Technology in Medicine

Conference on Medical Device Security

Overview of Medical Devices and HIPAA Security Compliance

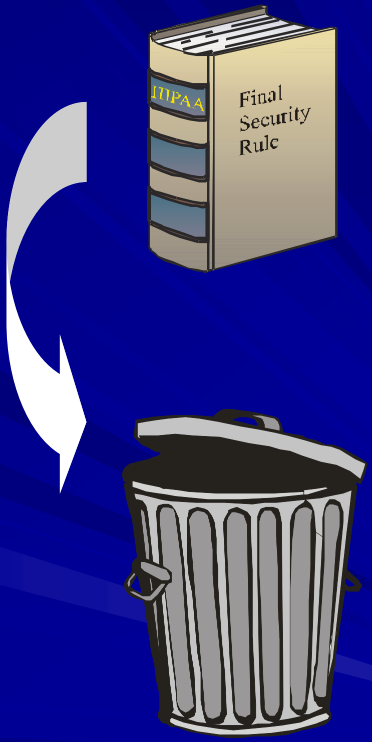
Wednesday, March 9, 2005

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

Medical Device Security: Is this just a HIPAA issue?

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

- Medical device security … particularly data *integrity* & data *availability* … is critical to healthcare quality, timeliness, and cost-effectiveness
- Today, a reasonable *standard of care* cannot be maintained without an effective an Information Security Management Program in place that includes *biomedical technology*

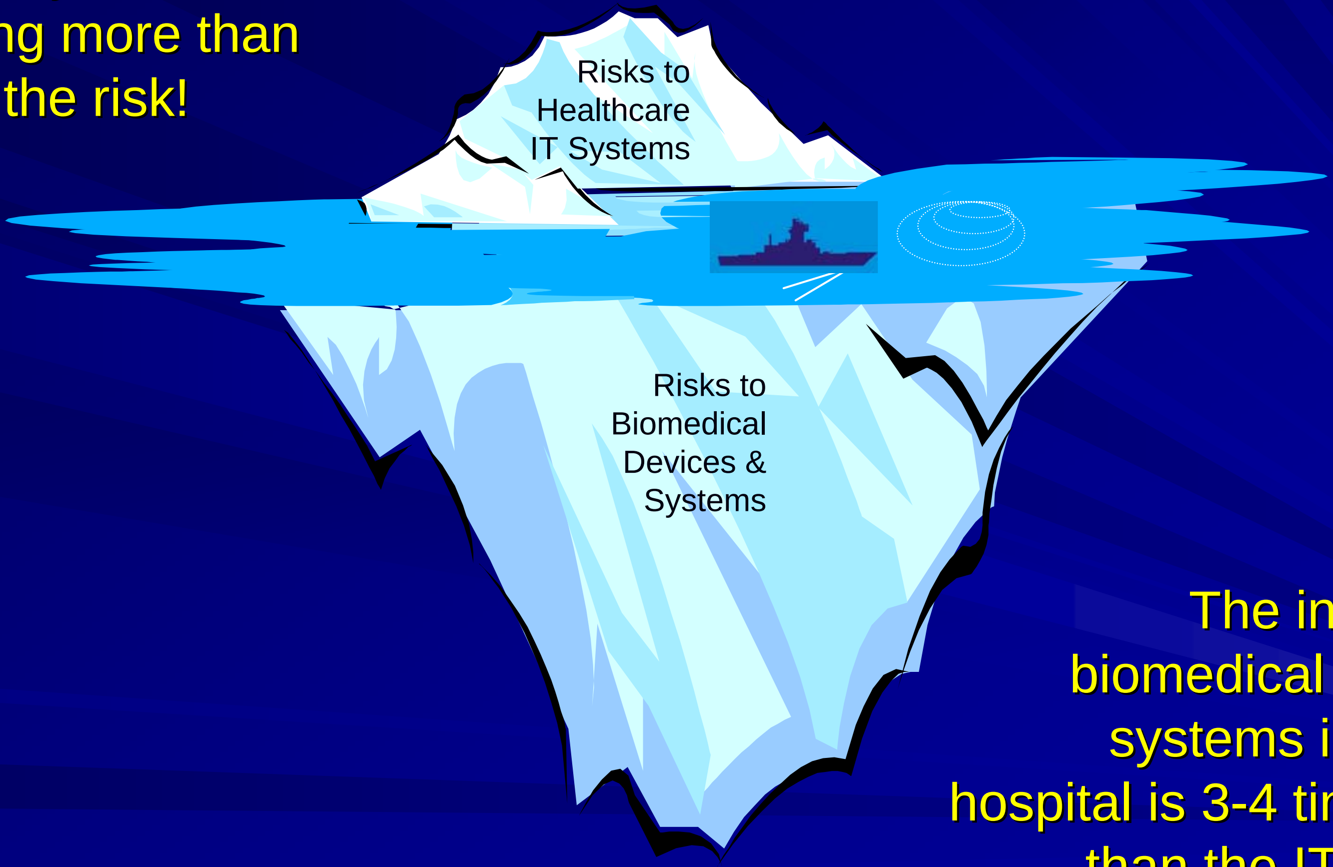


HIPAA’s Security Rule

Implications for Biomedical Devices & Systems

Security Risks to Healthcare Technology

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



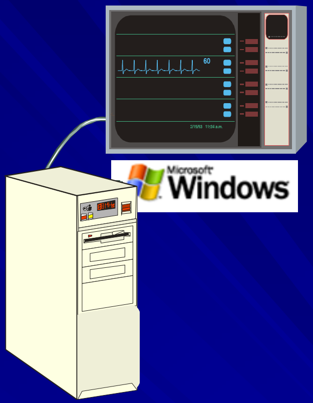
Risks to Healthcare IT Systems

Risks to Biomedical Devices & Systems

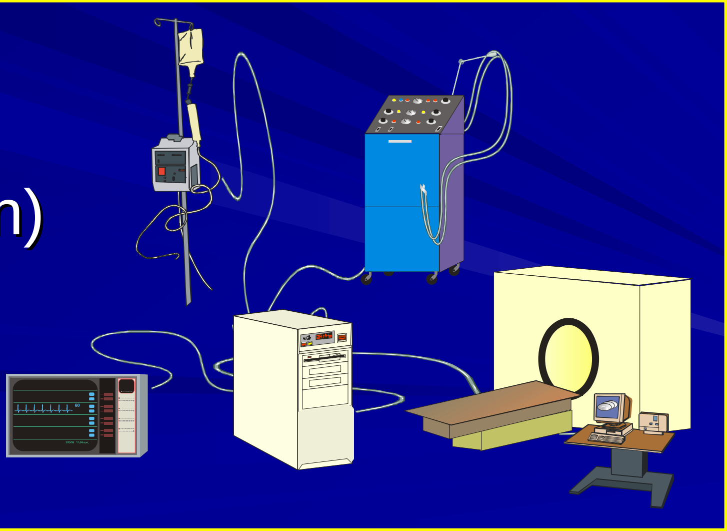
The inventory of biomedical devices & systems in a typical hospital is 3-4 times larger than the IT inventory

Significant Medical Device Industry Trends

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



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



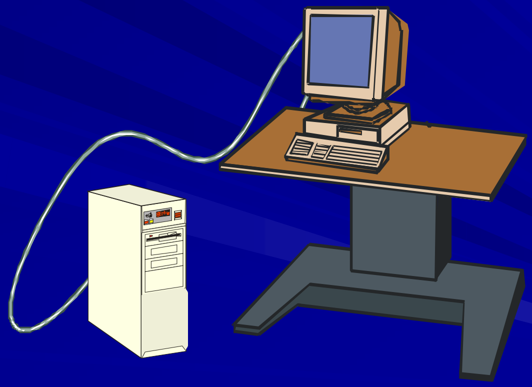
Information Technology Systems

- **Mission Critical**

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

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

MISSION CRITICAL

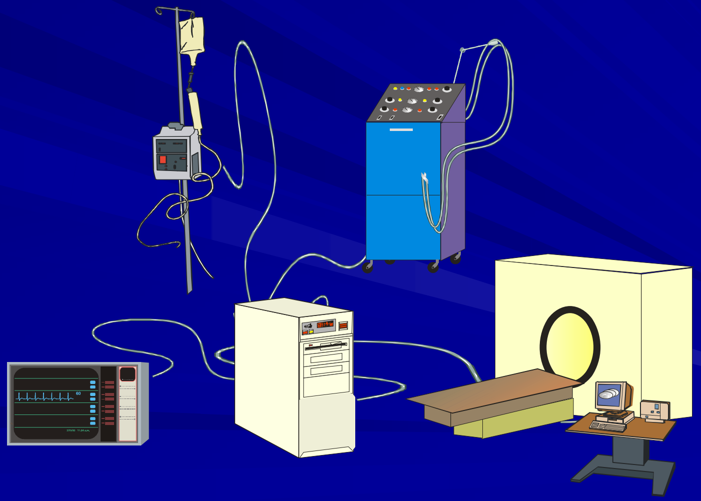


Biomedical Technology Systems

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

  Examples of ***Life Critical*** systems include physiologic monitoring, imaging, radiation therapy, and clinical laboratory systems.

LIFE
CRITICAL

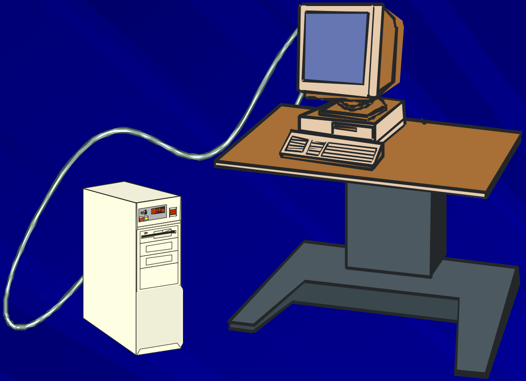


HIPAA Security requires Risk Analysis:

Risks Associated with IT vs Biomedical Systems

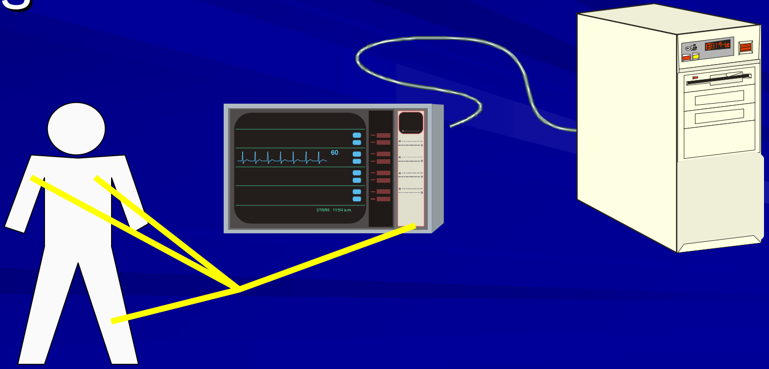
- IT Systems

MISSION CRITICAL



- Medical Devices & Systems

LIFE CRITICAL



HIPAA's Security Rule
Implications for Biomedical Technology

Why is security an issue for biomedical technology?

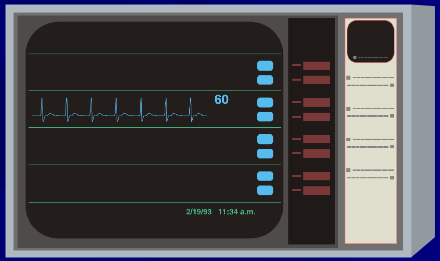
Because compromise in *ePHI* can affect

- *Integrity* or *Availability* … can result in improper diagnosis or therapy of patient resulting in harm (even death) because of delayed or inappropriate treatment
- *Confidentiality* … can result in loss of patient privacy … and, as a consequence, may result in financial loss to patient and/or provider organization

HIPAA’s Security Rule

Implications for Biomedical Technology

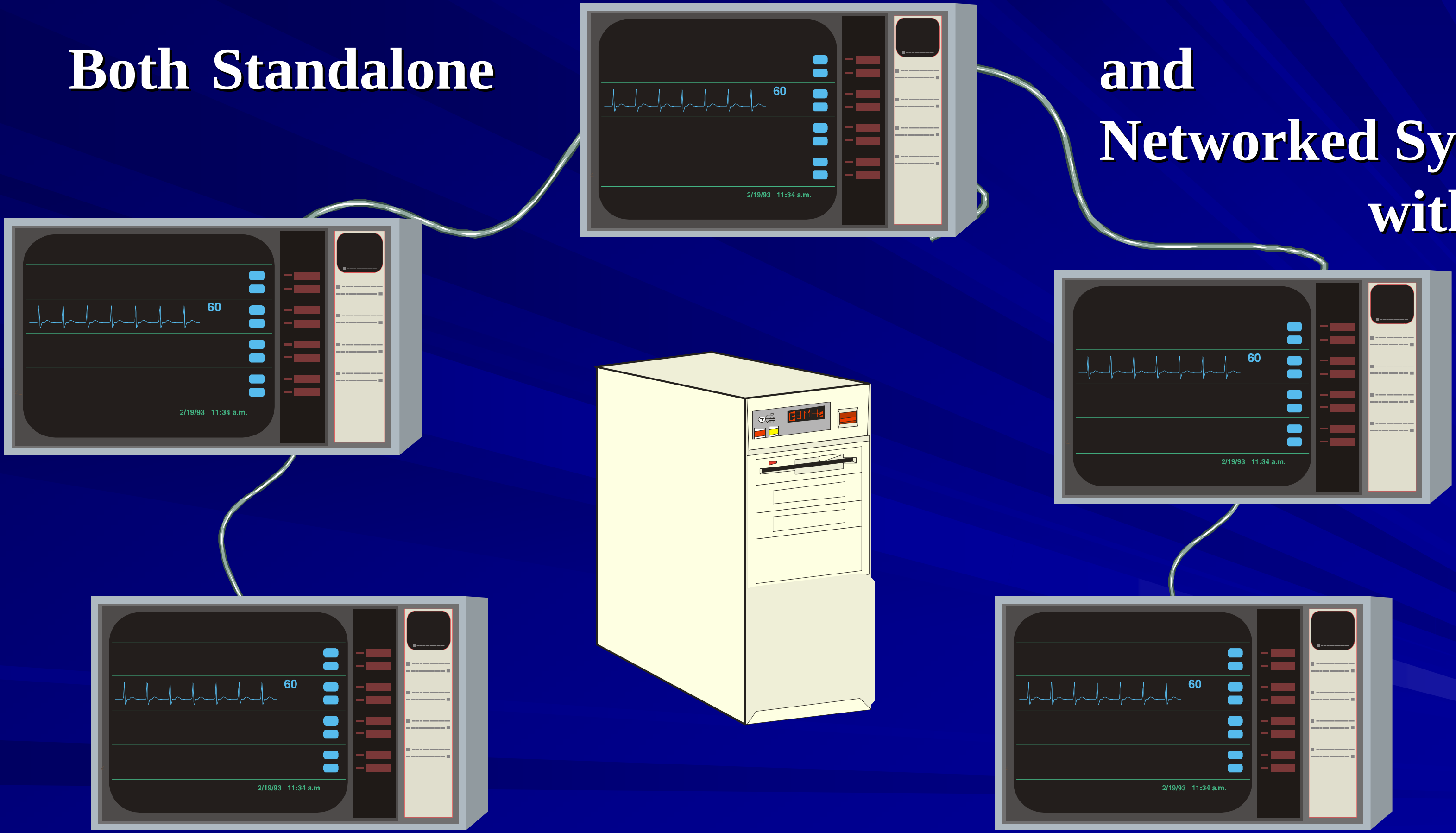
Standalone with ePHI



HIPAA's Security Rule

Implications for Biomedical Technology

Both Standalone **and Networked Systems with ePHI**

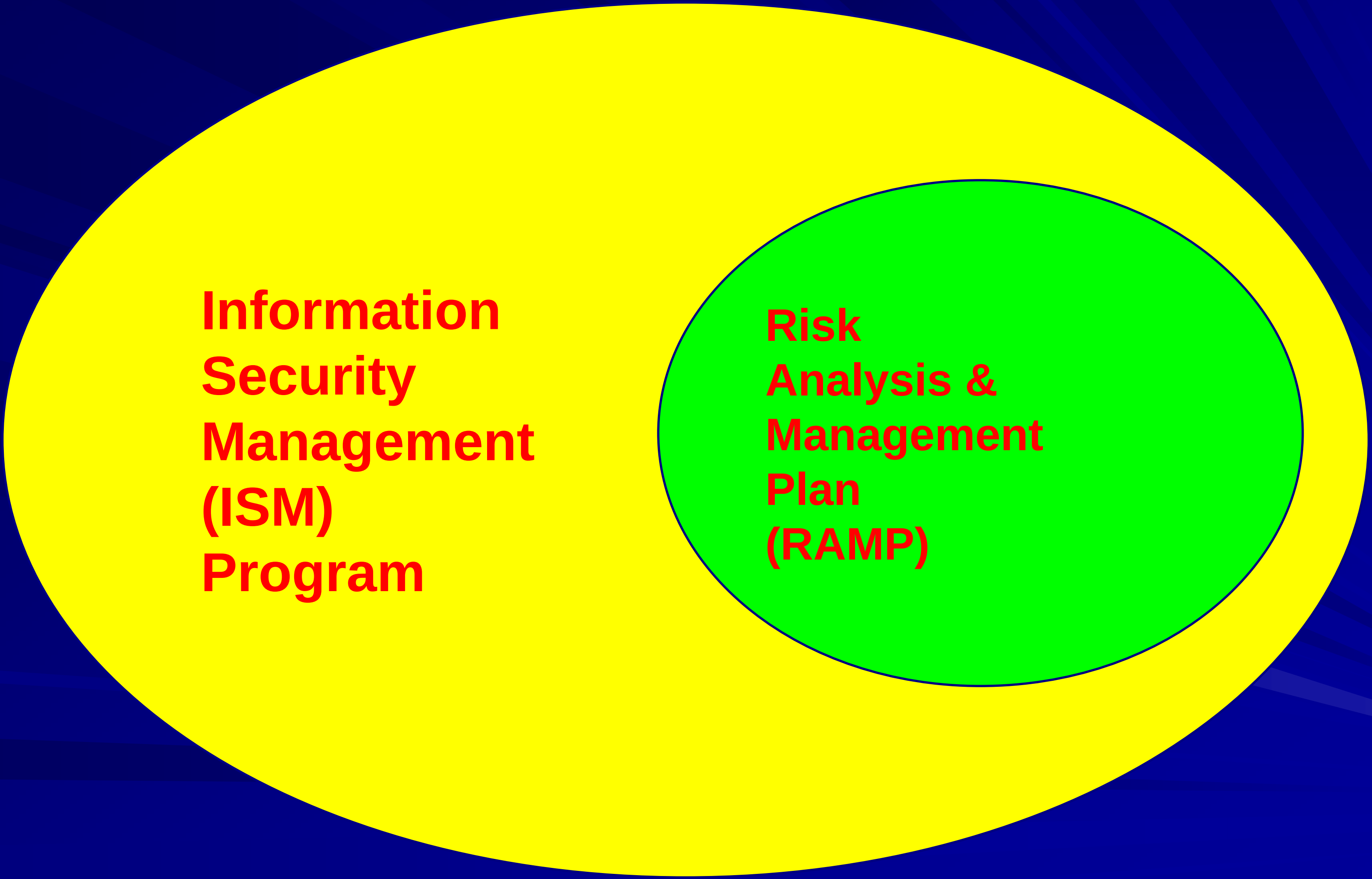


HIPAA’s Security Rule

Overview of
Compliance Process

HIPAA's Security Rule

Compliance Overview



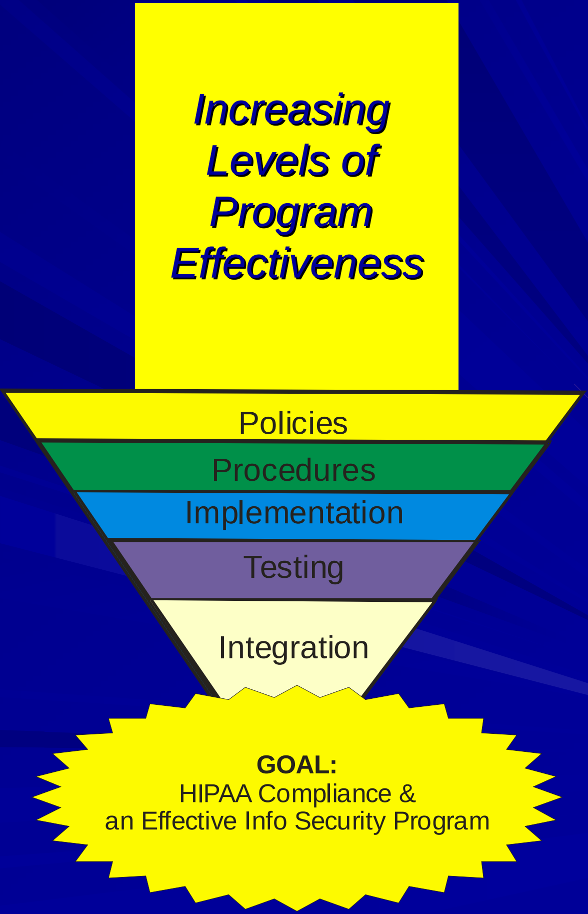
Information Security Management (ISM) Program

Risk Analysis & Management Plan (RAMP)

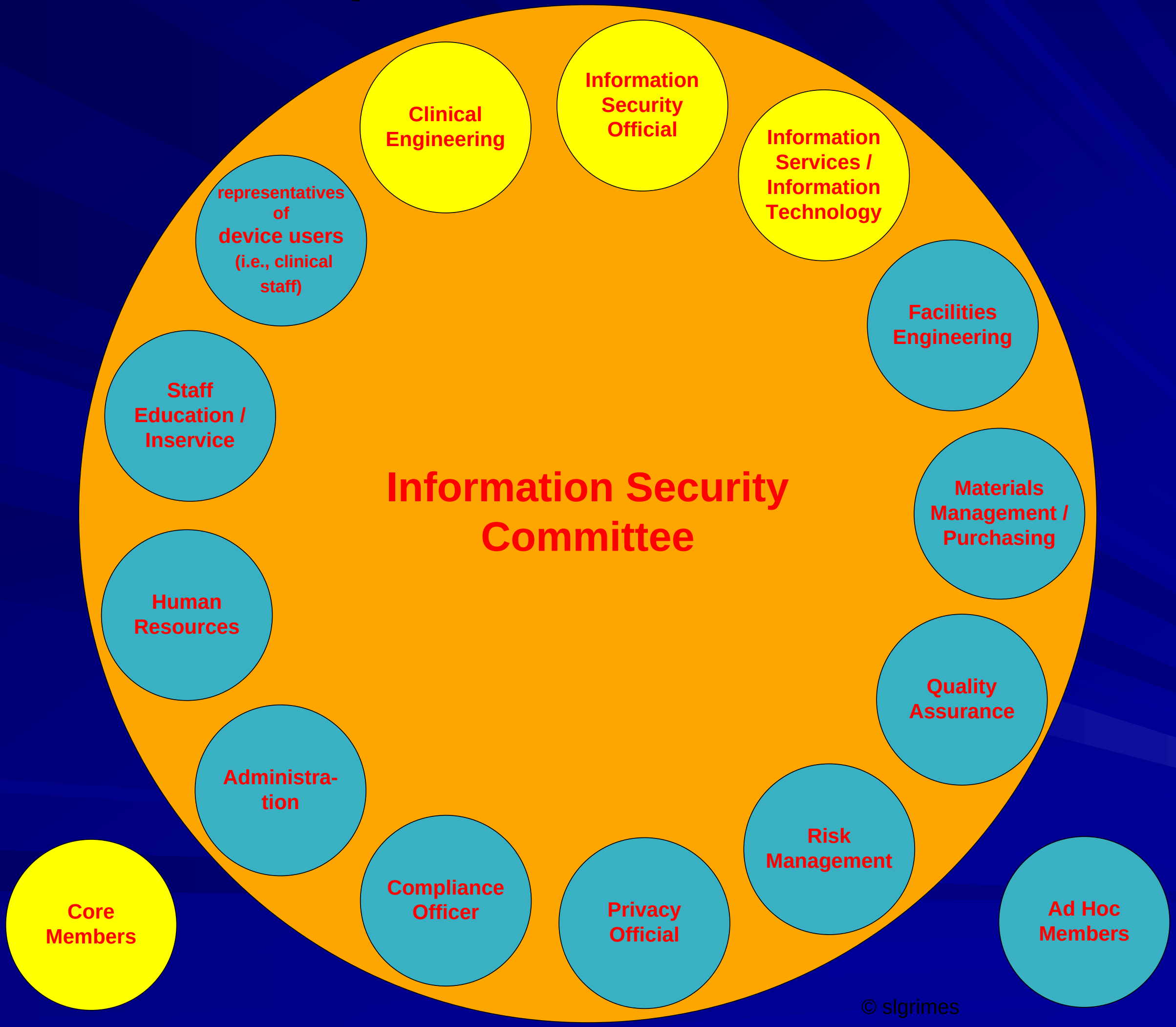
HIPAA's Security Rule
Compliance Overview

Establish effective Info Security Management (ISM) program:

1) Assign security official & establish information security committee
2) Develop necessary policies as per security *standards*
3) Develop necessary procedures, physical/technical safeguards as per *implementation specifications*
4) Implement Policies/procedures, Business associate agreements, Educate workforce & Install/Configure security "tools"
5) Test implementation
6) Integrate security measures into organization-wide program


Increasing Levels of Program Effectiveness
Policies
Procedures
Implementation
Testing
Integration
GOAL:
HIPAA Compliance &
an Effective Info Security Program

HIPAA's Security Rule
Compliance Overview



Information Security Committee

Clinical Engineering

Information Security Official

Information Services / Information Technology

Facilities Engineering

Materials Management / Purchasing

Quality Assurance

Risk Management

Privacy Official

Compliance Officer

Administra-tion

Human Resources

Staff Education / Inservice

representatives of device users (i.e., clinical staff)

Core Members

Ad Hoc Members

© slgrimes

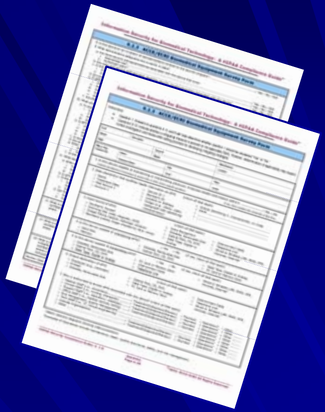
HIPAA's Security Rule
Compliance Overview

Establish Risk Analysis/Management Plan (RAMP):

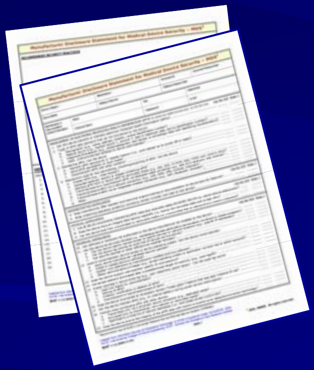
1) Conduct inventory (identify sources of ePHI) and survey current security practices & resources
2) Identify and Assess Security Risks
3) Establish Priorities
4) Determine Security Gap (i.e., need for additional safeguards) following "*best practices*" and Security Rule's *Standards* and *Implementation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

Compliance Overview

Risk Analysis/Management



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



New!

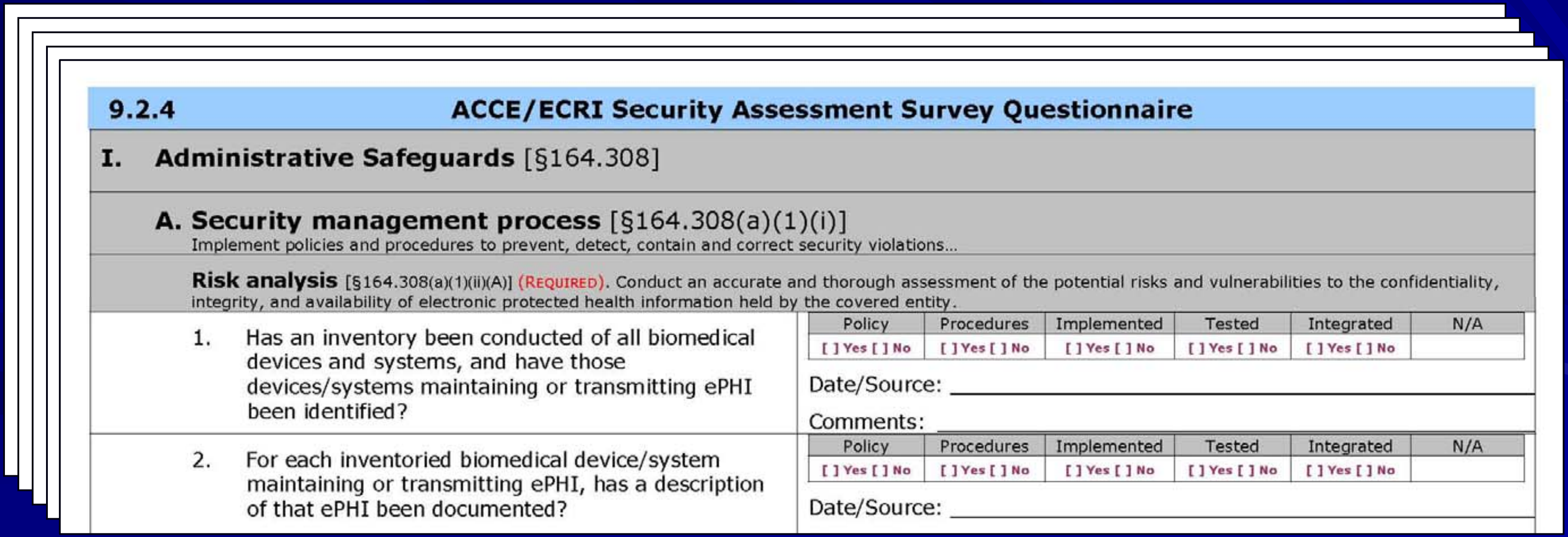
HIMSS Manufacturers Disclosure Statement for Medical Device Security (MDS^2)
http://www.himss.org/asp/medicalDeviceSecurity.asp

Nov 8, 2004

Compliance Overview

Risk Analysis/Management

1) and Survey current security practices & resources … *to analyze existing processes*
   - Policies & procedures
   - Training programs
   - Tools & security measures



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	

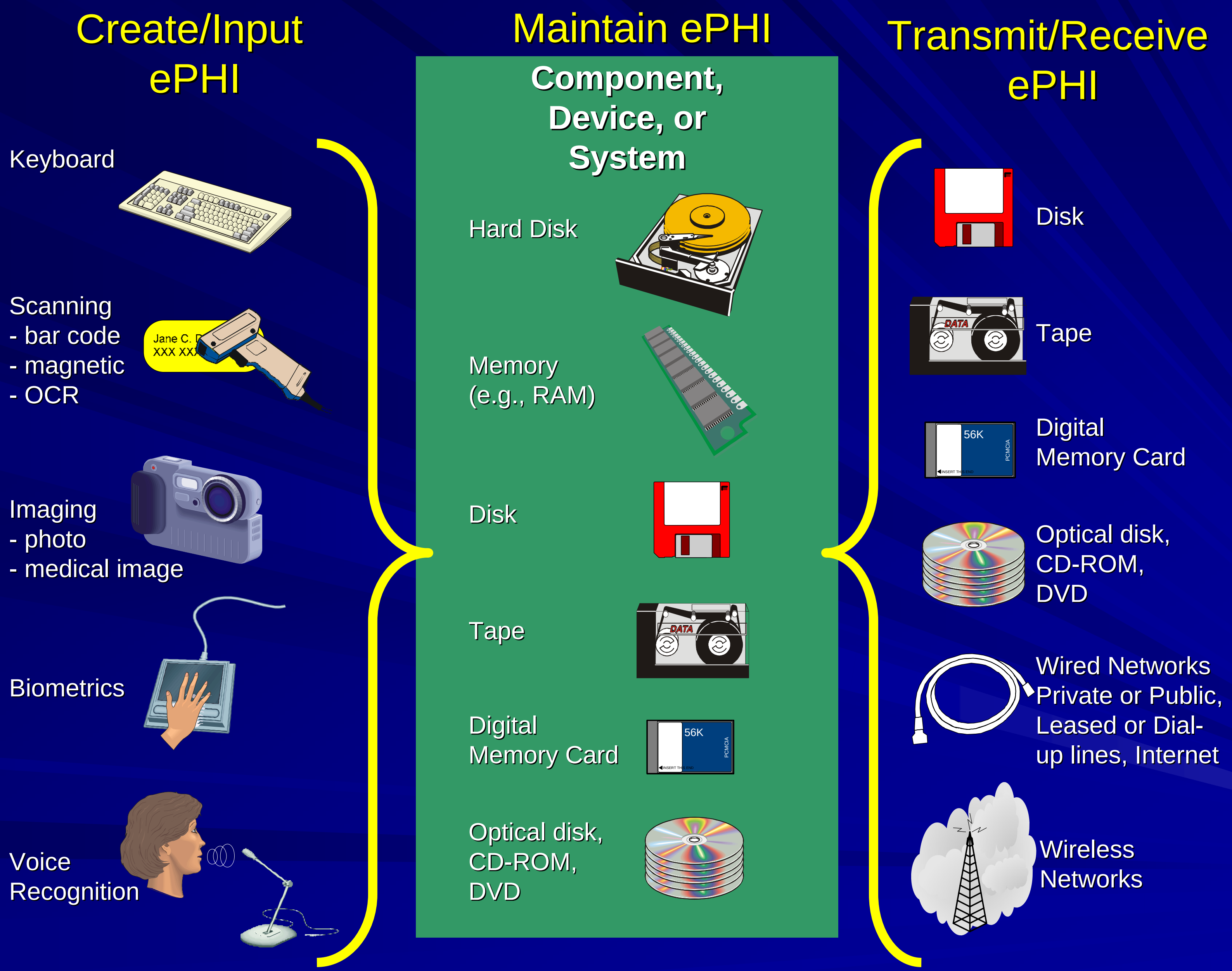
Date/Source: ______________________

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: ______________________



Create/Input ePHI

Keyboard

Scanning
- bar code
- magnetic
- OCR

Imaging
- photo
- medical image

Biometrics

Voice Recognition

Maintain ePHI

Component, Device, or System

Hard Disk

Memory (e.g., RAM)

Disk

Tape

Digital Memory Card

Optical disk, CD-ROM, DVD

Transmit/Receive ePHI

Disk

Tape

Digital Memory Card

Optical disk, CD-ROM, DVD

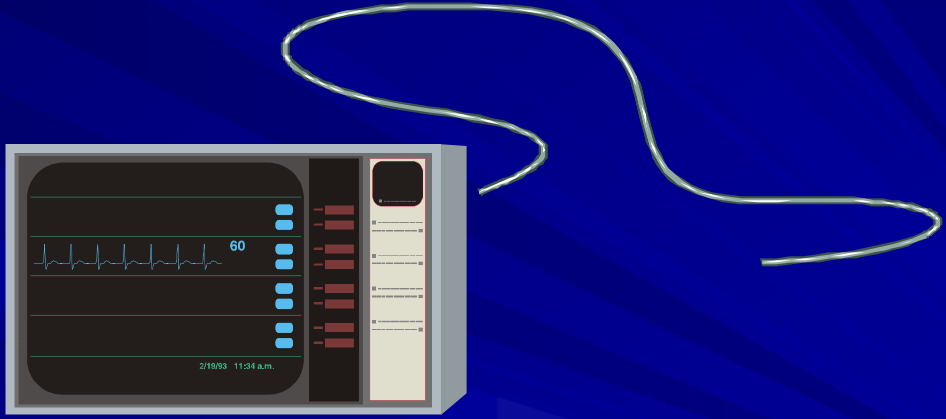
Wired Networks Private or Public, Leased or Dial-up lines, Internet

Wireless Networks

Compliance Overview

Inventory of Devices/Systems

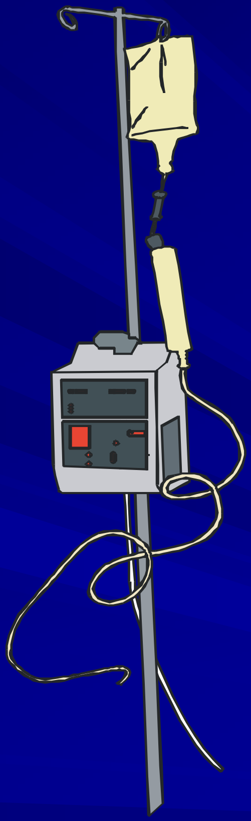
- Physiologic Monitor
  where ePHI may consist of patient identifying information and the following data:
  - ECG waveform
  - Blood pressure
  - Heart rate
  - Temp
  - O_2 Saturation
  - Respiration
  - Alarms



Compliance Overview

Inventory of Devices/Systems

- Infusion pump
  where ePHI may consist of patient identifying information
  and the following data:
  - Flow Rate
  - Volume delivered
  - Alarms



March 9, 2005

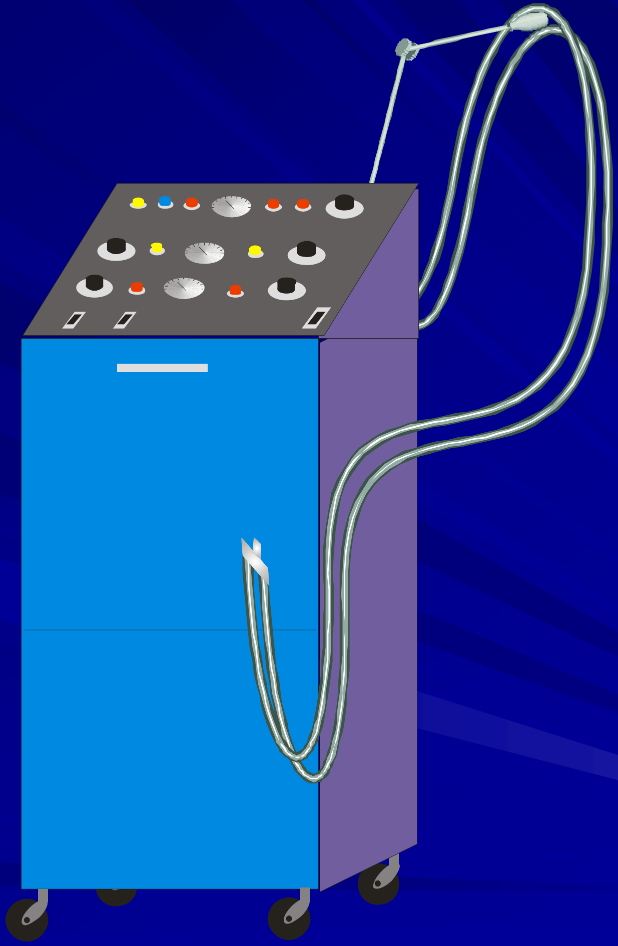
Compliance Overview

Inventory of Devices/Systems

- Ventilator

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

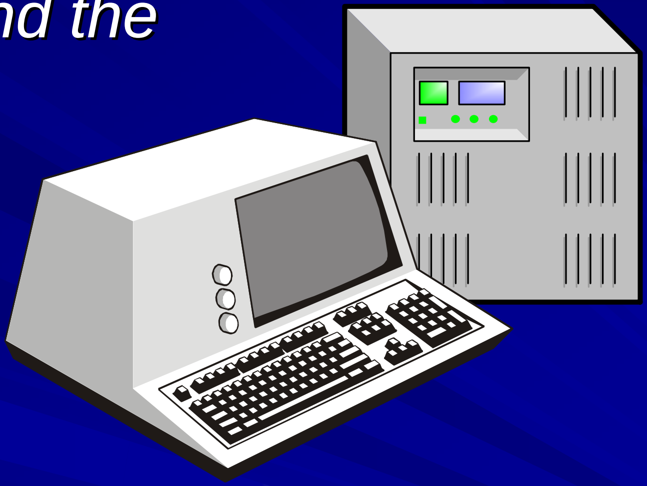
  - Flow Rate
  - Volume Delivered
  - Respiration (Breaths Per Minute)
  - O_2 Saturation
  - Alarms



Compliance Overview

Inventory of Devices/Systems

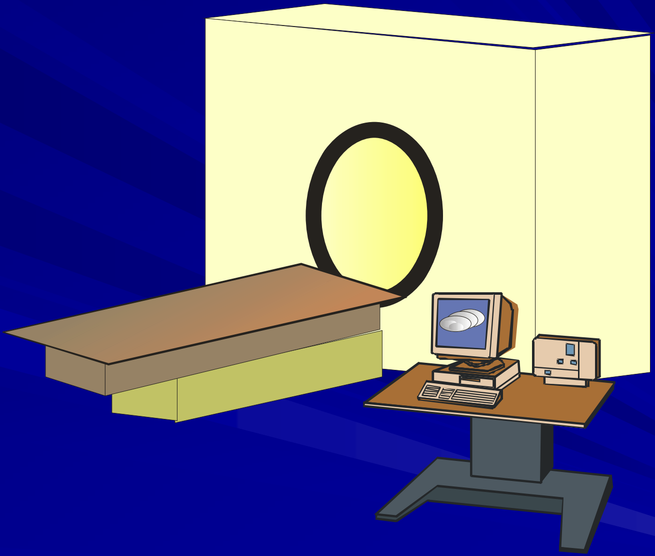
- Laboratory analyzer
  where ePHI may consist of patient identifying information and the following data :
  - Blood related
    - Hemoglobin
    - Glucose
    - Gas
    - pH
    - Electrolyte
  - Urine related
    - Albumin
    - Creatinine
    - Bilirubin

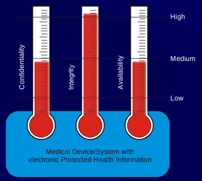


Compliance Overview

Inventory of Devices/Systems

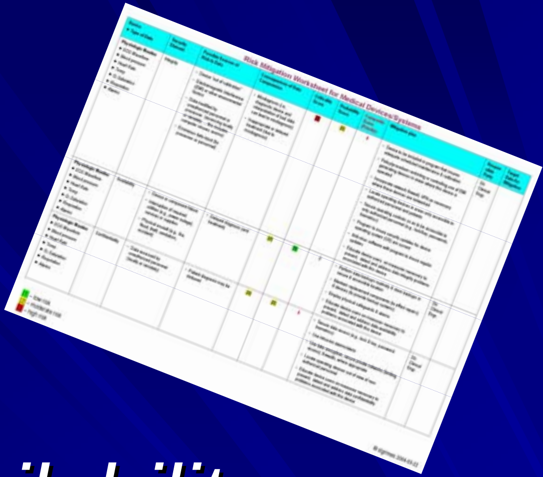
- MRI, CT Scanner, Diagnostic Ultrasound
  where ePHI may consist of patient identifying information and the following data :
  - Image




High
Medium
Low
Confidentiality
Integrity
Availability
Medical Device/System with
electronic Protected Health Information

Compliance Overview

Risk Analysis/Management

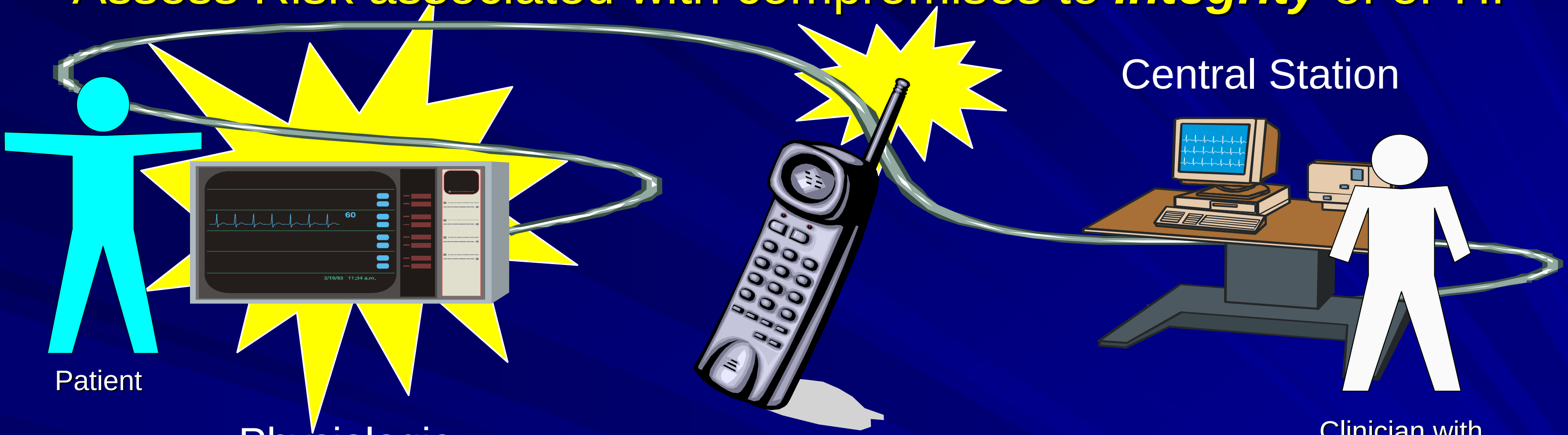

Risk Mitigation Worksheet for Medical Devices/Systems

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

- *Criticality*
  Categorize level of risk/vulnerability (e.g., high, medium, low) to CIA
- *Probability*
  Categorize the likelihood of risk (e.g., frequent, occasional, rare) to CIA
- *Composite Score* for *Criticality/Probability*

Taking into account ***Criticality***:

Assess Risk associated with compromises to ***Integrity*** of ePHI



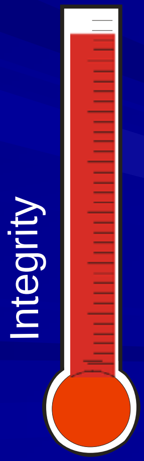
Patient

Physiologic Monitor

Central Station

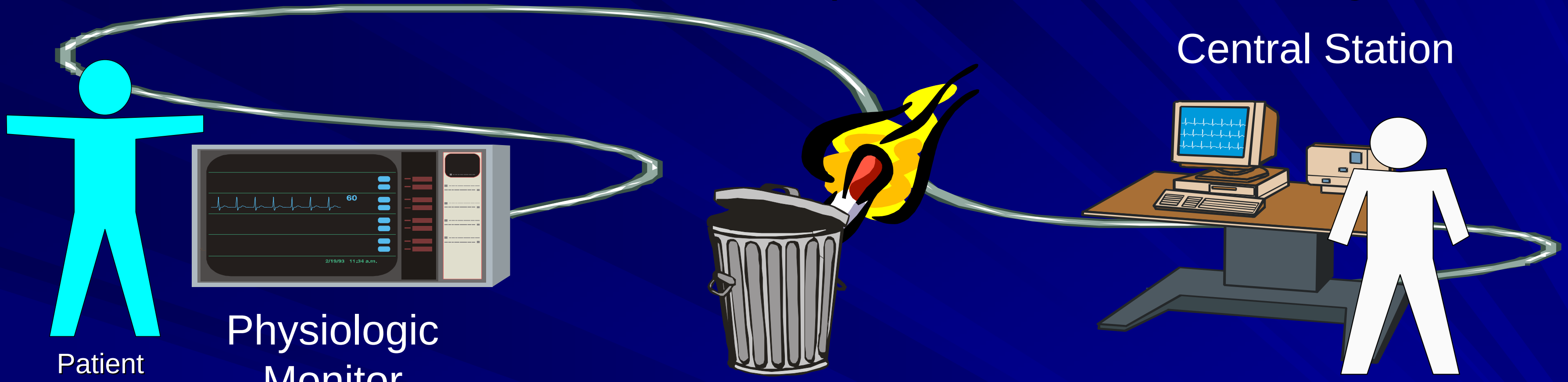
Clinician with Authorized Access

Data	**Actual**	**Maintained/ Transmitted**
Patient ID	7813244	7813254
Heart Rate	60 bpm	35 bpm
Blood Pressure	120/80 mmHg	90/50 mmHg
Temp	98.6º F	89.6º F
SpO2	92%	92%



Taking into account ***Criticality***:

Assess Risk associated with compromises to ***Availability*** of ePHI



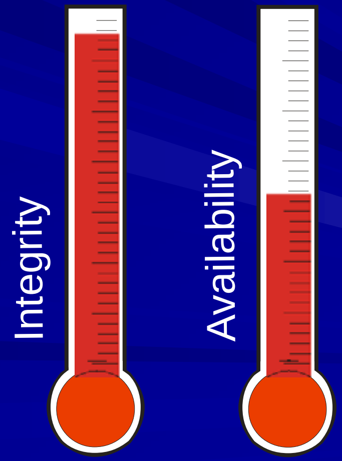
Central Station

Patient

Physiologic Monitor

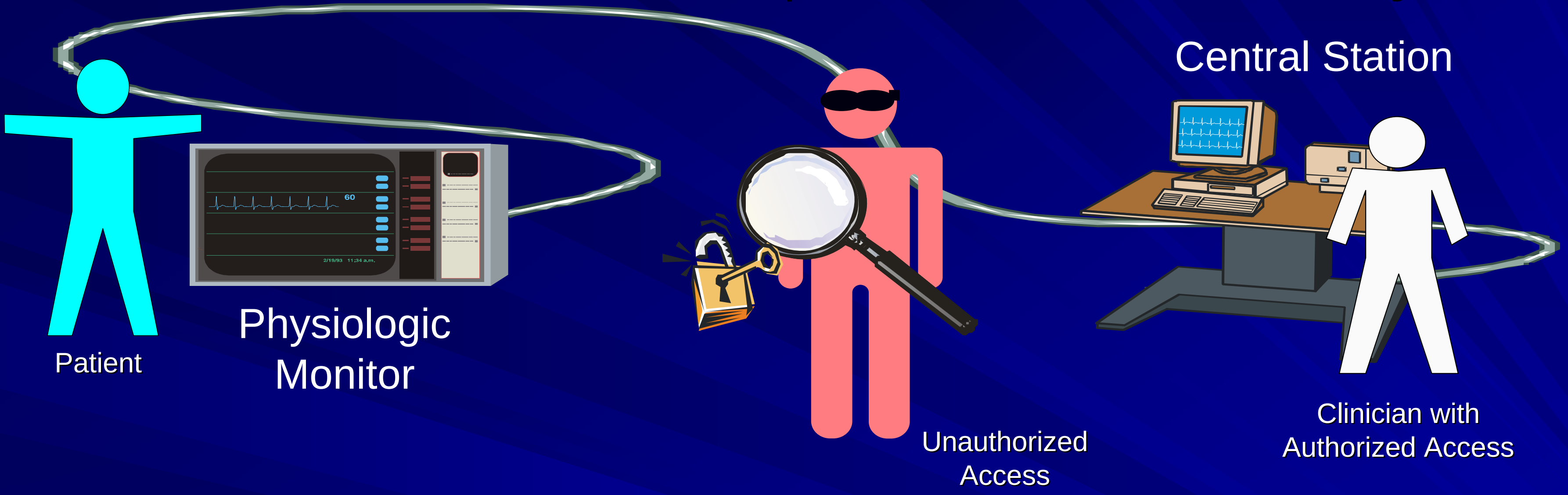
Clinician with Authorized Access

Data	**Actual**	**Maintained/ Transmitted**
Patient ID	7813244	XXXXX
Heart Rate	60 bpm	XX bpm
Blood Pressure	120/80 mmHg	XXX/XX mmHg
Temp	98.6º F	XX.Xº F
SpO2	92%	XX%



Taking into account ***Criticality***:

Assess Risk associated with compromises to ***Confidentiality*** of ePHI



Central Station

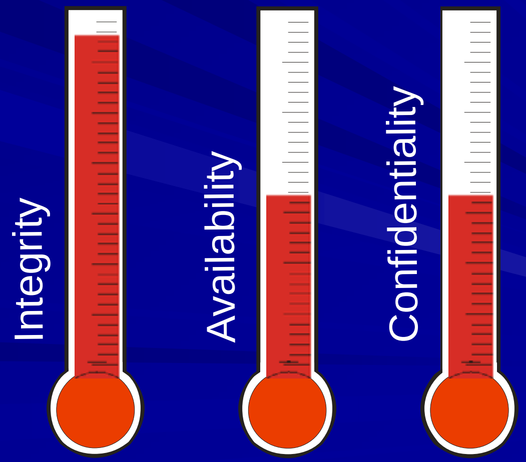
Patient

Physiologic Monitor

Unauthorized Access

Clinician with Authorized Access

Data	**Actual**	**Maintained/ Transmitted**
Patient ID	7813244	7813244
Heart Rate	60 bpm	60 bpm
Blood Pressure	120/80 mmHg	120/80 mmHg
Temp	98.6º F	98.6º F
SpO2	92%	92%



Assessing *Criticality* of Risk Associated with Biomedical Devices/Systems with ePHI

	Impact on Patient		**Impact on Organization**			
RISK LEVEL	***Potential degree to which health care would be adversely impacted by compromise of availability or integrity of ePHI***	***Potential degree to which privacy would be adversely impacted by compromise of confidentiality of ePHI***	***Potential degree to which interests would be adversely impacted by compromise of confidentiality, availability or integrity of ePHI***	***Potential financial impact***	***Potential legal penalties***	***Likely corrective measures required***
High	Serious impact to patient's health (including loss of life) due to: ▪ misdiagnosis, ▪ delayed diagnosis or ▪ improper, inadequate or delayed treatment	Could identify patient and their diagnosis	Extremely grave damage to organization's interests	Major $1,000K	Imprisonment and/or large fines	Legal
Medium	Minor impact to patient's health due to: ▪ misdiagnosis, ▪ delayed diagnosis or ▪ improper, inadequate or delayed treatment	Could identify patient and their health information (but from which a diagnosis could not be derived)	Serious damage	Moderate $100K	Moderate Fines	Legal
Low	Minor Impact	Could identify patient	Minor damage	Minor $10K	None	Administrative

Assessing ***Probability*** of Risks Associated with Biomedical Devices/Systems with ePHI

- ***Frequent***
  Likely to occur (e.g., once a month)
- ***Occasional***
  Probably will occur (e.g., once a year)
- ***Rare***
  Possible to occur (e.g., once every 5 -10 years)

Assessing ***Criticality*** & ***Probability*** of Risks associated with Biomedical Devices/Systems with ePHI

Determining the *Criticality/Probability Composite Score*		Probability		
		Rare	Occasional	Frequent
Criticality	High	3	6	9
	Medium	2	4	6
	Low	1	2	3

Compliance Overview

Risk Analysis/Management

3) Establish priorities

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

Compliance Overview

Risk Analysis/Management

4) Determine security gap

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

Compliance Overview
Risk Analysis/Management

5) Formulate & implement mitigation plan

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

Compliance Overview

Risk Analysis/Management

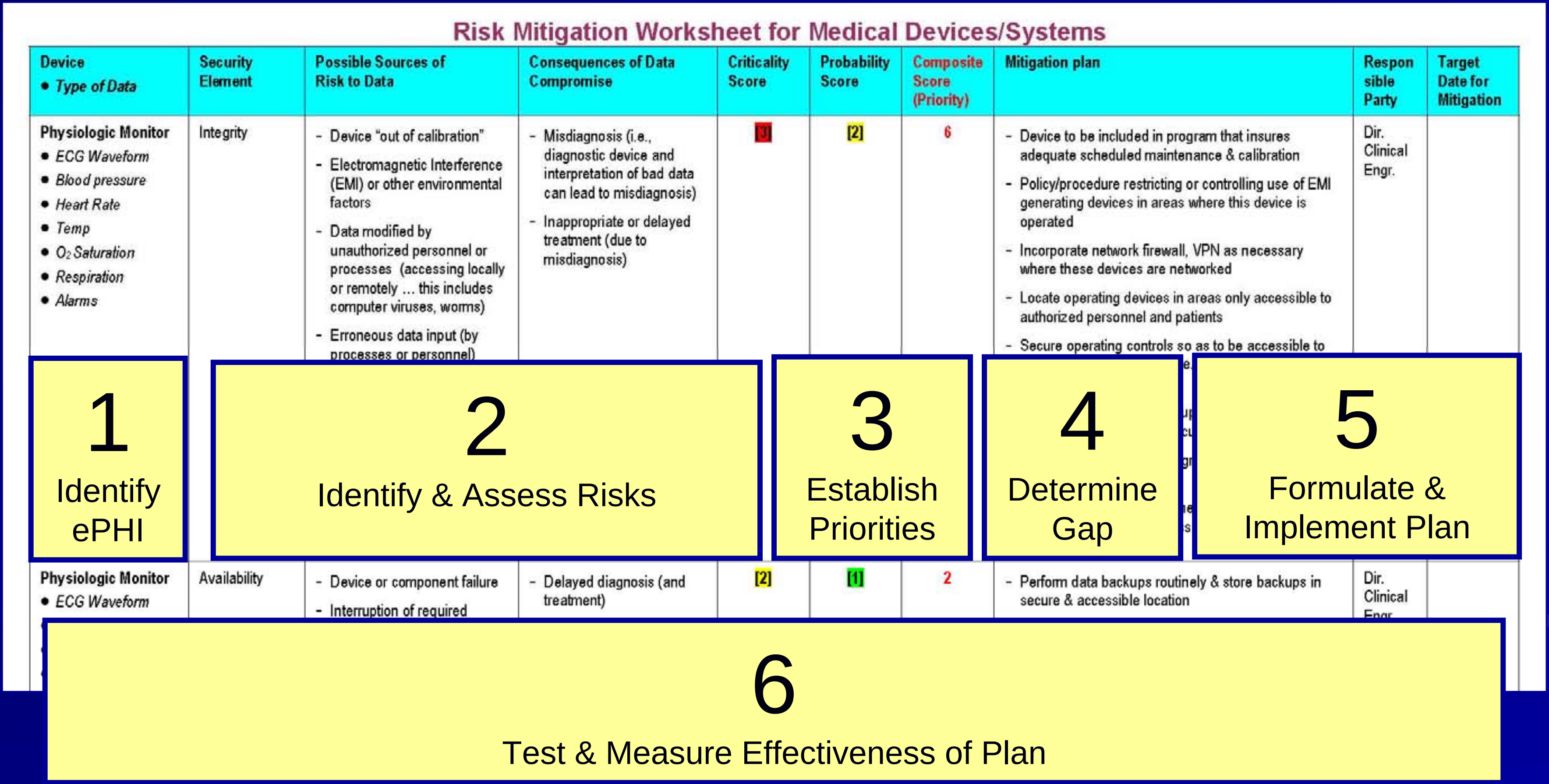
6) Monitor process

- Establish on-going monitoring system (including a security incident reporting system) to insure mitigation efforts are effective
- Document results of regular audits of security processes

Compliance Overview

Risk Analysis/Management

- Prepare a Risk Mitigation Worksheet



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	Respon sible Party	Target Date for Mitigation
Physiologic Monitor • *ECG Waveform* • *Blood pressure* • *Heart Rate* • *Temp* • *O_2 Saturation* • *Respiration* • *Alarms*	Integrity	- Device "out of calibration" - Electromagnetic Interference (EMI) or other environmental factors - Data modified by unauthorized personnel or processes (accessing locally or remotely … this includes computer viruses, worms) - Erroneous data input (by processes or personnel)	- 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 where these devices are networked - Locate operating devices in areas only accessible to authorized personnel and patients - Secure operating controls so as to be accessible to	Dir. Clinical Engr.	
Physiologic Monitor • *ECG Waveform*	Availability	- Device or component failure - Interruption of required	- Delayed diagnosis (and treatment)	[2]	[1]	2	- Perform data backups routinely & store backups in secure & accessible location	Dir. Clinical Engr	

1
Identify ePHI

2
Identify & Assess Risks

3
Establish Priorities

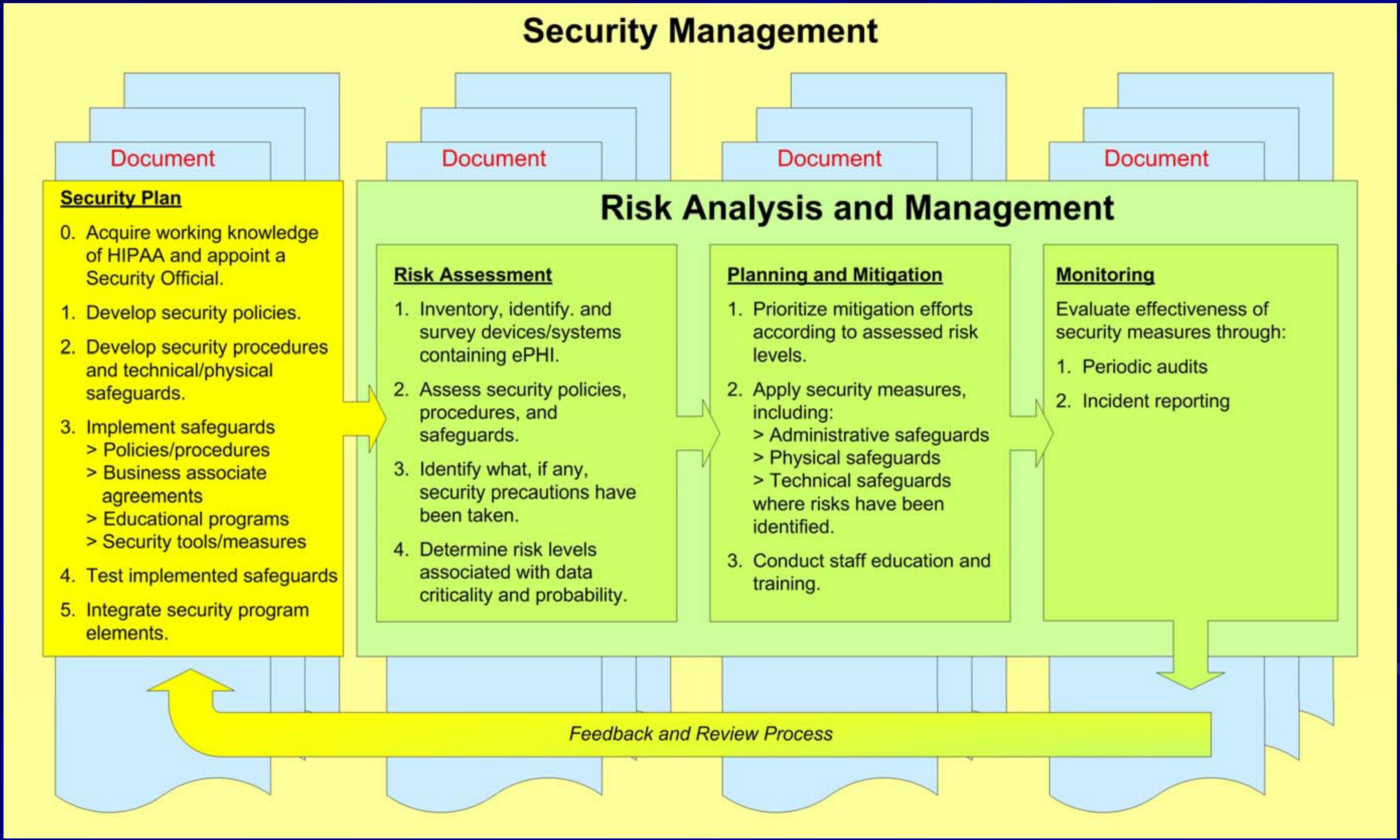
4
Determine Gap

5
Formulate & Implement Plan

6
Test & Measure Effectiveness of Plan

HIPAA's Security Rule

Overview of Compliance Process



Security Management

Document

Document

Document

Document

Security Plan

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

Risk Analysis and Management

Risk Assessment

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

Planning and Mitigation

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

Monitoring

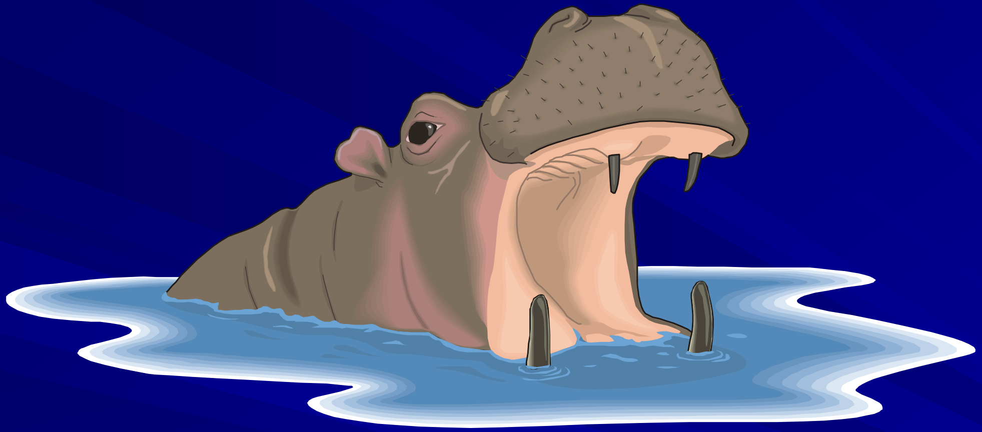
Evaluate effectiveness of security measures through:

1. Periodic audits
2. Incident reporting

Feedback and Review Process

Questions?

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



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