HIPAA Summit West

San Francisco, CA

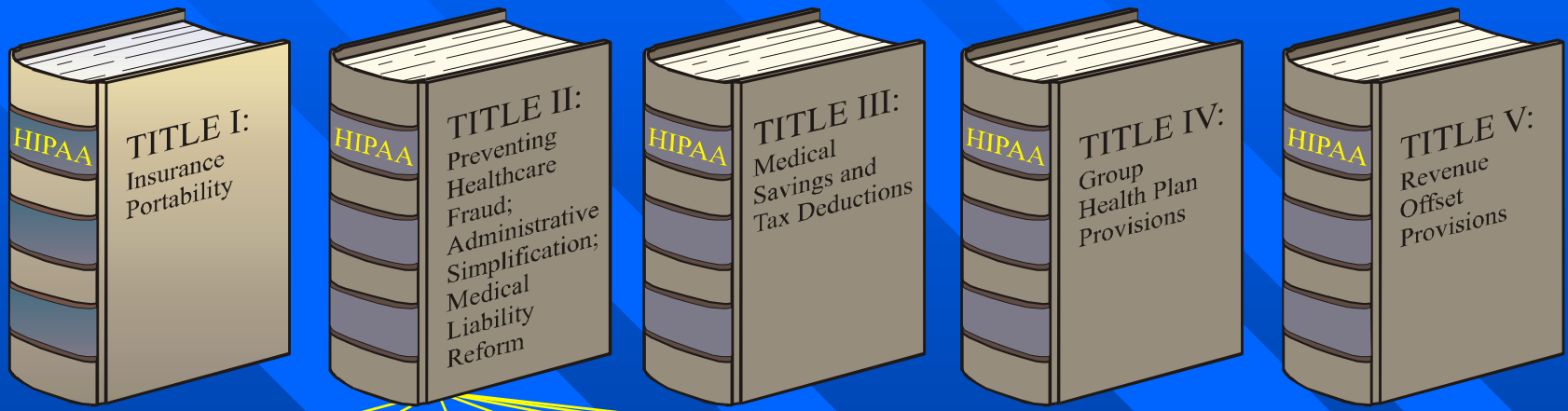
HIPAA Security: Impact on Biomedical Technology, Devices & Systems

June 22, 2001

Technology in Medicine,Inc

Portion of HIPAA That Most Impacts Healthcare Providers

Relevant Portion of HIPAA



Subtitle A: Fraud and Abuse Control Program

Subtitle B: Revisions to Current Sanctions for Fraud and Abuse

Subtitle C: Data Collection

Subtitle D: Civil Monetary Penalties

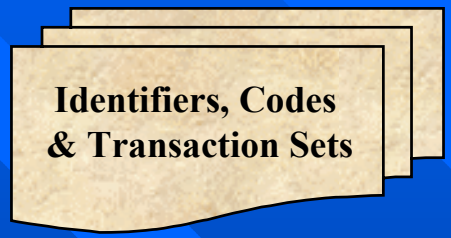
Subtitle E: Revisions to Criminal Law

Subtitle F: Administrative Simplification

Subtitle G: Duplication & Coordination of Medicare-Related Plans

- Identifiers, Codes & Transaction Sets
- Privacy Rules
- Security Rules

HIPAA Identifiers, Codes & Transaction Sets



Standards for electronic transactions

- Scheduled effective date: October 2002
- National standards developed for the healthcare industry for *electronic data interchange* (EDI)
- Intended to eliminate paper & incompatible electronic formats … reducing need for duplicate data entry, photocopying & faxing
- Goal is to improve efficiency & substantially reduce administrative costs in healthcare industry

HIPAA Privacy Rules

Privacy rules

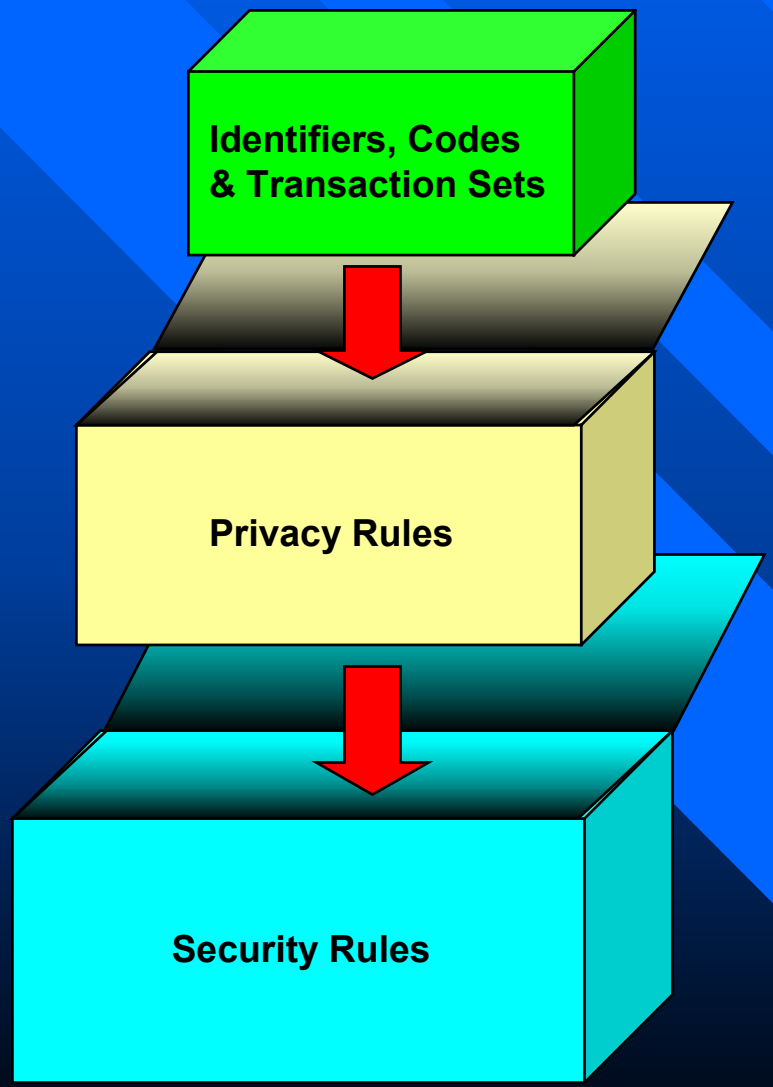
- Scheduled effective date: April 2003
- Rules deemed necessary to protect data in electronic transactions … but whose scope encompasses all protected health information (oral, written, or electronic)
- Rules limit use of protected health information
  - ✓ Patient's authorization required before protected health information can be used for anything other than treatment, payment or healthcare operations … and patient has right to know who has accessed their information
  - ✓ Patient must be permitted access to their own information and must be able to challenge any information they feel is in error

HIPAA Security Rules

Security rules

- Anticipated effective date: mid- to late- 2003
- Rules deemed necessary to insure privacy & confidentiality of protected health information … but whose scope encompasses not only *confidentiality* but also the *integrity* and *availability* of ***all*** health information related to an individual that is electronically maintained or transmitted
- Rules outline detail required administrative procedures, physical safeguards, technical security services & technical security mechanisms

Effective implementation depends on "packaging" HIPAA Rules



Because they are in electronic form, **Identifiers, Codes & Transaction Sets** require additional **Privacy** precautions (as spelled out by HIPAA)

Effective **Privacy** requires **Security** precautions (as spelled out by HIPAA)

Categories of Healthcare Information: HIPAA's Privacy & Security Rules

Info/Data Relevant to HIPAA's Privacy & Security Rules

- **Privacy Rule**
  Applies to ***Individually Identifiable Health Information*** (IIHI) or
  Protected Health Information (PHI)
- **Security Rule**
  Applies to ***Health Information Related to an Individual***

Standards for Privacy Apply to Individually Identifiable Information

Individually Identifiable Health Information (IIHI) is information/data that:

1. Is created or received by the healthcare provider… and
2. Relates to the past, present, or future … health or condition of an individual, the provision of care to an individual …and
   i. Which identifies the individual, or …
   ii. There is a reasonable basis to believe that the information can be used to identify the individual

Federal Register, December 20, 2000

Info/Data addressed by *Privacy Rule*

Individually Identifiable Health Information (IIHI) or ***Protected Health Information*** (PHI) ~ examples include:

- Patient name,
- Patient ID #
- Patient likeness (e.g., photo)
- Any data that in some combination could be used to identify patient (e.g., address)

Standards for Security Apply to *Health Information*

Health Information means any information, whether oral or recorded in any form or medium, that –

1) Is created or received by a health care provider … and
2) Relates to past, present or future … health or condition of an individual, the provision of health care to an individual …

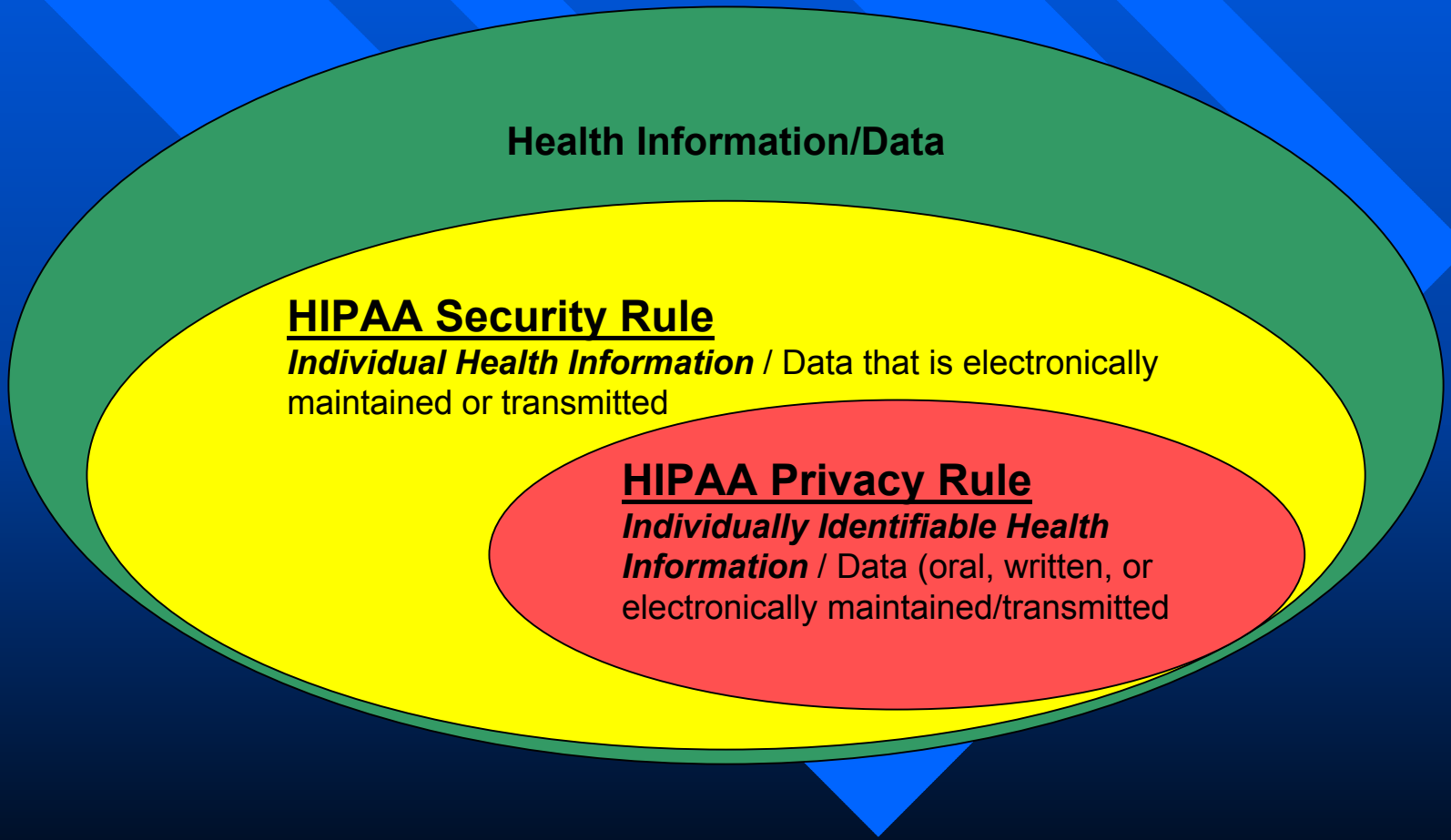
Federal Register, p. 43264
August 12, 1998

Info/Data Addressed by *Security Rule*

Health Information related to** (but not necessarily identifying) **an Individual ~ examples include:

- Diagnostic data
- Therapeutic data
- Any component of medical records
- Any component of billing info

Relationship between Info/Data addressed by *Privacy & Security Rules*



Complying with HIPAA's Privacy & Security Rules

Privacy & Security
are two separate concepts

- **Privacy** defined as controlling who is authorized to access information (the right of individuals to keep information about themselves from being disclosed)
- **Security** defined as the ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss

---

- Can have **Security** without **Privacy** but
- Cannot have **Privacy** without **Security**

Compliance with HIPAA's Privacy Rule

Typically 99% of HIPAA Privacy compliance is organizational, operational, cultural (i.e., the organization's policies, procedures and the staff's adherence to those policies & procedures). Key elements include:

- Privacy officer
- Privacy committee
- Policies
- Procedures
- Staff education
- Contacts with *Business Associates*
- Audit & review

Compliance with HIPAA's Security Rule

Typically 75% of HIPAA Security compliance is organizational, operational, cultural. The remaining 25% is "technical". Key elements include:

- Security officer
- Security committee
- Policies & Procedures
- Staff education
- Inventory
- Physical safeguards
- Technical security services
- Technical security mechanisms
- Contacts with *Business Associates*
- Audit & review

HIPAA Security Rule's Impact on Biomedical Technology

Scope of HIPAA Security Standards

- ***Applicability***

  The security provisions of HIPAA apply to … any **health care provider** that electronically maintains ***or*** transmits **any health information** ***relating to an individual***.

- ***Specific Requirements***

  The **security** standard requires that each health care entity engaged electronic maintenance *or* transmission of health information

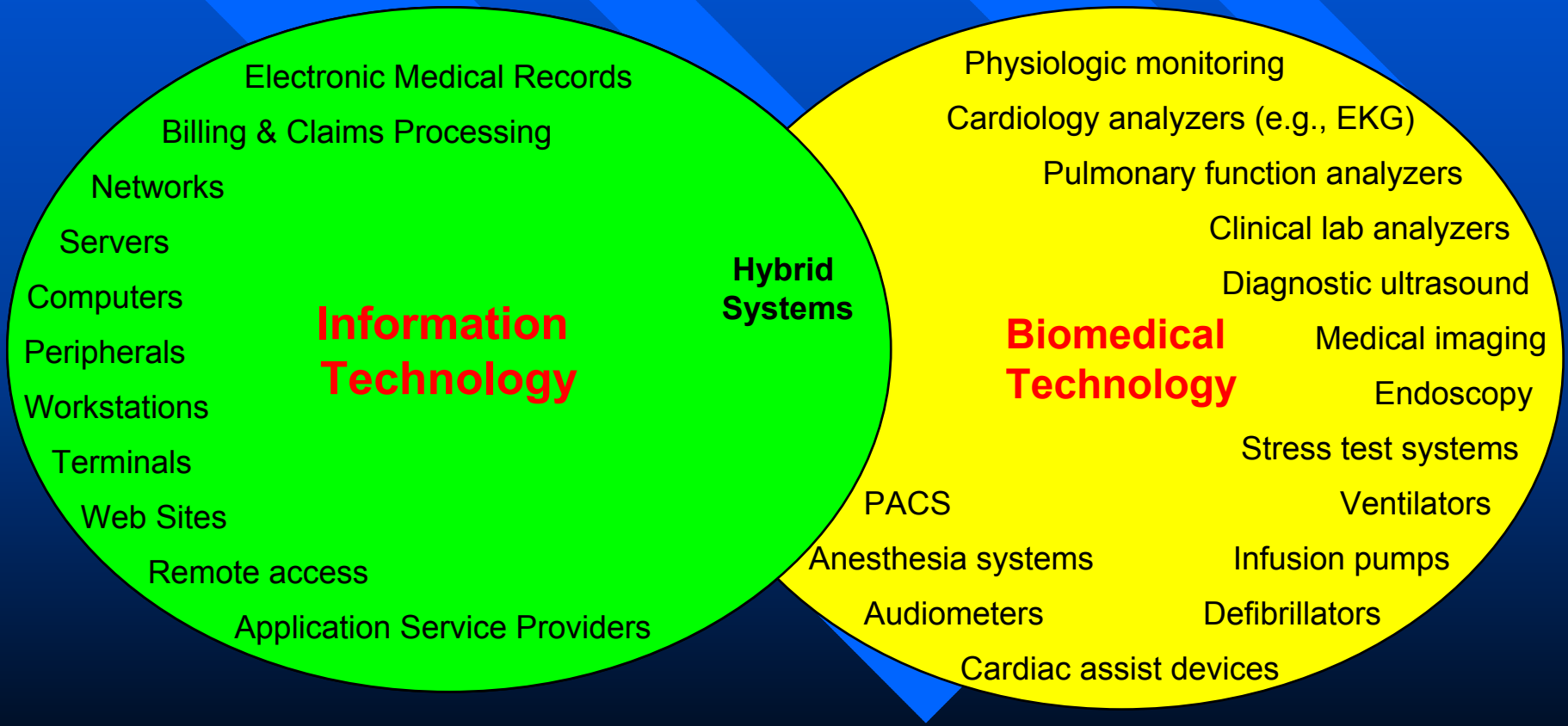
  - ✓ assess potential risks and vulnerabilities to the individual health data in its possession in electronic form, and
  - ✓ develop, implement, and maintain appropriate security measures.
  - ✓ Most importantly, these measures must be documented and kept current.

  The standard consists of

  - ✓ requirements that a health care entity must address in order to safeguard the ***integrity***, ***confidentiality***, and ***availability*** of its electronic data.
  - ✓ implementation features that must be present in order to satisfy each requirement

Federal Register, pp. 43245 & 43250
August 12, 1998

Examples of Devices/Systems Maintaining / Transmitting *Individual Health Data* in Electronic Form



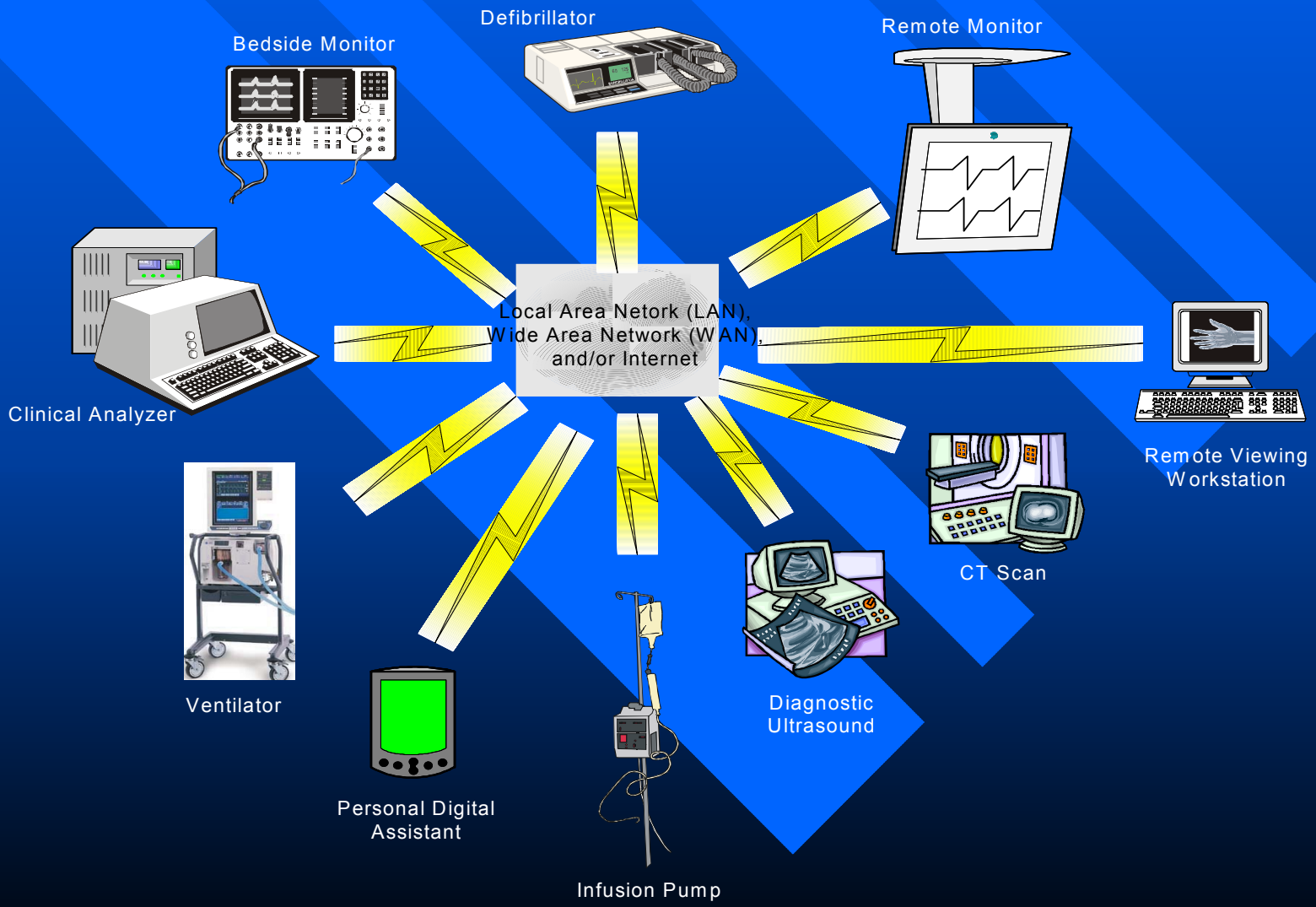
Relevance to Biomedical Technology

Biomedical devices & systems represent a substantial & growing risk area. The basis of growing security risk lies in two trends:

- Biomedical devices and systems are being designed and operated as special purpose computers…. more features are being automated, increasing amounts of health data are being collected, analyzed & stored in these devices
- There has been a rapidly growing integration & interconnection of disparate biomedical (and information) technology devices & systems where health information is being increasingly exchanged

Biomedical devices & systems represent a substantial repository of health information and therefore must be considered when implementing any comprehensive security program

Medical Devices & Systems
Typical Data Interconnects



Biomedical Technology: Preparatory Steps for HIPAA Security Compliance

1) Acquire working knowledge of relevant HIPAA rules
2) Inventory devices & systems
3) Identify devices & systems with health data
4) Assess risk associated data compromise for devices & systems containing health data
5) Determine existing precautions taken for affected devices & systems
6) Gap analysis (determining difference between where organization "is" and where it "should be")

Step 1: Acquire Working Knowledge of Relevant HIPAA Rules

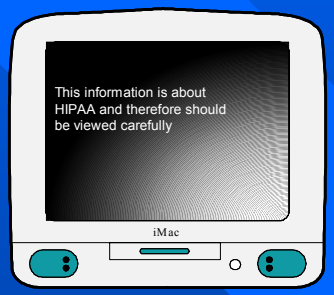
- Review proposed Security Rules published by HHS (Federal Register: Aug 12, 1998) or, when available later this year, final Security Rules
- Learn your organization's HIPAA Security preparedness
  - ✓ Roles & Responsibilities
  - ✓ Policies & procedures
  - ✓ Education programs
  - ✓ Physical safeguards
  - ✓ Technical security services & mechanisms
- Use internet (HIPAA related listservs & web-sites) and professional societies to stay current on HIPAA developments

Step 2: Inventory Medical Devices & Systems

Areas likely to have affected Devices & Systems

- Clinical lab information systems (chemistry)
- Medical imaging (ultrasound, NMR, CT, Mammo, Bone density)
- Radiation therapy
- Pharmacy
- Special Care (SCU, ICU, CCU)
- Fetal & Neonatal monitoring
- Surgery (video systems, monitoring)
- Pulmonary function
- Cardiology (EKG, Holter, pacing)
- Physical therapy (exercise systems)
- Telemedicine (extending diagnostic technologies to clinics, physician offices, patient's home & workplace)

Step 3: Identify Devices & Systems Containing Health Information

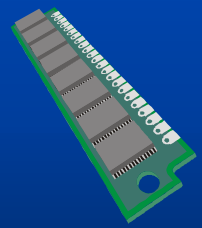


Displays

Paper (i.e., Printouts)

X-Rays

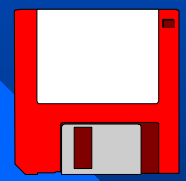
Photographs



Non-volitile Memory

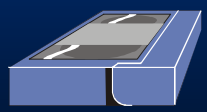
Hard Disk Drives

PC Card or Memory Stick

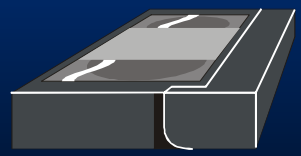


Removable Diskette

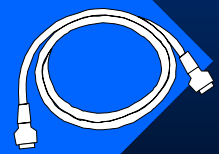
CD-Rom, DVD or Optical Disk



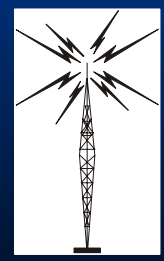
Digital Data Tapes



VCR Tapes



Telephone, Network or Direct Connect Cable



Wireless

Step 3: Identify Devices & Systems Containing Health Information

Health information is at risk where it is:

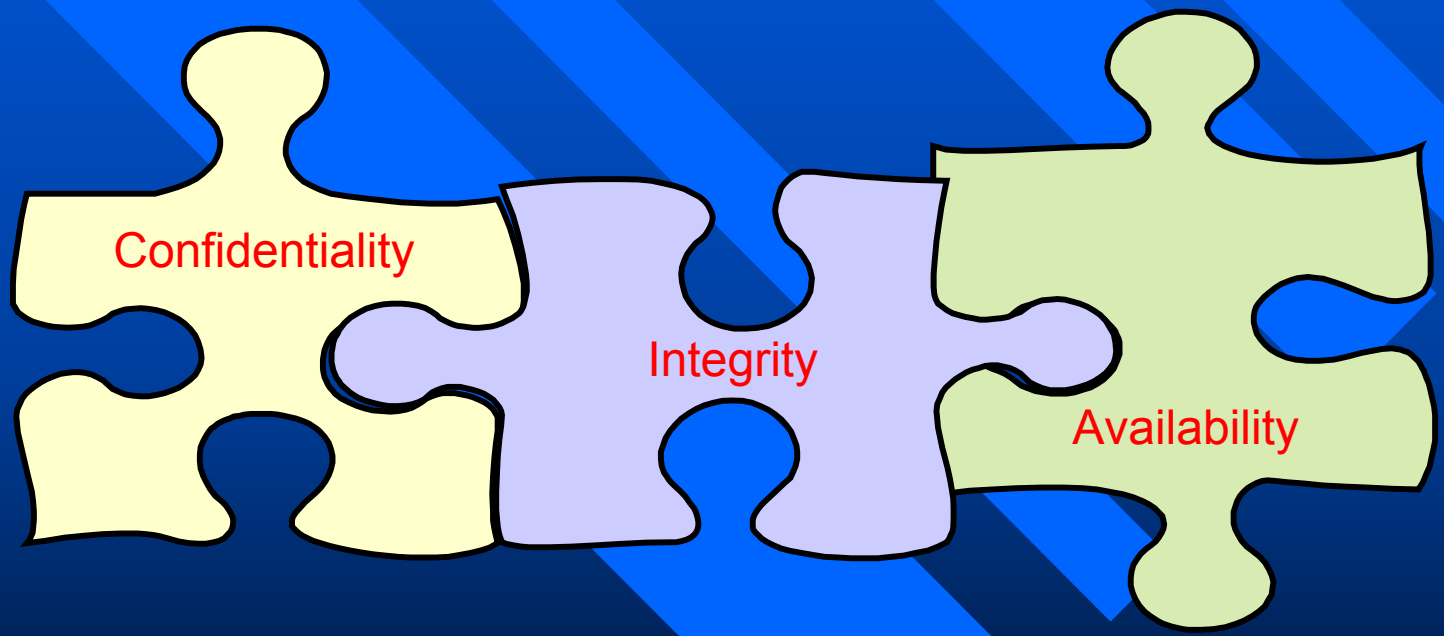
Printed
- Plain paper,
- Strip chart,
- photo, or
- X-ray film

Displayed
- CRT,
- liquid plasma,
- liquid crystal, or
- LED display

Transmitted and/or Received via
- Telephone,
- Network,
- Direct cable connect
- Wireless

Recorded electronically
- Hard disk,
- Floppy disk
- Compact disk,
- Non-volatile memory
- Tape

Step 4: Assess Risks associated with Health Info (3 Categories of Risk)



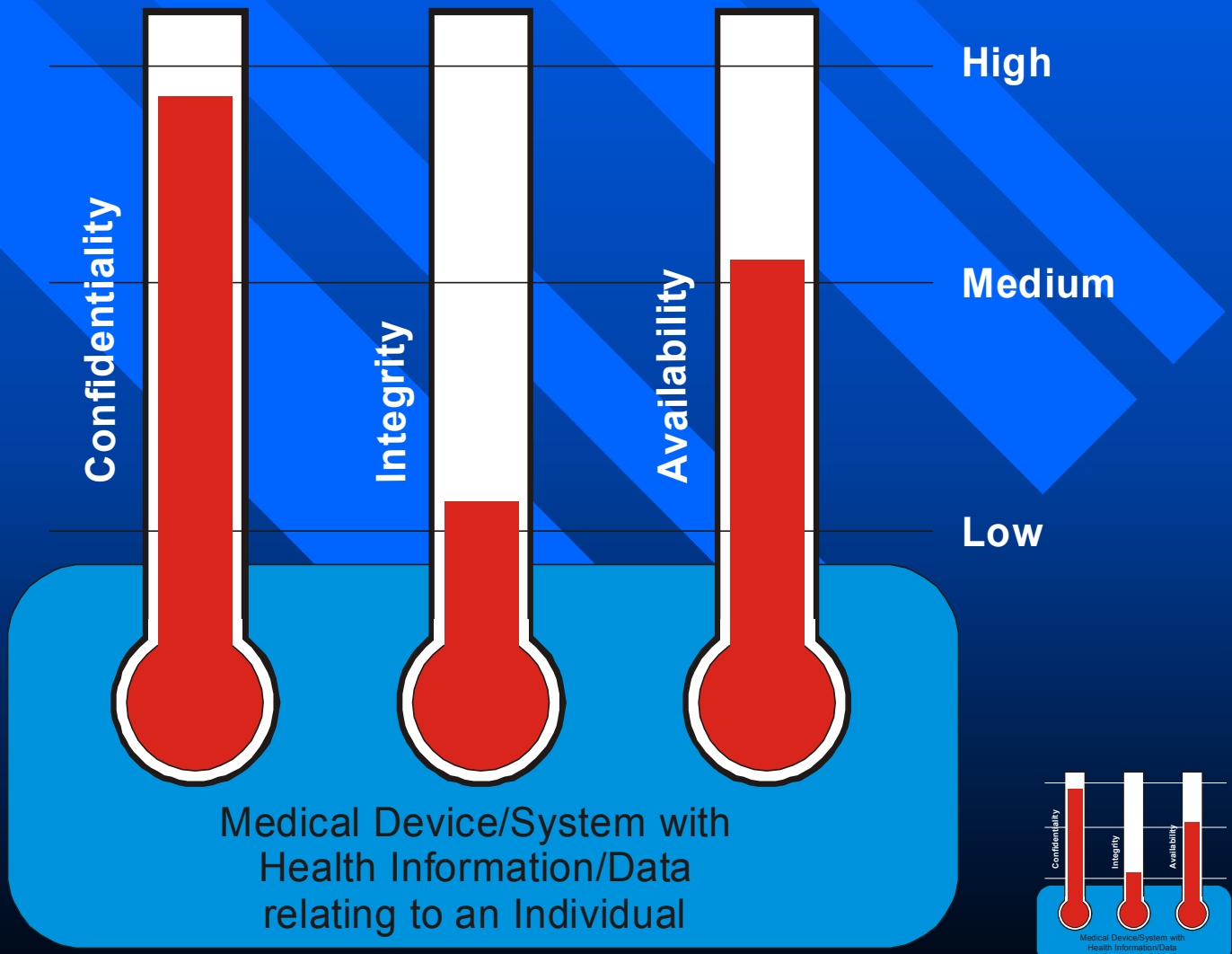
Step 4: Assess Risks associated with Health Info on Devices & Systems

Requirements a health care entity must address in order to safeguard electronic data's

- **Confidentiality:** degree to which *individual health data* requires protection from unauthorized disclosure
- **Availability**: degree to which *individual health information* must be available on a timely basis to meet operational requirements or to avoid compromising care … also includes insuring that health information is used only for intended purposes
- **Integrity**: degree to which *individual health data* must be protected from unauthorized, unanticipated, or unintentional modification

Federal Register, p. 43250
August 12, 1998

Step 4: Assess Risks Associated with Health Info on Device & Systems



Step 4: Assessing Risks

Ranking Security Risk Level

RISK LEVEL	Impact on Patient		Impact on Organization			
	Potential degree to which health care would be adversely impacted by compromise of availability or integrity of information	*Potential degree to which privacy would be adversely impacted by compromise of confidentiality of information*	*Potential degree to which interests would be adversely impacted by compromise of confidentiality, availability or integrity of information*	*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 and/or treatment	Extremely grave damage to organization's interests	Major	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	Serious damage	Moderate	Moderate Fines	Legal
Low	Minor Impact	Could not be associated with a specific patient	Minor damage	Minor	None	Admiistra-tive

Step 5: Determine Existing Precautions
(taken for affected devices & systems)

a) Affected Device/System *Displays* Data

- ✓ Is the display only physically observable by authorized staff/users?
- ✓ Is device/system kept in secure area accessible only by key, combination lock, access card or similar?
- ✓ Does data access require a user name & password (or other appropriate authentication method)?

Step 5: Determine Existing Precautions
(taken for affected devices & systems)

b) Affected Device/System *Outputs* Data (e.g., paper, film, photo, removable storage)

- ✓ Is the output stored in a secure location (i.e., in a room or cabinet secured by key, combination lock, access card or similar)?
- ✓ Is the output destroyed by acceptable means when no longer needed? For example:
  - o Shred paper, film, photo
  - o Erase/overwrite disks, pc cards, memory stick
  - o Deposit in locked "Destruction Bin" for disposal by a bonded service

Step 5: Determine Existing Precautions
(taken for affected devices & systems)

c) Affected Device/System *Stores* Data (e.g., hard disk, non-volatile memory, PC card, memory stick, diskette, CD-ROM, data tape, VHS tape)

- ✓ Is device/system kept in secure area accessible only by key, combination lock, access card or similar?
- ✓ If device/system is not kept in secure area, are all removable storage components (i.e., diskette, PC Card, memory stick, CD-ROM, data tape, VHS tape) secured (i.e., not removable) when not in use?
- ✓ Does data access require a user name & password (or other appropriate authentication method)?

Step 5: Determine Existing Precautions
(taken for affected devices & systems)

d) Affected Device/System *Transmits/Receives* Data via Cable or Wireless

- ✓ Is data transmitted via secure cable connection (i.e. no access possible via unsecured hub or other unsecured intermediate connection)?
- ✓ Is data encrypted prior to transmission via wireless or public network?
- ✓ Does the system permit remote access?
  - o Does the system security restrict remote access to specific devices or locations?
  - o Does the system log and provide audit trail of remote access activity?

Step 5: Determine existing precautions (taken for affected devices & systems)

e) All Affected Devices & Systems

- ✓ Is the device/system physically secure?
  - o Is the system kept in secure area, inaccessible except to authorized users?
  - o Are components secure within the system (i.e., can any component containing data be removed)?
- ✓ Does data access require appropriate ID & password (or other appropriate authentication)?
- ✓ Is critical data backed up & stored in secure location?
- ✓ Is the system PC based?
  - o Does the system run virus protection?
  - o Does it prevent boot-up from an unauthorized boot disk?
- ✓ Have device/system users been trained in security and are they practicing appropriate security procedures?

Step 6: Gap Analysis

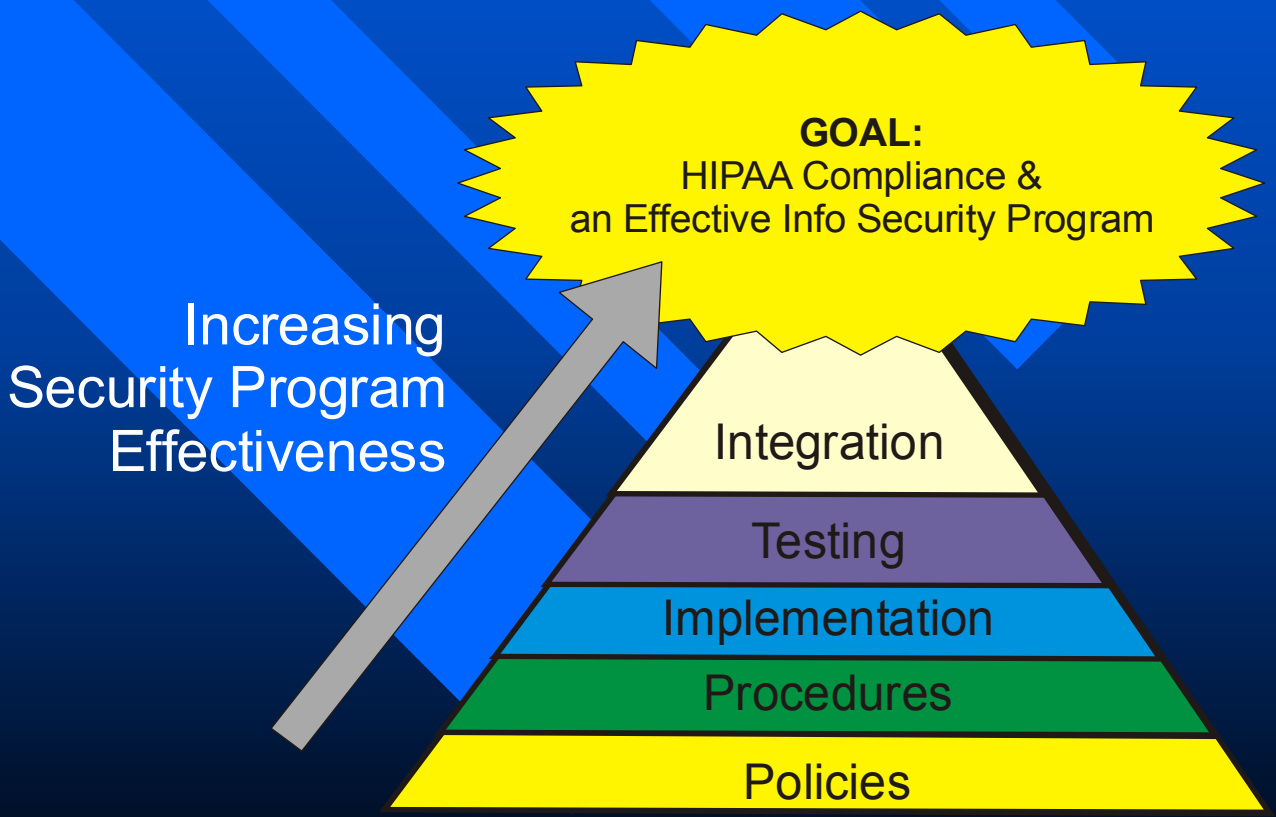
"Gap" is difference between:

- Current security program (from inventory, risk assessment & determination of current security precautions) and
- Security program mandated by HIPAA

Step 6: Gap Analysis

Gap analysis (and subsequent audits) security program effectiveness in terms of:

- ✓ Policies
- ✓ Procedures
- ✓ Implementation
- ✓ Testing
- ✓ Integration



Step 6: Gap Analysis

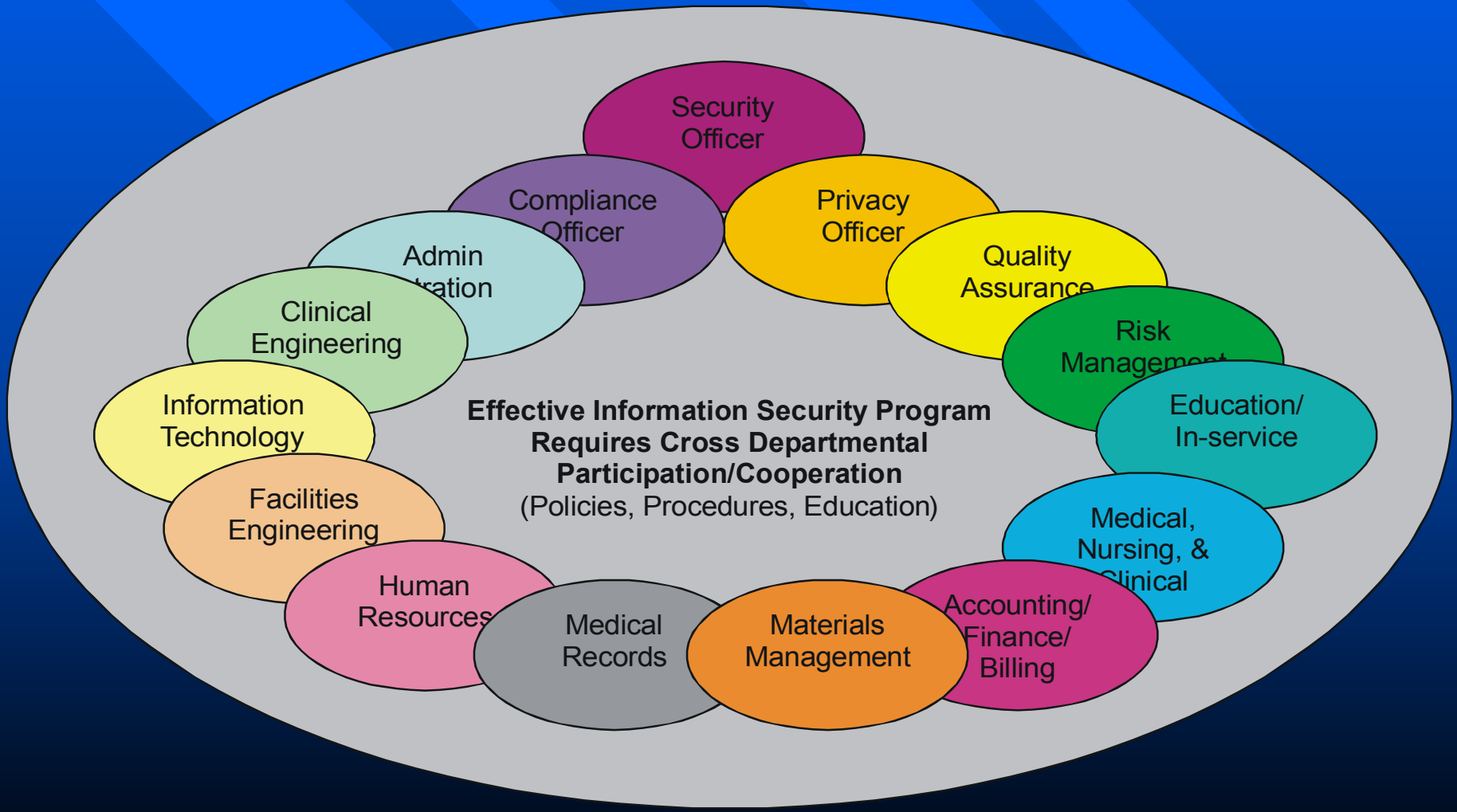
Gap analysis is used to prepare plan for

- Achieving HIPAA compliance and
- Implementation priorities

Biomedical Technology: Steps for achieving HIPAA Compliance

1. Assign roles & responsibilities ~ involve all affected departments
2. Treat Security Risks (HIPAA Security Matrix)
   a) Administrative procedures
   b) Physical safeguards
   c) Technical security services
   d) Technical security mechanisms
3. Educate Staff
4. Require cooperation of *Business Associates*
5. Establish on-going audit & review process
6. Document! Document! Document!

Step 1: Assign roles & responsibilities
Cross-departmental Participation/Cooperation



Step 2: Treat Security Risks

Four Categories of Requirements in HIPAA's Security Matrix			
Administrative Procedures	**Physical Safeguards**	**Technical Security Services**	**Technical Security Mechanisms**
Documented, formal practices to manage the ✓ Selection & execution of security measures to protect data and ✓ Conduct of personnel in relation to the protection of data	Protection of physical computers systems (*any hardware storing or transmitting health data*) and related buildings & equipment from ✓ Natural & environmental hazards (e.g., fire, flood) ✓ Intrusion (i.e., use of locks, keys and administrative measures to control access)	Processes that are put in place to ✓ Protect information access ✓ Control & monitor information access	Processes put in place to prevent unauthorized access to data that is transmitted over a communications network

Step 3: Educate Staff

Conduct orientation of new staff and on-going education of existing staff on:

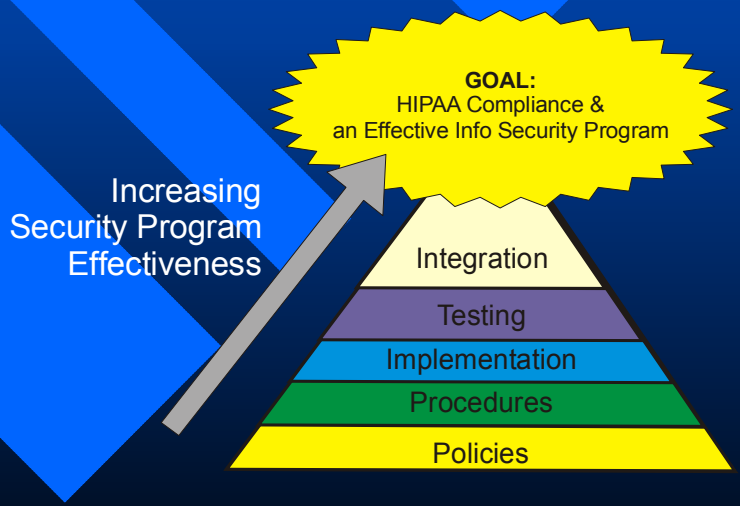
- Privacy & Security concerns
- Organization's Privacy policies & procedures
- Organization's
  - ✓ Security Policies,
  - ✓ Security Procedures
  - ✓ Technical security services
  - ✓ Technical security mechanisms

Step 4: Require Cooperation of *Business Associates*

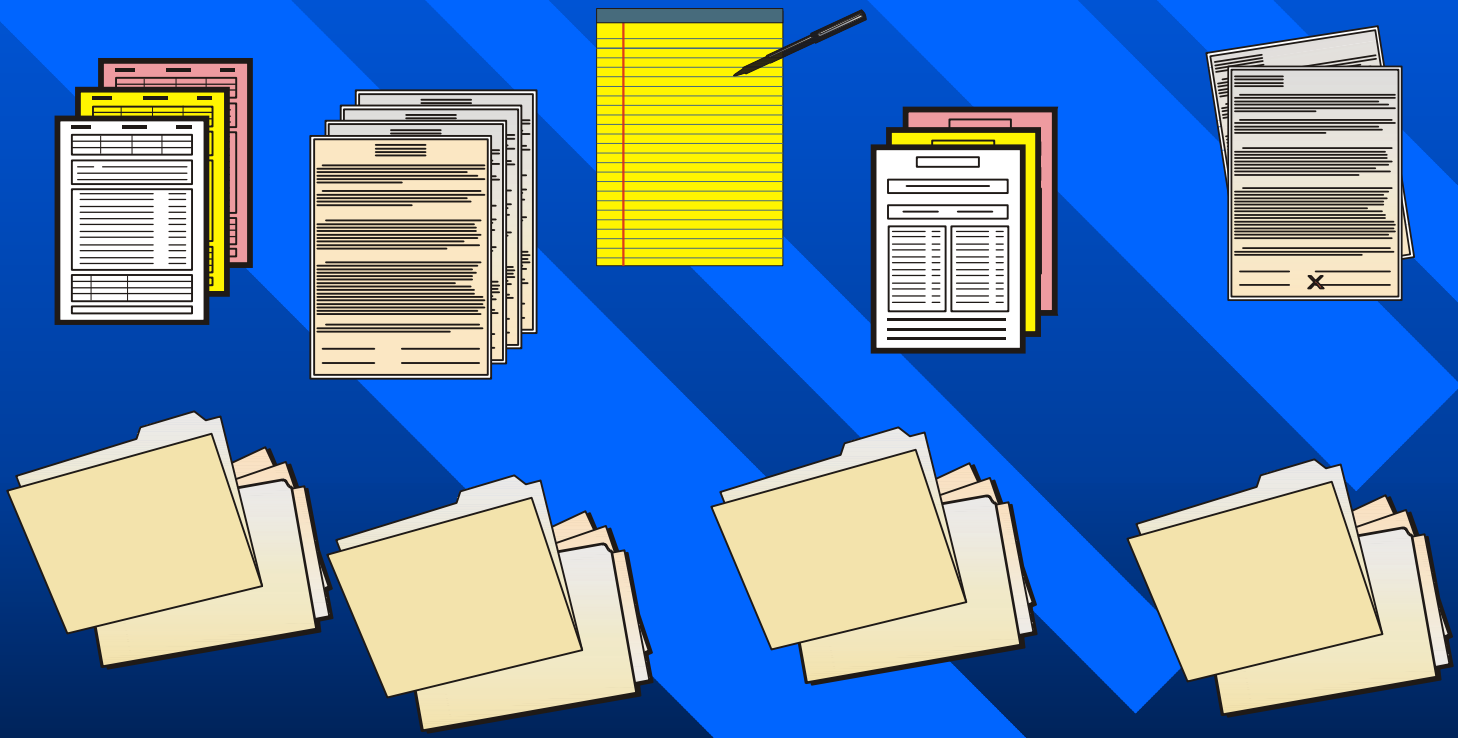
- Identify *Business Associates* (businesses that could conceivably access health data) ~ e.g.,
  - Medical device/system manufacturers
  - Independent service organizations (ISO)
  - Consultants, educators
- Establish formal agreements where *BA* agrees to:
  - Limit uses and disclosures of health data
  - Destroy or return any health data when no longer needed
  - Maintain safeguards to protect health data
  - Report to organization the use or disclosure

Step 5: Establish on-going audit & review process

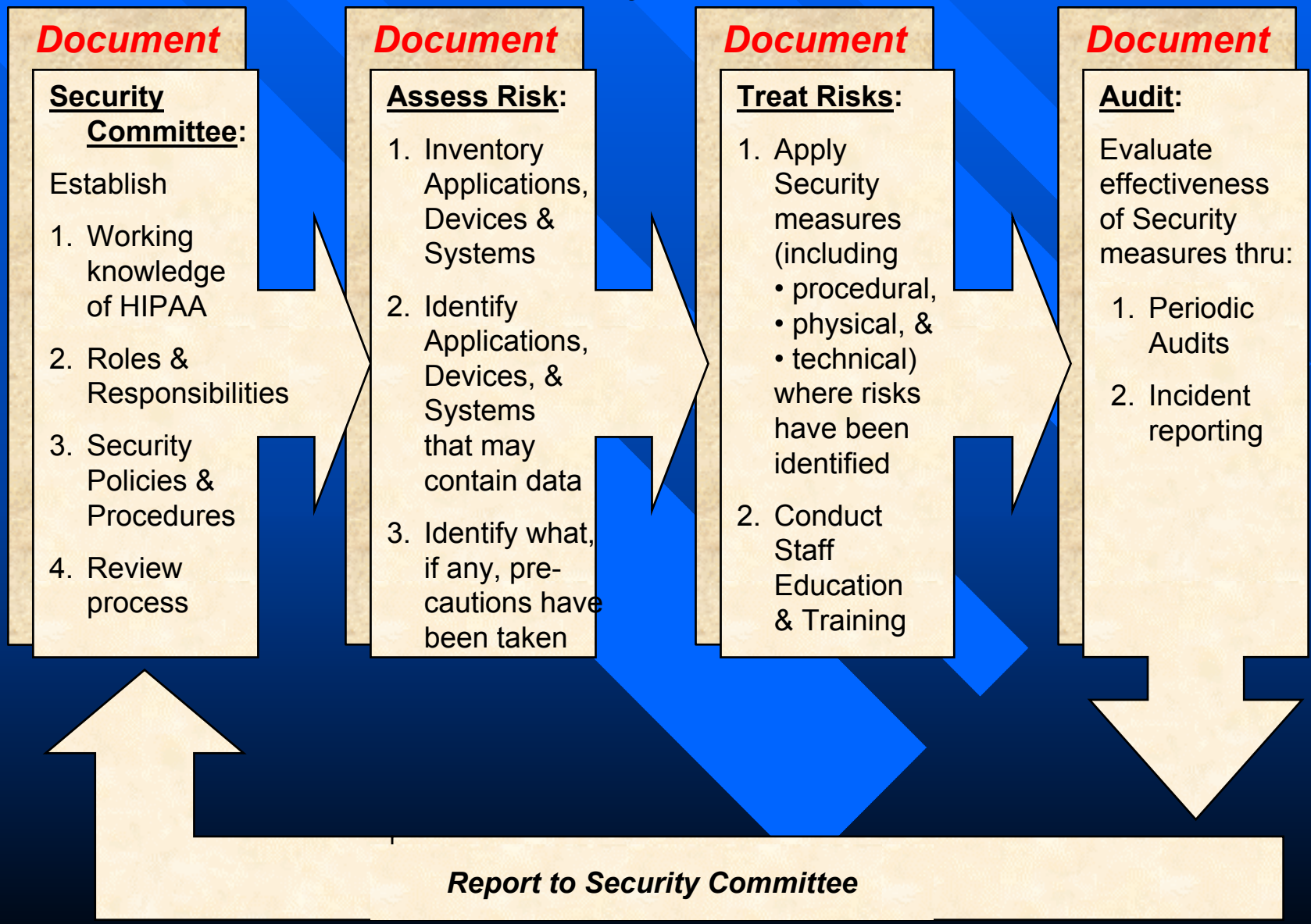
- Audit to insure requirements associated with security elements & their implementation features are effectively met
- Analyze information security Incident Reports to determine need for corrective action



Step 6: Document, Document, Document



HIPAA Security Risk Assessment



Technology Standards for Medical Device/System Manufacturers

- How are the technology manufacturers incorporating current standards in their products?
- What implication do these standards have on HIPAA compliance?

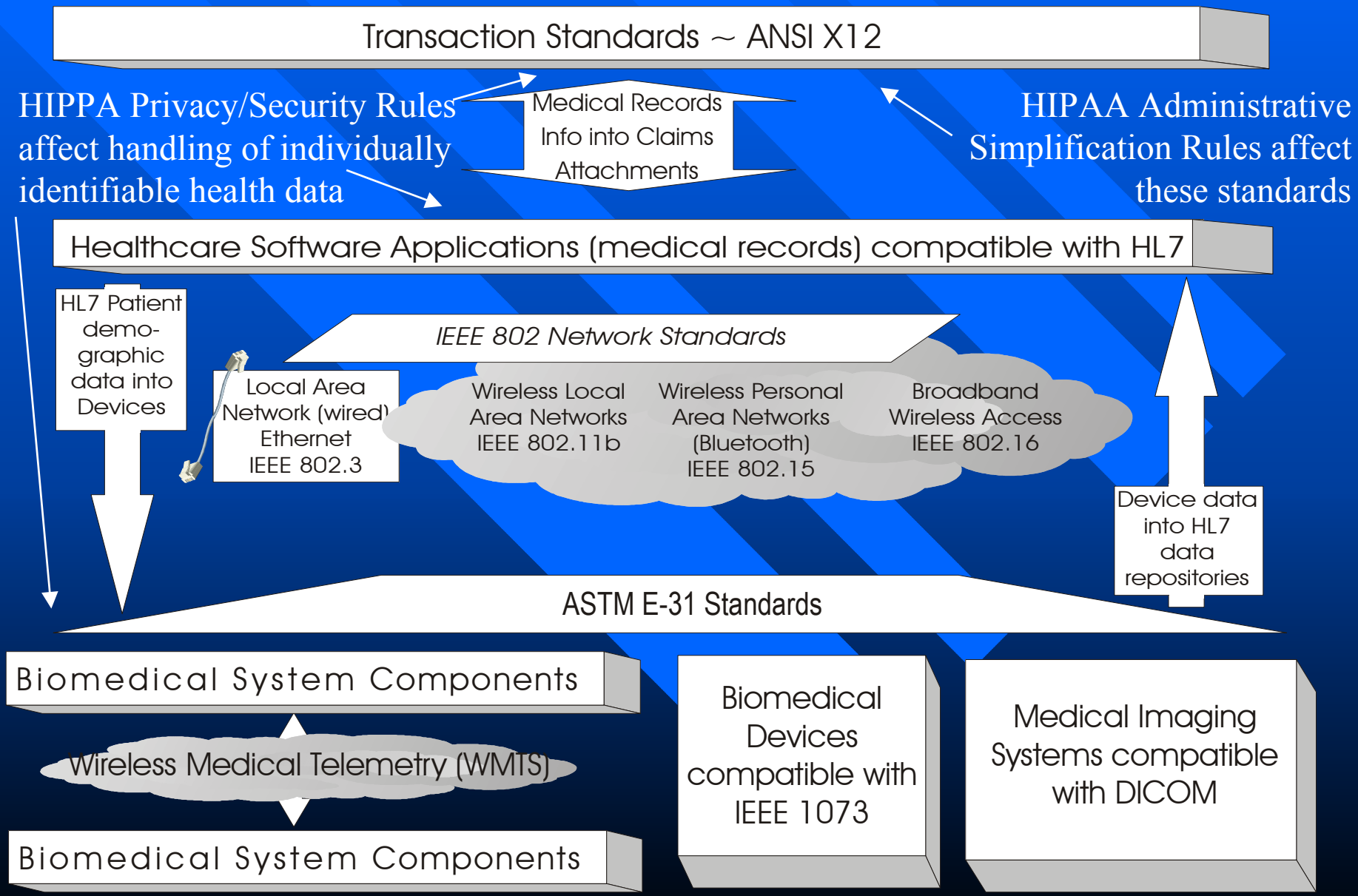
Industry Standards

- **Medical Information Bus ~ MIB (IEEE 1073)**
  Designed for communications in health care applications, primarily between bedside medical devices and patient care information systems (e.g., transmitting data to/from patient-connected bedside devices such as monitors, ventilators & infusion pumps)
- **Digital Imaging & Communications in Medicine (DICOM 3.0)**
  Designed for transmitting radiological images between imaging systems (ultrasound, MRI, CT, and x-ray) and computerized systems and peripherals (monitors, printers, storage devices)
- **Standards on Healthcare Informatics (ASTM *E-31*)**
  Designed to address architecture, content, portability, format, privacy, security and communications in medical devices and healthcare information systems

Industry Standards (cont)

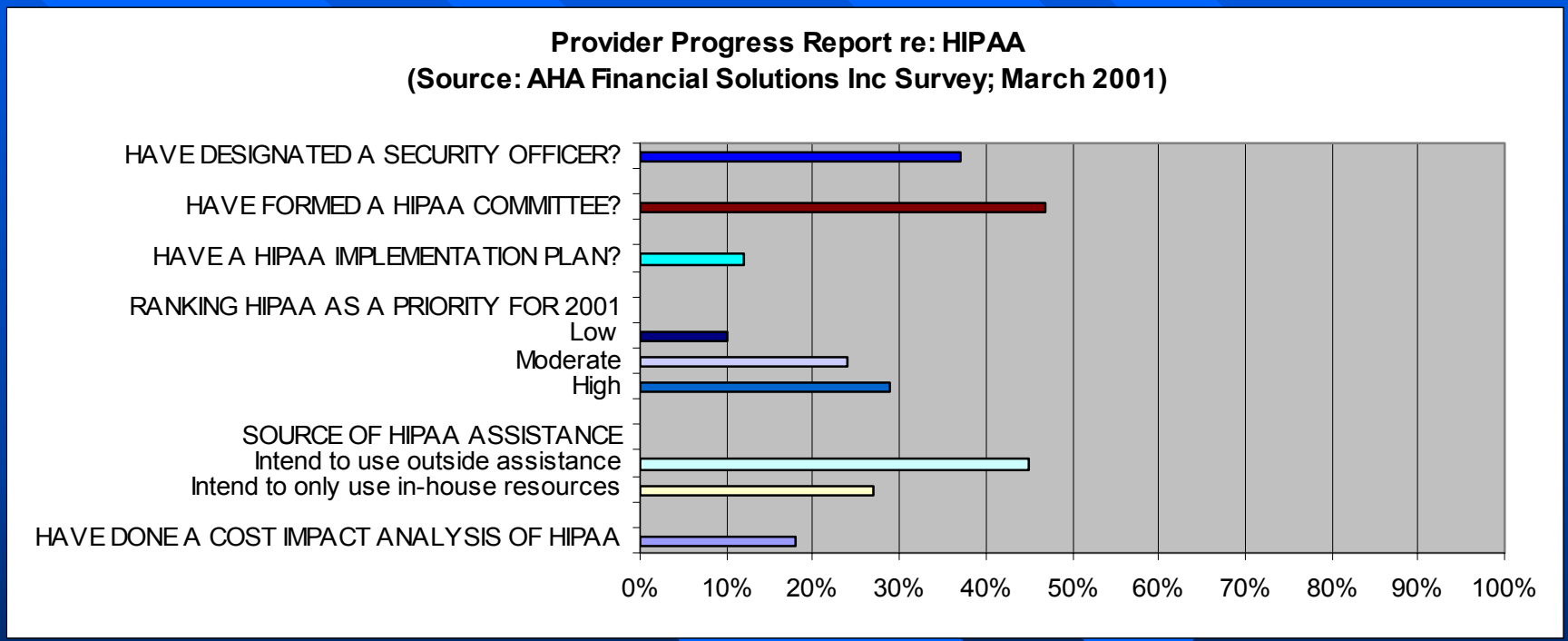
- **IEEE 802 Wired & Wireless Networking Standards**
  Standards for networking devices and systems
  - Local Area Network (*Wired*) ~ Ethernet (IEEE 802. 3)
  - Wireless Local Area Network (IEEE 802.11b)
  - Wireless Personal Area Network ~ WIPAN (IEEE 802.15 ~ includes Bluetooth)
  - Broadband Wireless Access (IEEE 802.16)
- **Wireless Medical Telemetry (WMTS)**
  Standard for transmission of data between medical device components over 14 MHz of radio-frequency spectrum (priority allocated to medical applications by FCC in June 2000)
- **Health Level 7 (HL7)**
  ASCII-based, batch transaction standard defining application level messages used by major applications such as admission/discharge/ transfer (ADT), orders, results, and clinical observations.
- **ANSI ASC X12**
  ASCII-based standard used for healthcare claims, referrals, payment/remittance advice, claim status, claim attachments, insurance plan eligibility, etc

Relationships between Industry Standards



Other HIPAA Issues

Provider Progress Report re: HIPAA



HIPAA Strategy for Providers

- Don't wait for final HIPAA disposition.
- "Writing is on the wall" …
- Embrace security & take lead …
- Experience with Y2K shows delay only results in:
  - ✓ Outlay of more effort (i.e., *delay = inefficiency*)
  - ✓ A compressed timeline
  - ✓ Significantly larger expenditures
- Delaying implementation of security
  - ✓ Postpones (i.e., loses) savings gained by efficiencies inherent in HIPAA
  - ✓ Results in competitive disadvantage …
    - » consider e-commerce (and e-health) in their business plans
    - » comprehensive information security program is an essential element in the foundation of any e-commerce or e-health enterprise

HIPAA vs Y2K

- **Y2K was a "*project*"**
  - Was a fixed time effort with a known deadline and "end date"
  - Compliance requires solution that was technology-oriented
  - Required coordinated effort across functional & organizational lines
- **HIPAA is a "*process*"**
  - Like Y2K has deadline (to achieve compliance) but unlike Y2K, requires on-going effort (i.e., no project "end date")
  - Compliance requires solution involving organizational & procedural changes as well as some technology changes
  - Like Y2K, also requires coordinated effort across functional & organizational lines

HIPAA Regulations are "Technology Neutral"

- No such thing as "HIPAA-compliant" technology
- HIPAA compliance requires development and implementation of effective Security Policies that are appropriate for the provider organization
- Technology must be selected & applied so as to support the implementation of whatever Security Policies the organization has established
- ***Therefore***, there is not a "HIPAA-compliant technology" but rather "HIPAA-compliant Security Policies"

HIPAA's Impact is Broad & Substantial

HIPAA will lead to tangible and intangible benefits by:

- Standardizing EDI format ~
  Reduced complexity associated with multiple standards, formats, definitions, identifiers
- Encouraging electronic data transfer
  Standardized electronic formats will make electronic data transfer more appealing among providers, payers and other business entities
- Vendors will not have to customize their products (reducing their cost)
- Serving as an enabler for e-Health (est. *$240 billion annually*) ~ a flood of new e-Health applications will be considered that would have been impossible to implement without standardized data systems

HIPAA will enable the Future of Healthcare

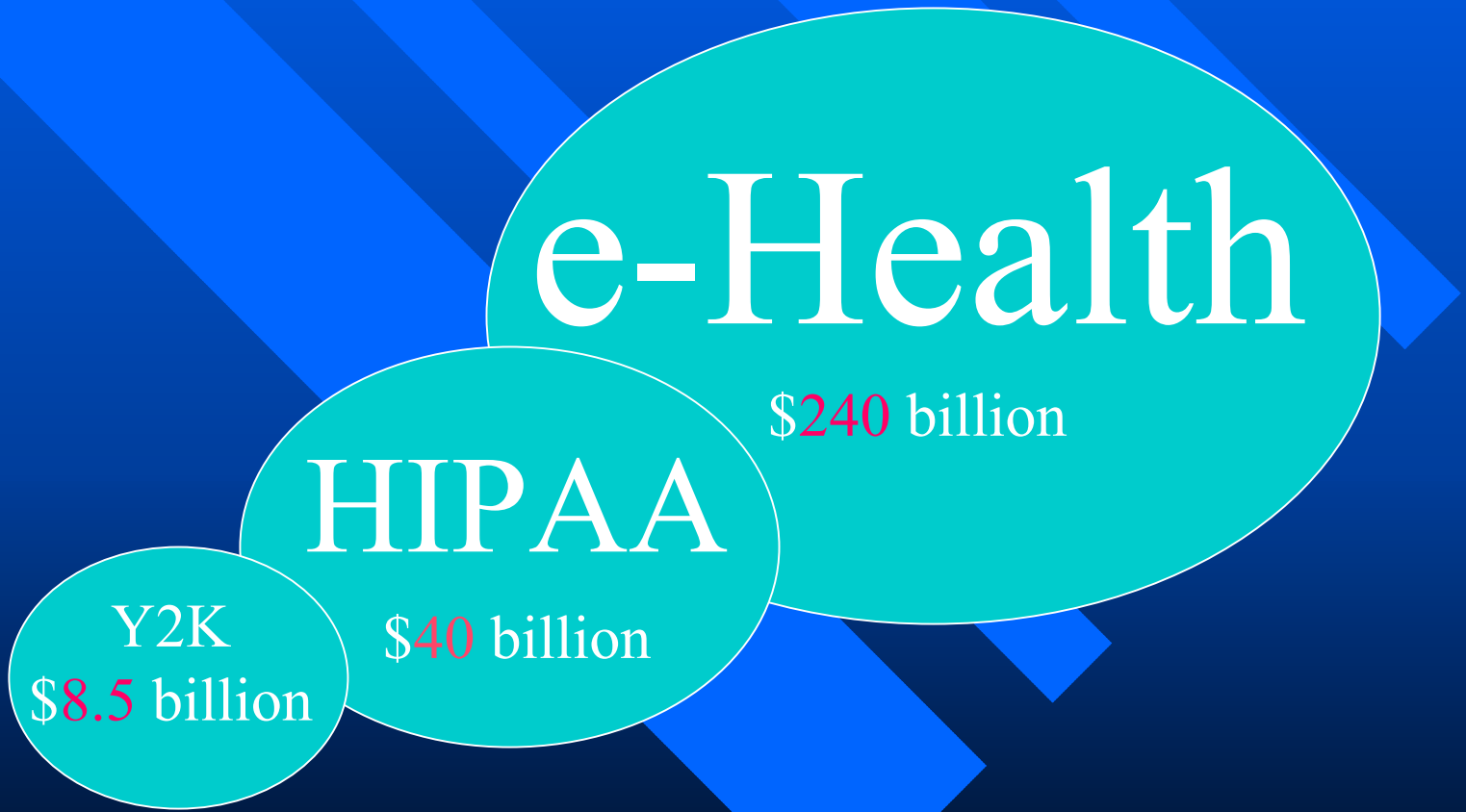
e-Health will result in revolutionary changes in application of Biomedical Technology:

- Biomedical Technology will make expanded use of broadband internet
- Technology will enable patients to access expert diagnosis & therapy regardless of where patient is located
- Focus of diagnosis & therapy will move from doctor's office & hospital to patient's home & workplace

Beyond HIPAA

Some (not so) Long-Term Implications

May you live in interesting times!
(Ancient Chinese blessing/ curse)



e-Health

Internet, World Wide Web, and networking technologies are substantially changing delivery of healthcare services.

- E-mail & Teleconferencing
- Access to medical information (i.e., medical web sites)
- Application Service Providers (ASP)
  Expert information systems
- Access to Patient Medical Records & Medical Images
- Telemedicine
  - ✓ Diagnosis (gather/analyze data) &
  - ✓ Therapy (administer treatment) remotely

e-Health: Telemedicine Provides the "Virtual Office" Visit

@Home or @Work

- Check physiologic parameters using sensors connected to transmitter
  - ✓ EKG, EEG, Respiration
  - ✓ Oximetry
  - ✓ Blood Pressure
  - ✓ Weight
  - ✓ Temperature
  - ✓ Auscultation of heart & breath sounds
  - ✓ Blood, urine, stool analysis
  - ✓ Expired respiratory gas
- Visual Examination
  - ✓ teleconference (video camera),
  - ✓ endo/oto/opthalmo scopes

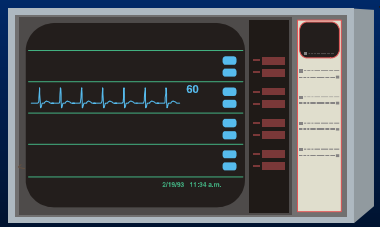
Trends Driving e-Health

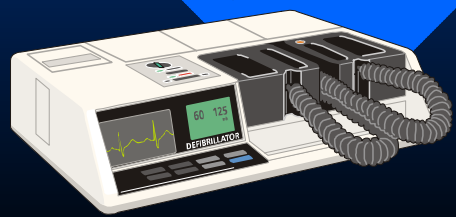
- Development of "enabling" standards for
  - ✓ Healthcare, Internet, networking & communication technologies
  - ✓ Content, format, privacy & security of data transmitted
- Demographics ~ aging population
  79% of healthcare spending is managing chronic disease
- Population demand for quality & thorough care
- "Wiring" of society (i.e., broadband Internet access)
- Need to reduce expenses
  moving from "bricks" to "clicks"
- Reimbursement changes (3rd party payers covering new technologies that improve care and help reduce costs)

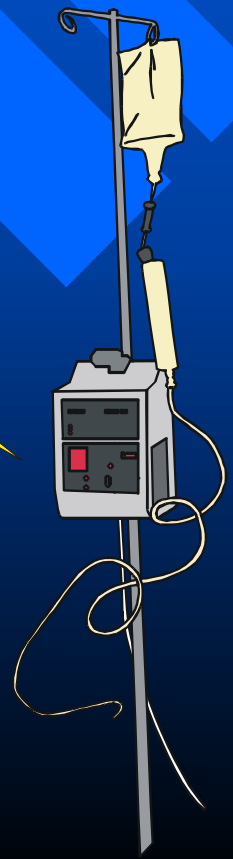
Equipment Management with Internet-connected Medical Devices

Devices on Internet transmit:

- Location
- Current Status & Settings
- Diagnostics
- Error Codes





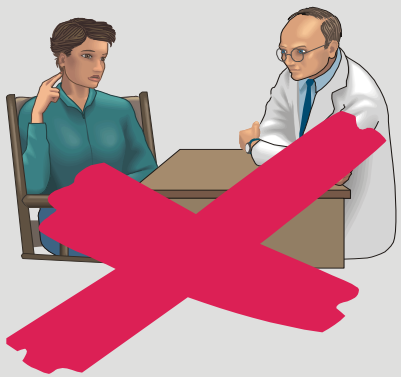


e-Health: Physician's & Other Healthcare Providers On-line

Physicians & other medical providers are using personal digital assistants (PDAs) to:

- Send/receive e-mail with patients and other members of healthcare team
- Obtaining patient status reports, test results
- Issuing prescriptions (less error prone) & orders

e-Health: Telemedicine Provides the "Virtual Office" Visit



Traditional
Patient - Doctor
Communications

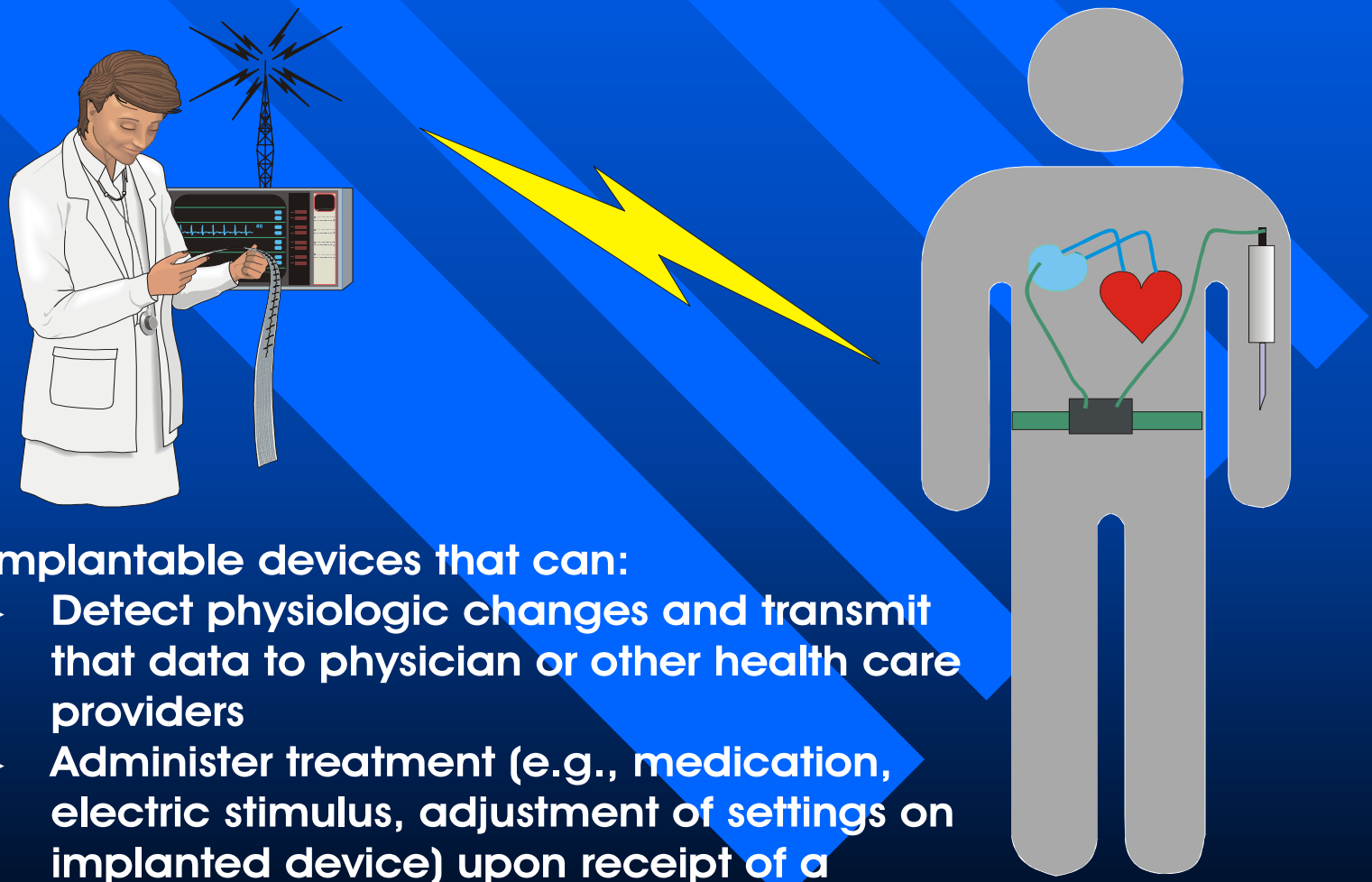
Physician

Teleconferencing & e-Mail
will become common form
of Patient - Doctor
communication

Patient

Specialist

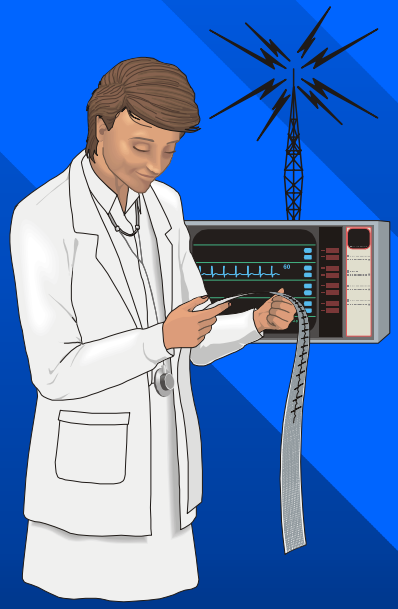
e-Health: Telemedicine Delivers Remote Diagnostics & Therapy

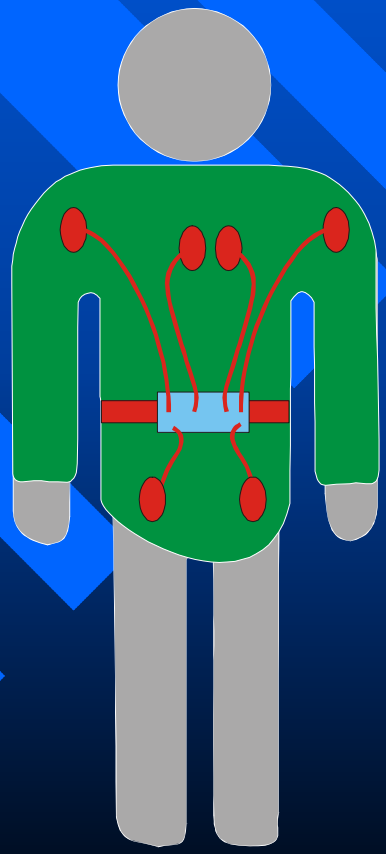


Implantable devices that can:

- Detect physiologic changes and transmit that data to physician or other health care providers
- Administer treatment (e.g., medication, electric stimulus, adjustment of settings on implanted device) upon receipt of a signal from a remote healthcare provider

e-Health: Telemedicine Delivers Remote Diagnostics & Therapy

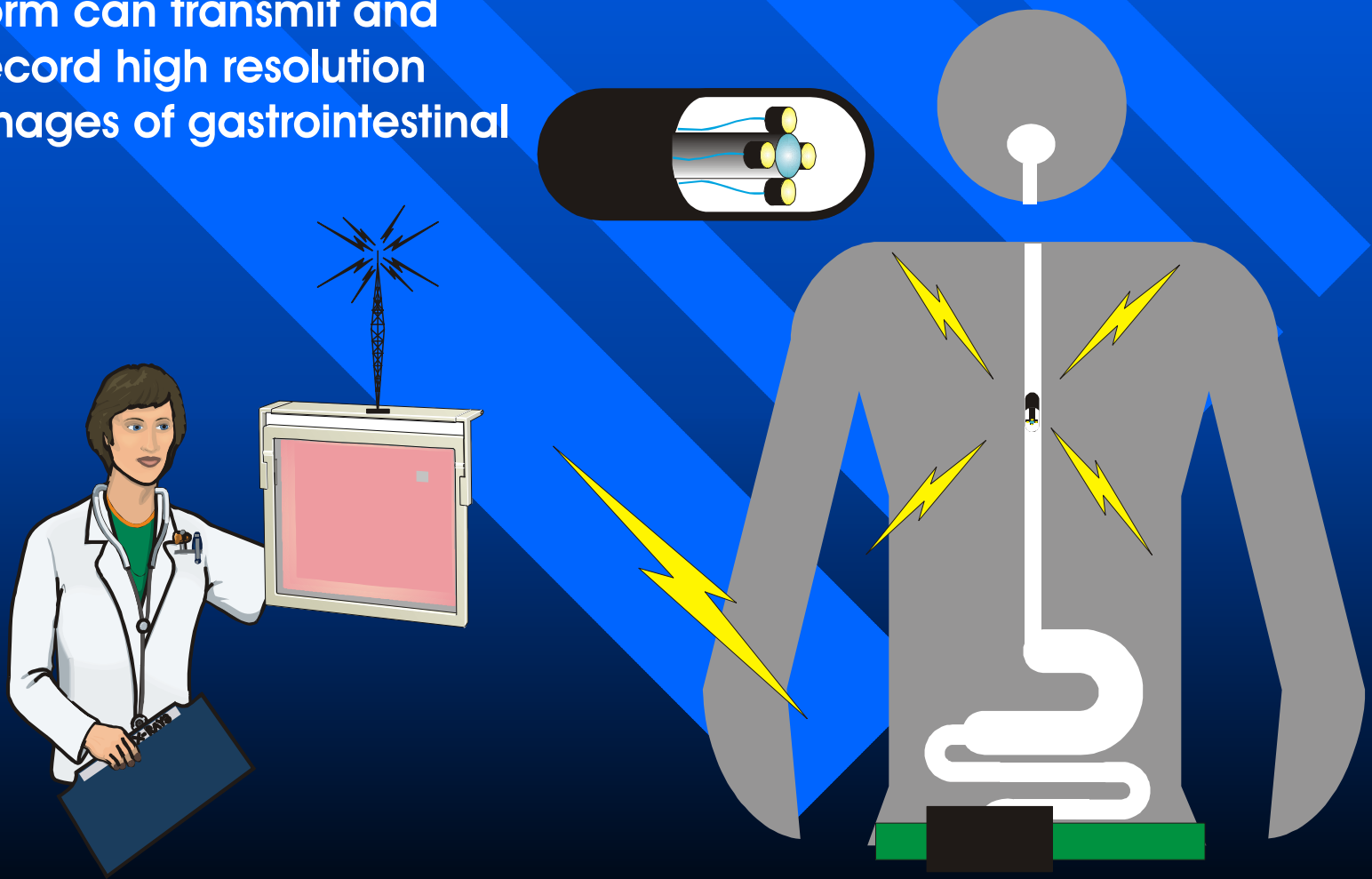




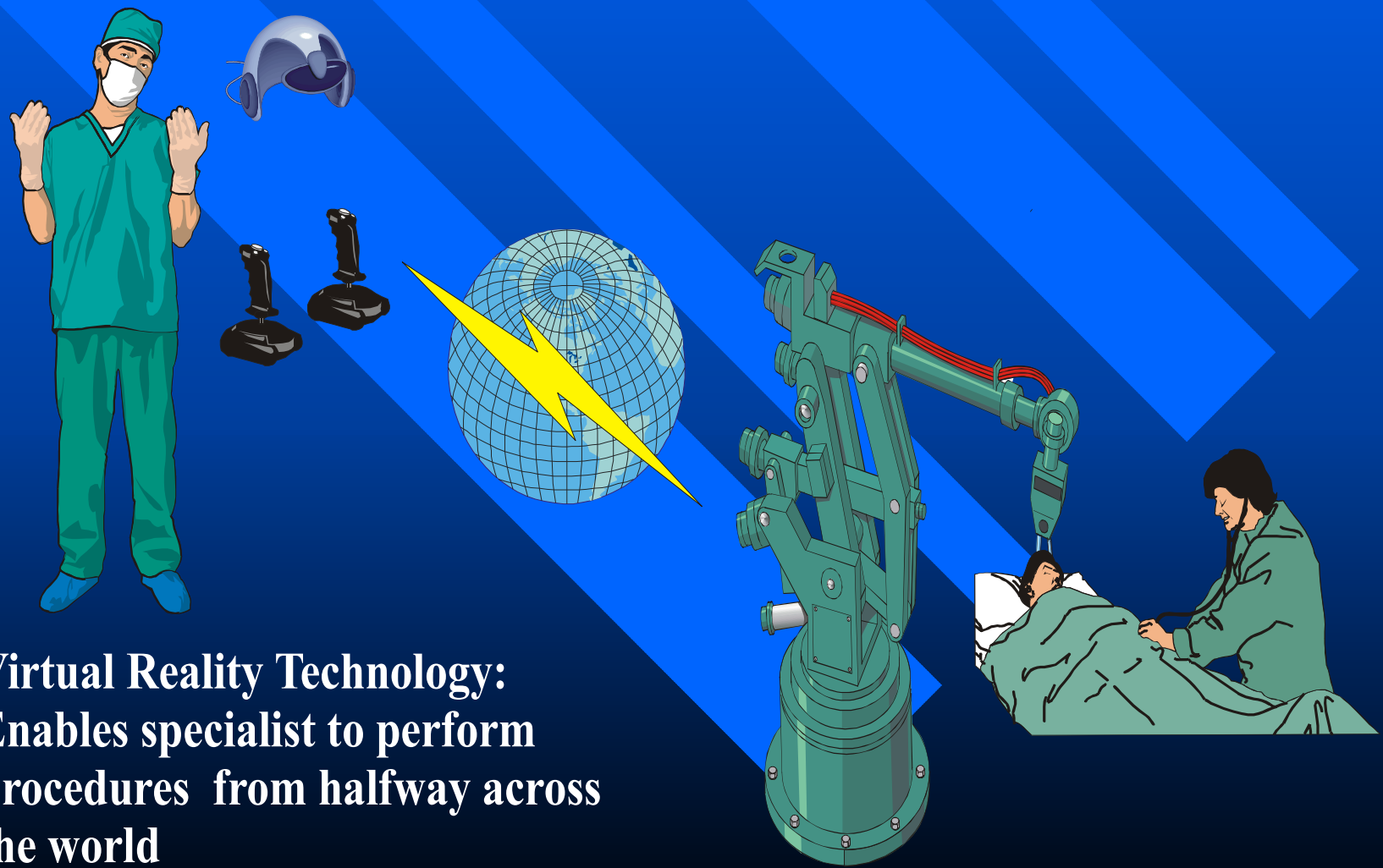
- Clothing with embedded sensors will enable medical personnel to monitor a wide range of physiologic conditions for patients who are known risks
- Problems can be detected and appropriate care initiated often before the patient is aware any problem exists

e-Health: Telemedicine Delivers Remote Diagnostics

Miniature cameras in pill form can transmit and record high resolution images of gastrointestinal



e-Health: Telemedicine Can Deliver Medical Expertise to Remote Locations



Virtual Reality Technology: Enables specialist to perform procedures from halfway across the world

Questions?