 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? ..... ▫ Yes ▫ No ▫ N/A
      ii. Are any removable media containing ePHI kept secured so as to be accessible only to authorized staff? ..... ▫ Yes ▫ No ▫ N/A
      iii. Are device displays containing ePHI physically observable only by authorized staff? ..... ▫ Yes ▫ No ▫ N/A
   b. Is ePHI access restricted by
      i. Unique ID *and* password (properly formatted and periodically updated)? ..... ▫ Yes ▫ No ▫ N/A
      ii. Lock and ▫ key, ▫ combination, ▫ *PIN* ..... ▫ Yes ▫ No ▫ N/A
      iii. Biometric ..... ▫ Yes ▫ No ▫ N/A
      iv. Token ..... ▫ Yes ▫ No ▫ 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 logoff)? ..... ▫ 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)? ..... ▫ Yes ▫ No ▫ N/A
      ii. Deposited in a locked "destruction bin" for disposal by a bonded service? ..... ▫ Yes ▫ No ▫ 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)? ..... ▫ Yes ▫ No ▫ N/A
      ii. Encrypted prior to transmission over Internet, public network, or wireless? ..... ▫ Yes ▫ No ▫ N/A
      iii. Located on a device that is behind a firewall? ..... ▫ Yes ▫ No ▫ 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
      Are virus definitions updated regularly? ..... ▫ Yes ▫ No ▫ N/A
      ii. Does the device prevent boot-up from an unauthorized boot disk? ..... ▫ Yes ▫ No ▫ N/A
   d. Can the device be accessed remotely? ..... ▫ Yes ▫ No ▫ N/A
      i. Does the system security restrict remote access to specific devices or locations? ..... ▫ Yes ▫ No ▫ N/A
      ii. Does the device log and provide an audit trail of remote-access activity? ..... ▫ Yes ▫ No ▫ N/A

12. What is device *criticality* rating for ePHI confidentiality, integrity, and availability where Low = 1, Medium = 2, High = 3	Confidentiality ☐	Integrity ☐	Availability ☐
13. What is device *probability* rating for ePHI confidentiality, integrity, and availability where Rare = 1, Occasional = 2, Frequent = 3	Confidentiality ☐	Integrity ☐	Availability ☐
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 ☐
Review Date: Reviewer:			

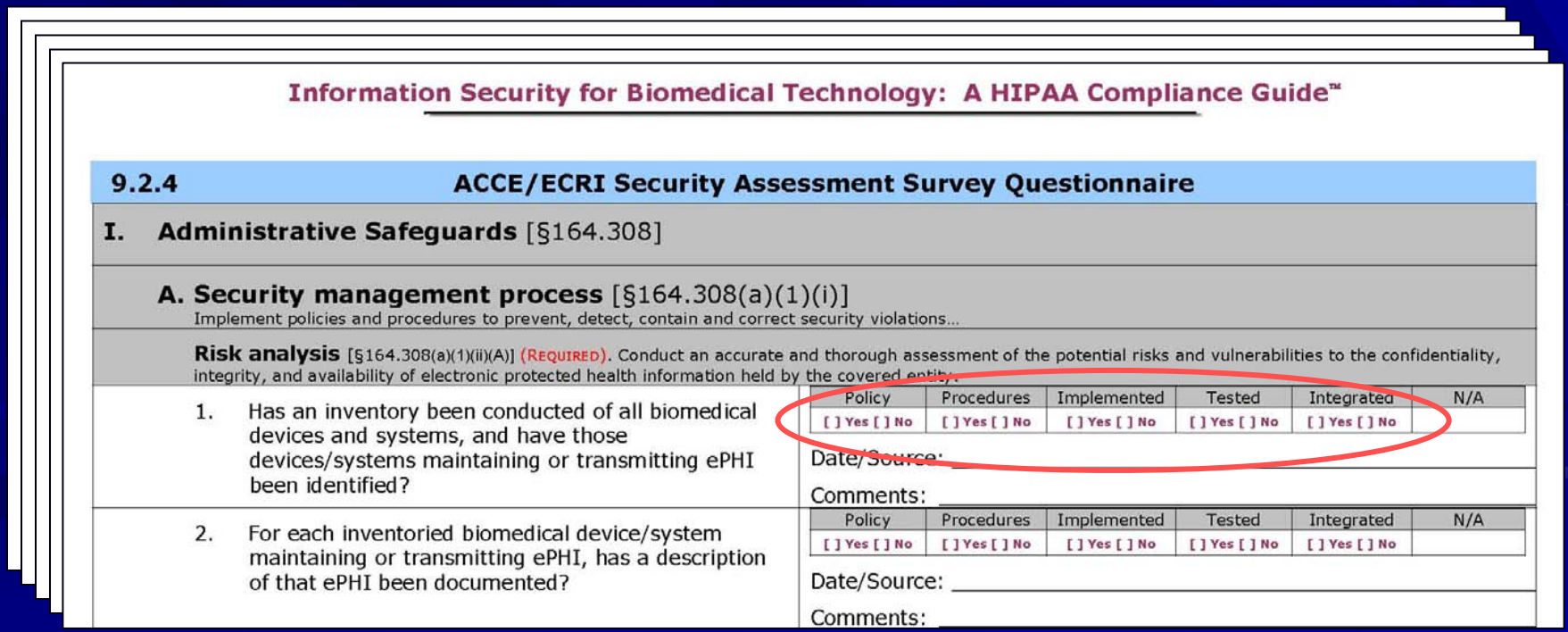
HIPAA Security Compliance Guide, V. 1.0 Appendix Page A 29 ©2004, ACCE/ECRI All Rights Reserved

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?

Policy	Procedures	Implemented	Tested	Integrated	N/A
[ ] Yes [ ] No	[ ] Yes [ ] No	[ ] Yes [ ] No	[ ] Yes [ ] No	[ ] Yes [ ] No	

Date/Source:

Comments:

2. For each inventoried biomedical device/system maintaining or transmitting ePHI, has a description of that ePHI been documented?

Policy	Procedures	Implemented	Tested	Integrated	N/A
[ ] Yes [ ] No	[ ] Yes [ ] No	[ ] Yes [ ] No	[ ] Yes [ ] No	[ ] Yes [ ] No	

Date/Source:

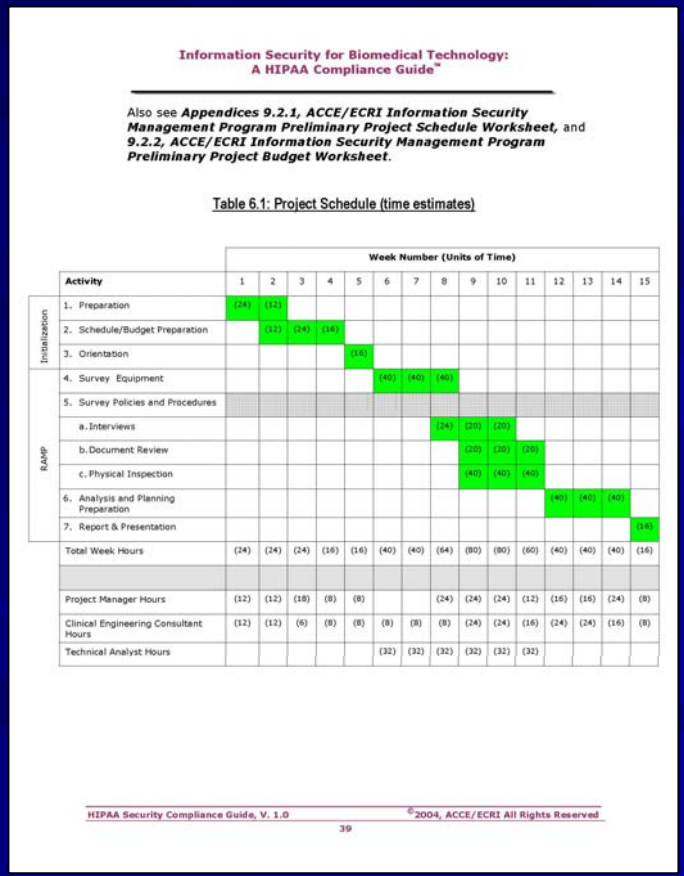
Comments:

ACCE / ECRI

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

Key elements/tools

- Management templates for project scheduling and budgeting



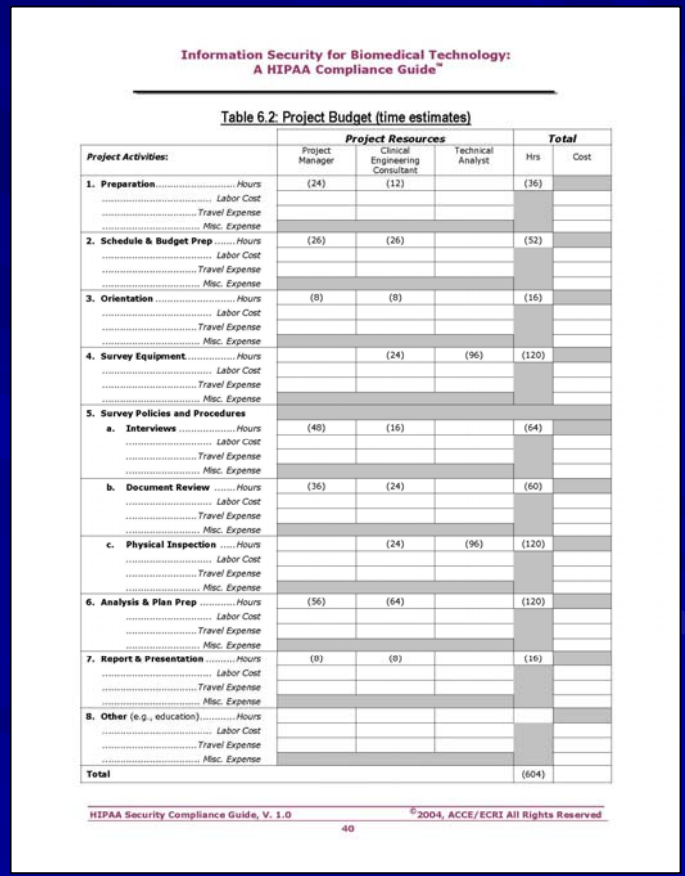
Information Security for Biomedical Technology:
A HIPAA Compliance Guide™

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)

		Week Number (Units of Time)													
	Activity	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)	(16)											
	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)	(40)	(16)
	Project Manager Hours	(12)	(12)	(18)	(8)	(8)			(24)	(24)	(24)	(12)	(16)	(16)	(24)	(8)
	Clinical Engineering Consultant Hours	(12)	(12)	(6)	(8)	(8)	(8)	(8)	(8)	(24)	(24)	(16)	(24)	(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
39



Information Security for Biomedical Technology:
A HIPAA Compliance Guide™

Table 6.2: Project Budget (time estimates)

Project Activities:	Project Resources: Project Manager	Clinical Engineering Consultant	Technical Analyst	Total: Hrs	Cost
1. Preparation ..... Hours	(24)	(12)		(36)	
..... Labor Cost					
..... Travel Expense					
..... Misc. Expense					
2. Schedule & Budget Prep ..... Hours	(26)	(26)		(52)	
..... Labor Cost					
..... Travel Expense					
..... Misc. Expense					
3. Orientation ..... Hours	(8)	(8)		(16)	
..... Labor Cost					
..... Travel Expense					
..... Misc. Expense					
4. Survey Equipment ..... Hours		(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 Prep ..... Hours	(56)	(64)		(120)	
..... Labor Cost					
..... Travel Expense					
..... Misc. Expense					
7. Report & Presentation ..... Hours	(8)	(8)		(16)	
..... Labor Cost					
..... Travel Expense					
..... Misc. Expense					
8. Other (e.g., education) ..... Hours					
..... Labor Cost					
..... Travel Expense					
..... Misc. Expense					
Total				(604)	

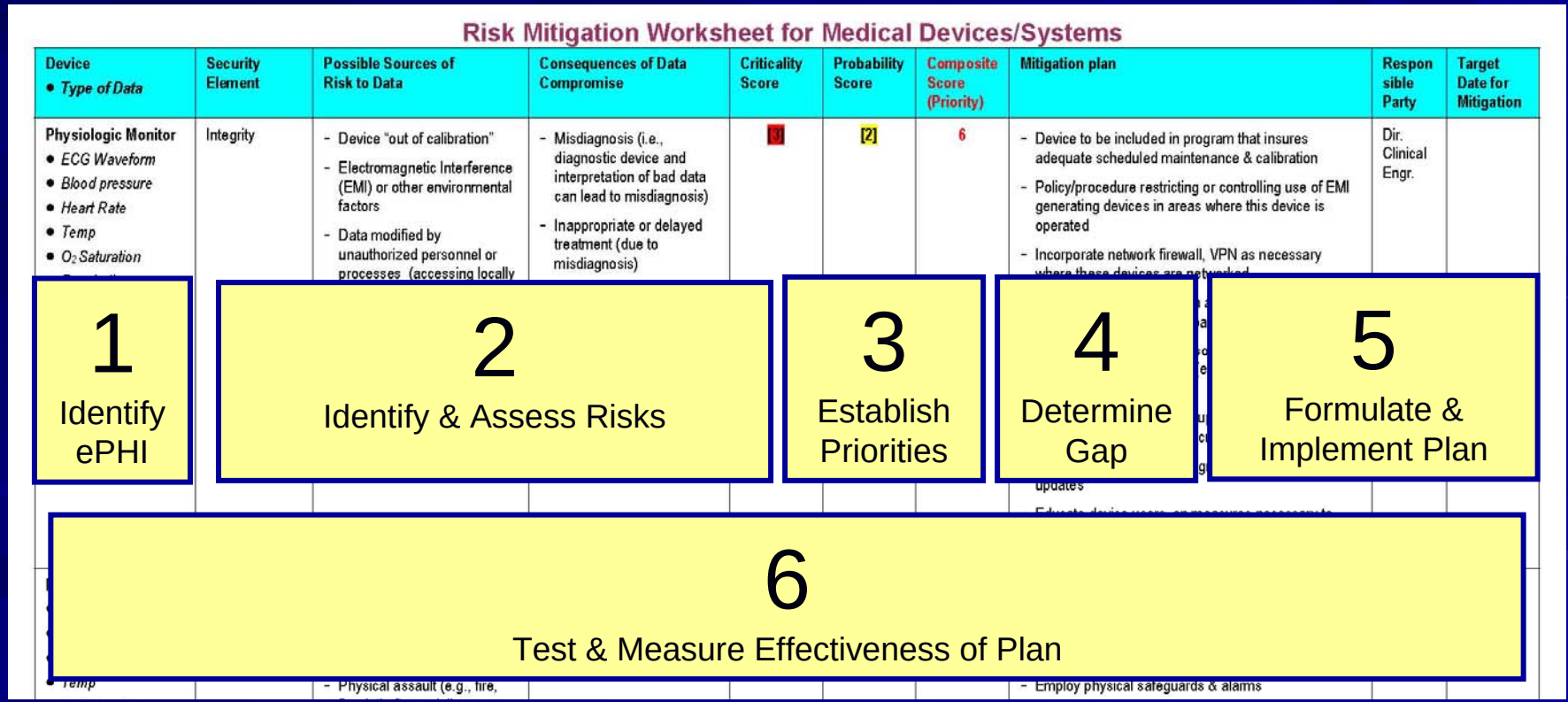
HIPAA Security Compliance Guide, V. 1.0 ©2004, ACCE/ECRI All Rights Reserved
40

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)	[3]	[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	Dir. Clinical Engr.	
Temp		- Physical assault (e.g., fire,					- Employ physical safeguards & alarms		

1 Identify ePHI

2 Identify & Assess Risks

3 Establish Priorities

4 Determine Gap

5 Formulate & Implement Plan

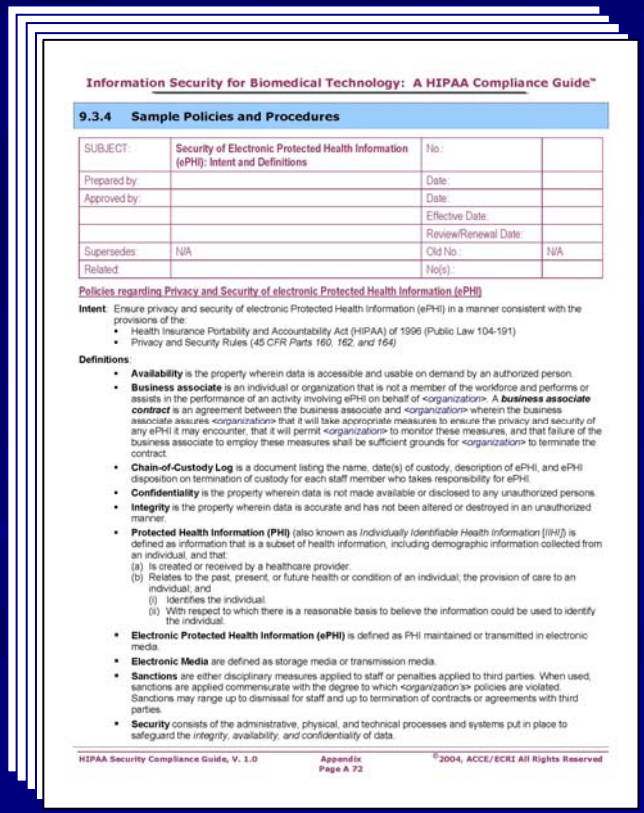
6 Test & Measure Effectiveness of Plan

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)

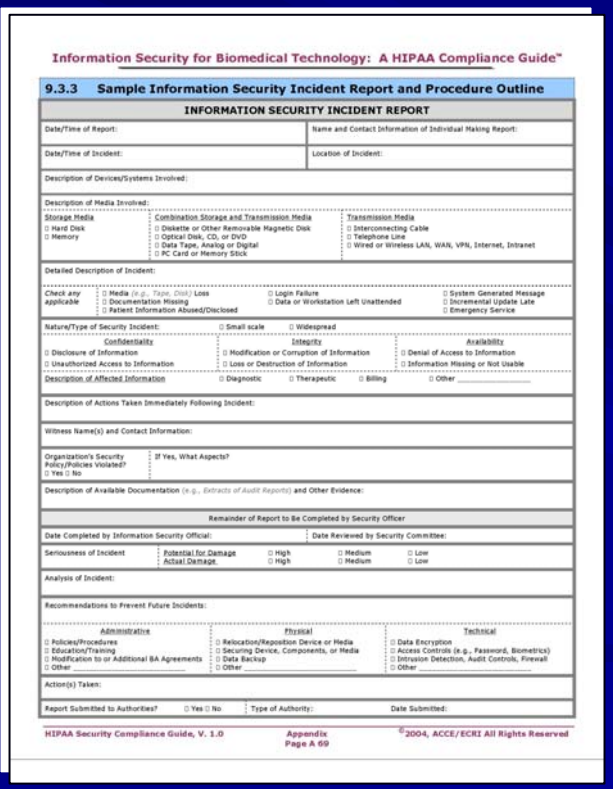
Intent: Ensure privacy and security of electronic Protected Health Information (ePHI) in a manner consistent with the provisions of the:

- 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
    - (i) Identifies the individual.
    - (ii) With respect to which there is a reasonable basis to believe the information could be used to identify 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.

HIPAA Security Compliance Guide, V. 1.0 Appendix Page A 72 ©2004, ACCE/ECRI All Rights Reserved



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 Devices/Systems Involved:

Description of Media Involved:

Storage Media	Combination Storage and Transmission Media	Transmission Media
☐ Hard Disk ☐ Memory	☐ Diskette or Other Removable Magnetic Disk ☐ Optical Disk, CD, or DVD ☐ Data Tape, Analog or Digital ☐ PC Card or Memory Stick	☐ Interconnecting Cable ☐ Telephone Line ☐ Wired or Wireless LAN, WAN, VPN, Internet, Intranet

Detailed Description of Incident:

Check any applicable			
	☐ Media (*e.g., Tape, Disk*) Loss	☐ Login Failure	☐ System Generated Message
	☐ Documentation Missing	☐ Data or Workstation Left Unattended	☐ Incremental Update Late
	☐ Patient Information Abused/Disclosed		☐ Emergency Service

Nature/Type of Security Incident: ☐ Small scale ☐ Widespread

Confidentiality	Integrity	Availability
☐ Disclosure of Information ☐ Unauthorized Access to Information	☐ Modification or Corruption of Information ☐ Loss or Destruction of Information	☐ Denial of Access to Information ☐ Information Missing or Not Usable

Description of Affected Information ☐ Diagnostic ☐ Therapeutic ☐ Billing ☐ Other _____

Description of Actions Taken Immediately Following Incident:

Witness Name(s) and Contact Information:

Organization's Security Policy/Polices Violated? ☐ Yes ☐ 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 Official: | Date Reviewed by Security Committee:

Seriousness of Incident	Potential for Damage		Actual Damage	
	☐ High	☐ Medium	☐ High	☐ Medium
	☐ Low		☐ Low	

Analysis of Incident:

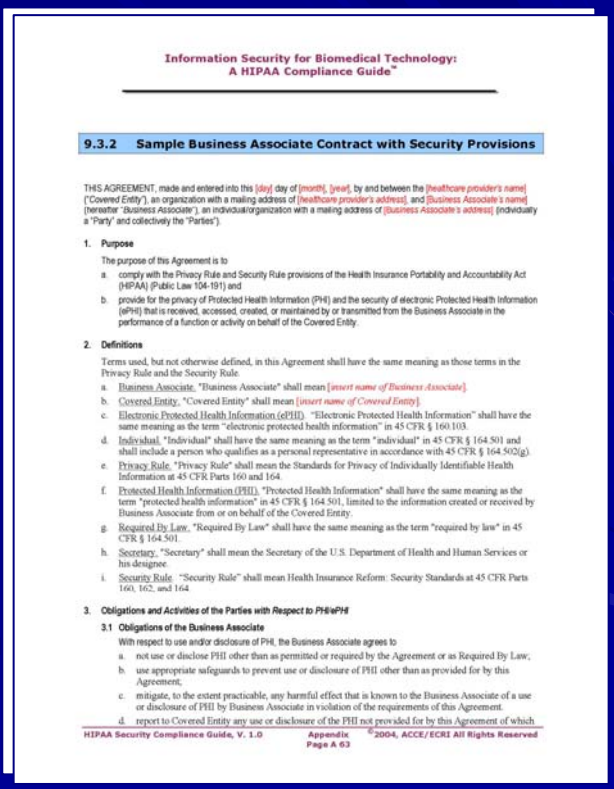
Recommendations to Prevent Future Incidents:

Administrative	Physical	Technical
☐ Policies/Procedures ☐ Education/Training ☐ Modification to or Additional BA Agreements ☐ Other _____	☐ Relocation/Reposition Device or Media ☐ Securing Device, Components, or Media ☐ Data Backup ☐ Other _____	☐ Data Encryption ☐ Access Controls (e.g., Password, Biometrics) ☐ Intrusion Detection, Audit Controls, Firewall ☐ Other _____

Action(s) Taken:

Report Submitted to Authorities? ☐ Yes ☐ No | Type of Authority: | Date Submitted:

HIPAA Security Compliance Guide, V. 1.0 Appendix Page A 69 ©2004, ACCE/ECRI All Rights Reserved



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*] (hereafter "*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

a. comply with the Privacy Rule and Security Rule provisions of the Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191) and

b. 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.

a. Business Associate. "Business Associate" shall mean [*insert name of Business Associate*].

b. Covered Entity. "Covered Entity" shall mean [*insert name of Covered Entity*].

c. 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.

d. 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).

e. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164.

f. 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.

g. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

h. Secretary. "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his designee.

i. 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

a. not use or disclose PHI other than as permitted or required by the Agreement or as Required By Law;

b. use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement;

c. 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.

d. report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which

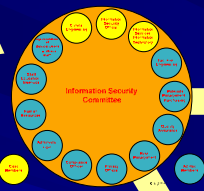
HIPAA Security Compliance Guide, V. 1.0 Appendix Page A 63 ©2004, ACCE/ECRI All Rights Reserved

ACCE / ECRI Security Process

Manufacturer-supplied MDS^2 Forms

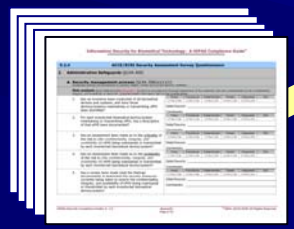
Biomedical Equipment Survey Forms (*sources of ePHI*)

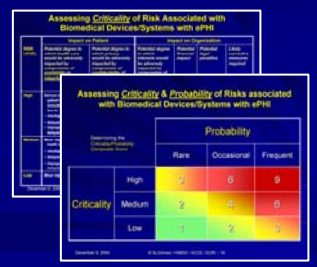
Information Security Officer & Committee (*risk assessment*)



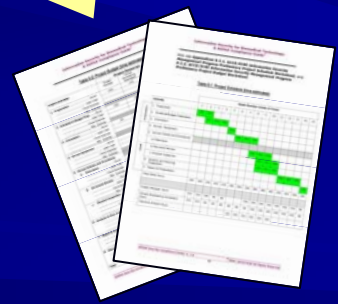
Risk Mitigation Worksheets (*plan & priorities*)

Security Assessment Survey Questionnaire (*process analysis*)





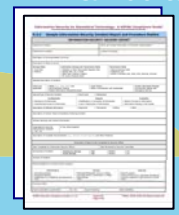
Criteria & Guidelines



Security Management Schedule & Budget

Administrative Safeguards

Incident Reports & Audits

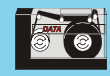


Policies & Procedures; Contingency Plans

Business Associate Agreements

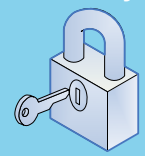
Training

Physical Safeguards



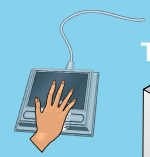
Data Backup

Lock & Key

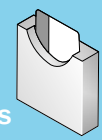


Intrusion & Environmental Alarms

Technical Safeguards



Biometrics



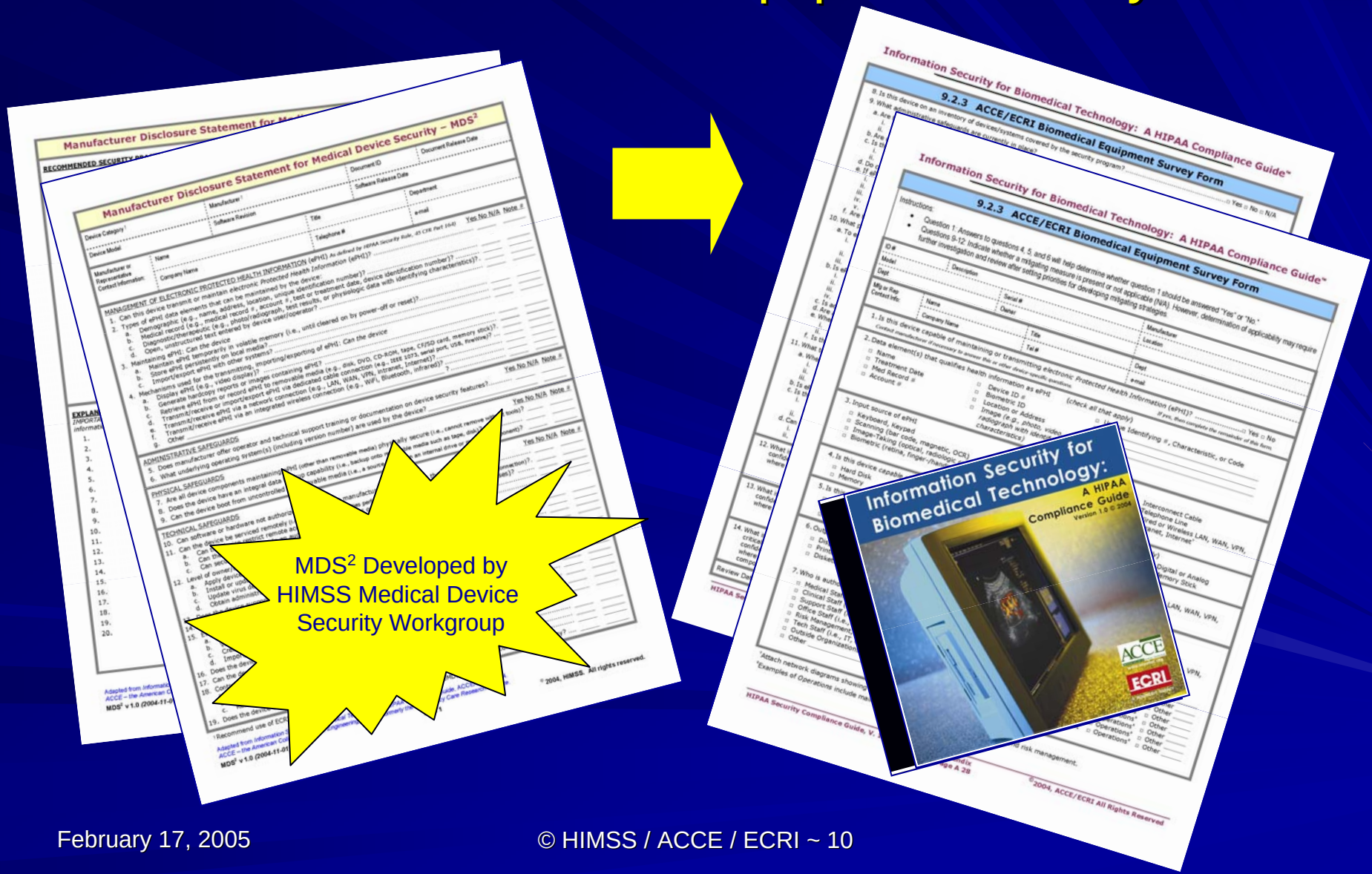
Tokens

Encryption

Firewalls

Error Correction

MDS^2 supplies key data to the ACCE / ECRI Biomedical Equipment Survey Form



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

HIMSS

SEARCH

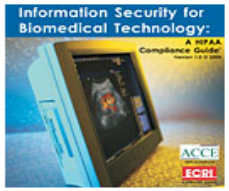
HIMSS Web Powered by Google

Home | About HIMSS | Contact Us | Member Login

News & Research | Topics & Tools | Professional Development | Conferences & Events | Membership | HIMSS Store

HIMSS Store

- 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
  - Professional Certification



Information Security for Biomedical Technology: A HIPAA Compliance Guide CD-ROM Just Released!

by ECRI

Price:
$495 for members
$695 for non-members

BUY IT NOW >>

Discount for Members

Information Security for Biomedical Technology: A HIPAA Compliance Guide CD-ROM is an ideal resource to help healthcare organizations prepare to meet HIPAA's April 21, 2005 Security Rule deadline. The CD-ROM contains an extensive overview of the HIPAA Security Rule, reviews necessary compliance measures for medical technology, and provides recommendations on implementing the rules, with specific medical-technology-related examples. It also provides guidance on assigning appropriate staff, getting set up, assessing current security conditions, and developing a plan for mitigating risks. Implementation and monitoring of the compliance program will vary among organizations.

The Guide also provides valuable tools and resources to use with a security program, including cu stomizable worksheets, typical policies and procedures, recommended best practices, checklists for risk inventory and analysis, self-assessment tools to analyze ongoing levels of compliance, tools for setting priorities and implementing a mitigation plan, sample information security incident report, sample business associate agreement, and typical policies and procedures.

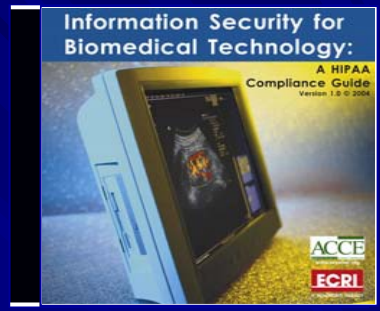
Finally, the Guide provides a working framework through which information from the HIMSS-produced Manufacturers Disclosure Statement for Medical Device Security (MDS 2) can be analyzed and acted upon. The industry-endorsed and manufacturer-supplied MDS 2 was designed to complement the security management processes outlined in the Guide.

Produced by ECRI, a nonprofit health services research agency, and the American College of Clinical Engineering

HIMSS, 230 East Ohio Street, Suite 500, Chicago, IL 60611-3269
Phone: 312/664-4467 Fax: 312/664-6143

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/HIPAATOCwithCover.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

