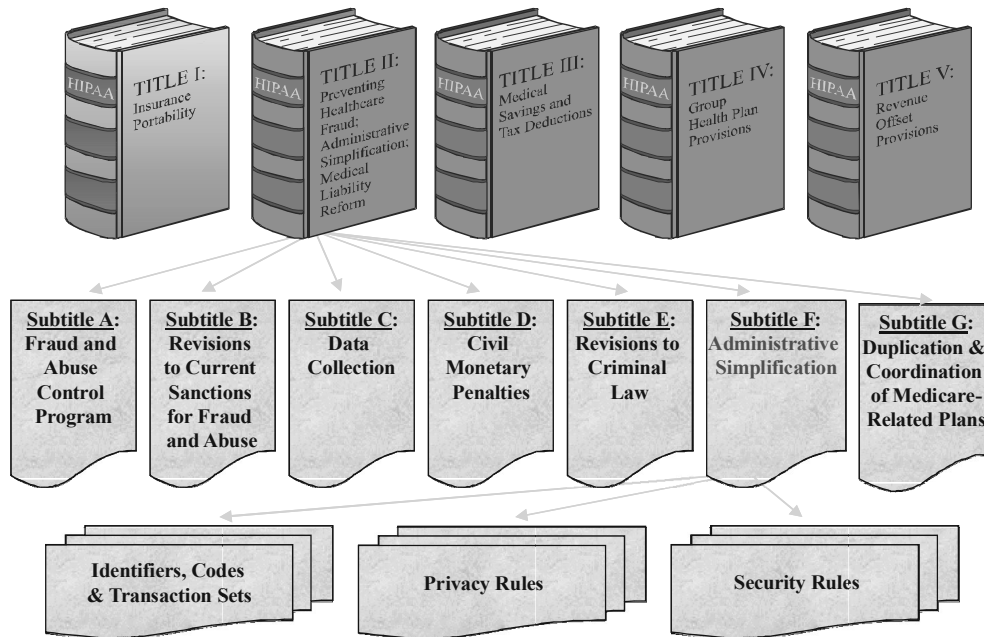


HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am



HIPAA Regulations

➤ Portion of HIPAA that most affects Healthcare Providers



➤ HIPAA Identifier, 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 and faxing
- Goal is to improve efficiency & substantially reduce administrative costs in healthcare industry

➤ Privacy Rules

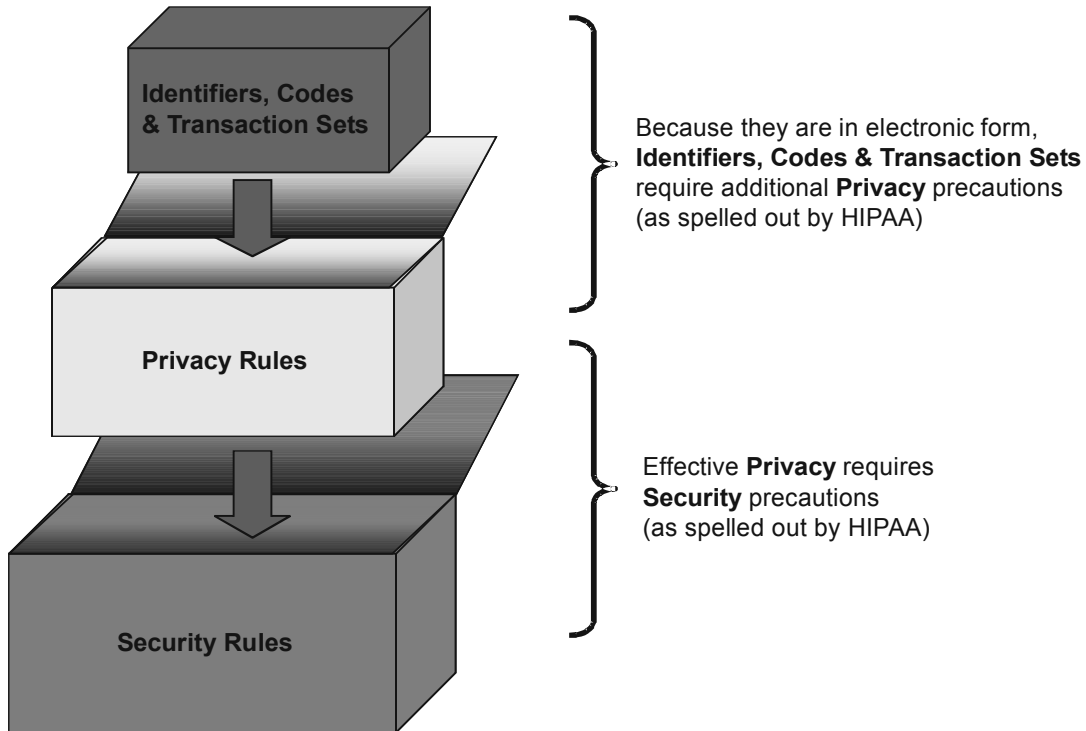
- Scheduled effective date: April 2003
- Rules deemed necessary to protect data in electronic transactions ... but whose scope encompasses all protected health information (oral, written, or electronic)
- Rules limit use of protected health information
 - Patient's authorization required before protected 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 Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

➤ **Security Rules**

- Scheduled 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

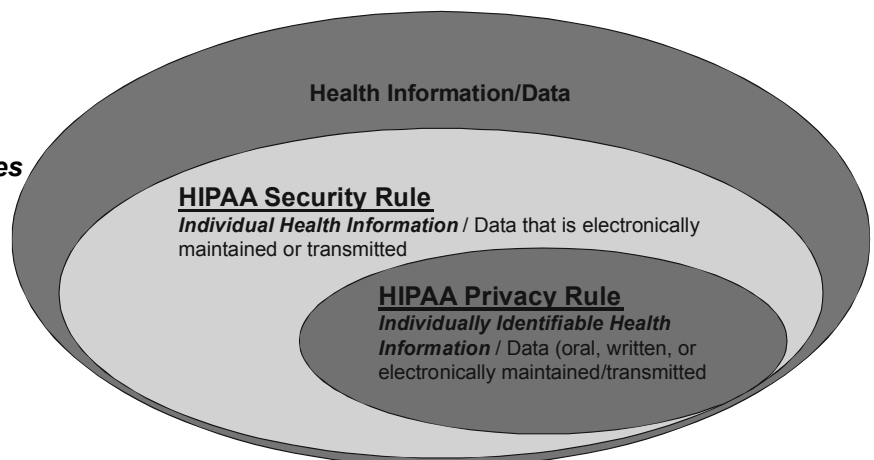
➤ **Effective Implementation depends on “packaging” HIPAA Rules**



HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

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, health plan, employer, or health care clearinghouse; and
 2. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of care to an individual, or the past, present, or future payment for the provision of health care to an individual, and
 - a. Which identifies the individual, or
 - b. With respect to which there is a reasonable basis to believe that the information can be used to identify the individual
- **Info/Data addressed by Privacy Rule**
Individually Identifiable Health Information (IIHI) or *Protected Health Information* (PHI) ~ any health information/data that is created or received by the healthcare provider, relates to the health, condition or provision of care and that includes:
 - 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**, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
 2. **Relates to past, present or future physical or mental health or condition of an individual**, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual
- **Data addressed by Security Rule**
Health Information related to an Individual ~ any health info/data that is created or received by the healthcare provider and that relates to the health, condition or provision of care of an individual ... but does not necessarily identify a patient. Includes, but not necessarily limited to:
 - Diagnostic data
 - Therapeutic data
 - Medical records
 - Billing info
- **Relationship between Info/Data addressed by Privacy & Security Rules**



HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

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 (at administrative level)
- Policy committee (broad departmental participation)
- Policies established regarding privacy
- Procedures created to insure adherence to privacy policies
- Staff education to insure their understanding of privacy issues and the organization's policies & procedures
- Contracts with Business Associates to insure their adherence to the organization's policies/procedures
- Audit & review to insure effectiveness of privacy compliance

➤ **Compliance with HIPAA's Security Rule**

Typically 75% of HIPAA Privacy compliance is organizational, operational, cultural (i.e., the organization's policies, procedures and the staff's adherence to those policies & procedures). The remaining 25% is "technical". Key elements include:

- Security officer (at administrative level)
- Security committee (with broad departmental participation)
- Policies established regarding security, and
Procedures created to insure adherence to those security policies
- Staff education to insure their understanding of security issues, the organization's policies & procedures, and (where appropriate) use of security technology
- Inventory of devices/systems capable of maintaining or transmitting health information (to assess risks associated with compromised *confidentiality*, *integrity* or *availability* of data)
- Physical safeguards to protect hardware storing or transmitting data
- Technical security services to protect, control & monitor data access
- Technical security mechanisms to prevent unauthorized access over network
- Contacts with *Business Associates* to insure their adherence to the organization's policies & procedures and employs physical safeguards technical security services & mechanisms
- Audit & review to insure effectiveness of all elements in security compliance

HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

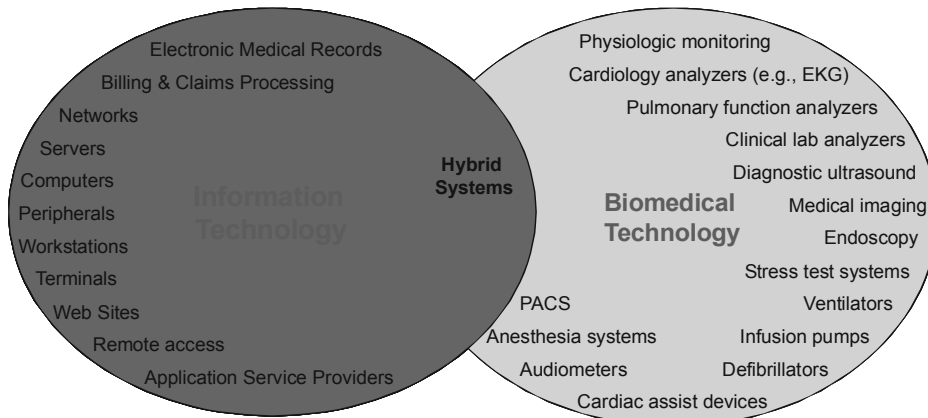
HIPAA Security Rule's Impact on Biomedical Technology

➤ Scope of HIPAA Security Provisions

The scope of HIPAA's Security Standards can be illustrated by reviewing the applicability and specific requirements of those standards:

- **Applicability**
Security provisions of HIPAA apply to any health plan, any health care clearinghouse, and 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 the requirements that a health care entity must address in order to safeguard the ***integrity, confidentiality, and availability*** of its electronic data. The standard also describes the implementation features that must be present in order to satisfy each requirement

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



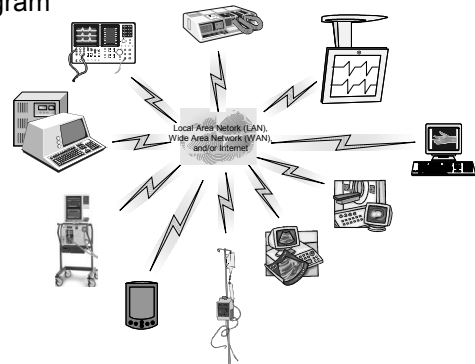
➤ Relevance to Biomedical Technology

The biomedical devices & systems used by healthcare providers represent a substantial and growing area of risk with respect to HIPAA security issues. The basis of this growing security risk lies principally in the following 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 ... also*
- *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 now represent a substantial repository of ***health information*** and therefore **must** be considered when implementing any comprehensive security program

➤ Medical Devices & Systems: Typical Data Interconnects

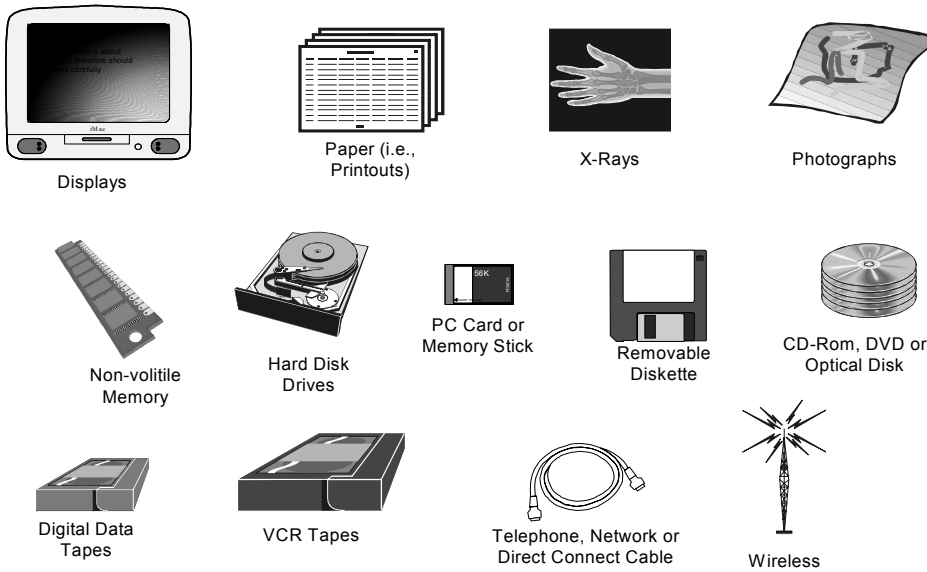


HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

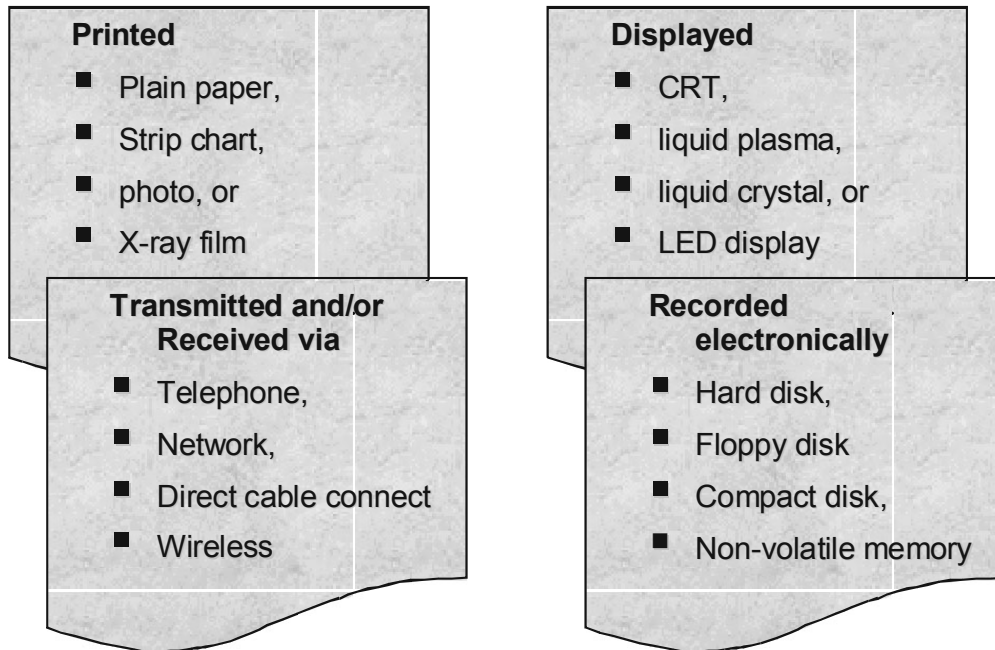
- **Biomedical Technology: Preparatory Steps for HIPAA Security Compliance**
 1. Acquire working knowledge of relevant HIPAA rules
 2. Inventory devices & systems
 3. Identify devices & systems with health data
 4. Assess risk associated data compromise for devices & systems containing health data
 5. 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)

HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

➤ **Step 3: Identify Devices & Systems Containing Health Information**

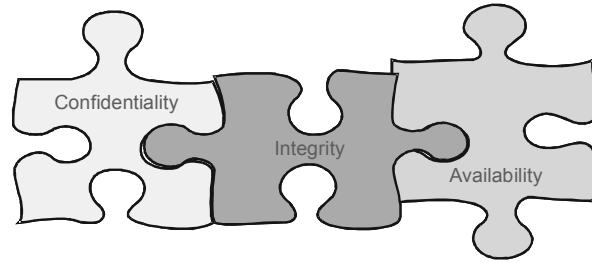


Health Information is at risk where it is:



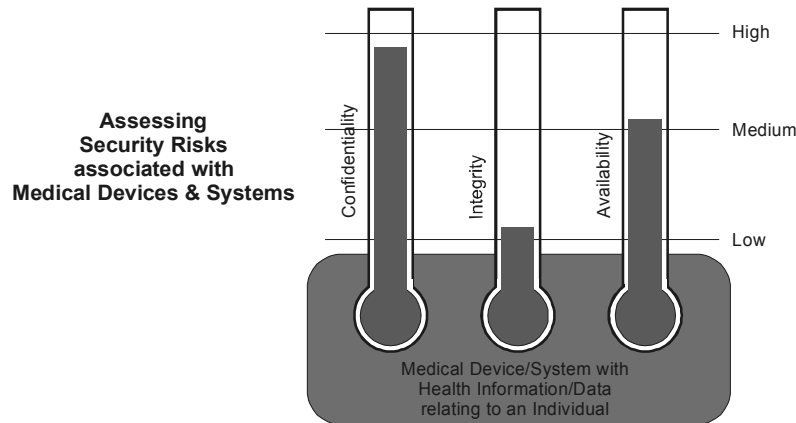
HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

➤ **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



RISK LEVEL	Impact on Patient		Impact on Organization			
	<i>Potential degree to which health care would be adversely impacted by compromise of availability or integrity of information</i>	<i>Potential degree to which privacy would be adversely impacted by compromise of confidentiality of information</i>	<i>Potential degree to which interests would be adversely impacted by compromise of confidentiality, availability or integrity of information</i>	<i>Potential financial impact</i>	<i>Potential legal penalties</i>	<i>Likely corrective measures required</i>
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	Administrative

HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

➤ **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)?
- (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:
 - ✓ Shred paper, film, photo
 - ✓ Erase/overwrite disks, pc cards, memory stick
 - ✓ Deposit in locked "Destruction Bin" for disposal by a bonded service
- (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)?
- (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?
 - ✓ Does the system security restrict remote access to specific devices or locations?
 - ✓ Does the system log and provide audit trail of remote access activity?
- (e) **All** Affected Devices & Systems
 - Is the device/system physically secure?
 - ✓ Is the system kept in secure area, inaccessible except to authorized users?
 - ✓ 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?
 - ✓ Does the system run virus protection?
 - ✓ 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**

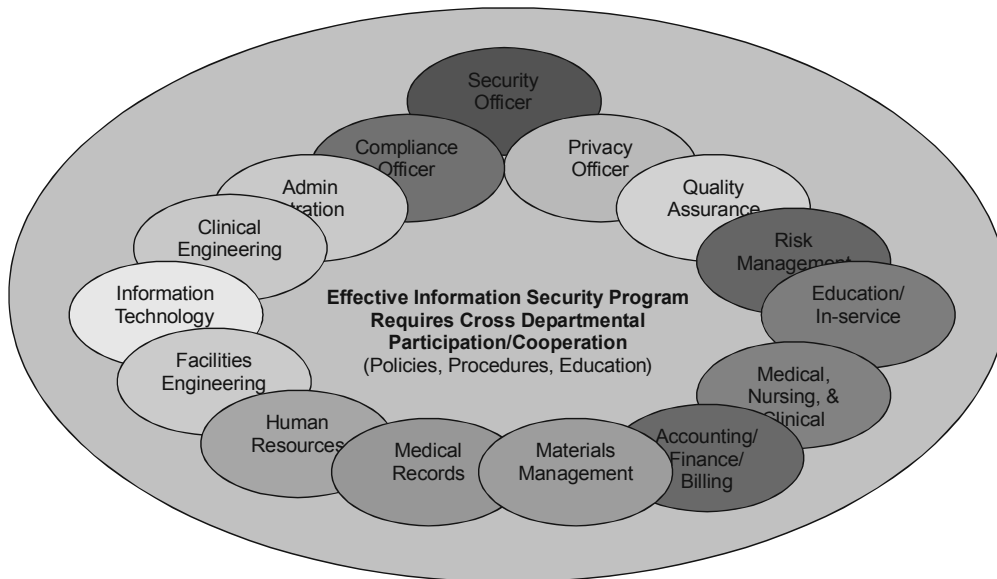
- "Gap" is difference between
 - Current security program (from inventory, risk assessment & determination of current security precautions) and
 - Security program mandated by HIPAA
- Gap analysis (and subsequent audits) security program effectiveness in terms of:
 - Policies
 - Procedures
 - Implementation
 - Testing
 - Integration
- Gap analysis is used to prepare plan for achieving HIPAA compliance and implementation priorities:

HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

➤ **Biomedical Technology: Steps for achieving HIPAA Compliance**

1. Assign roles & responsibilities ~ involve all affected departments
2. Treat Security Risks (HIPAA Security Matrix)
 - Administrative procedures
 - Physical safeguards
 - Technical security services
 - 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**



➤ **Step 2: Treat Security Risks**

HIPAA's Four Categories of Security Requirements			
Administrative procedures Documented, formal practices to manage the <ul style="list-style-type: none"> ✓ Selection and execution of security measures to protect data and ✓ Conduct of personnel in relation to the protection of data 	Physical safeguards ~ Protection of physical computers systems (<i>any hardware storing or transmitting health data</i>) and related buildings & equipment from <ul style="list-style-type: none"> ✓ Natural & environmental hazards (e.g., fire, flood) ✓ Intrusion (i.e., use of locks, keys and administrative measures to control access) 	Technical security services ~ Processes that are put in place to <ul style="list-style-type: none"> ✓ Protect information access ✓ Control & monitor information access 	Technical security mechanisms Processes put in place to prevent unauthorized access to data that is transmitted over a communications network

HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

➤ **Step 3: Educate Staff**

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

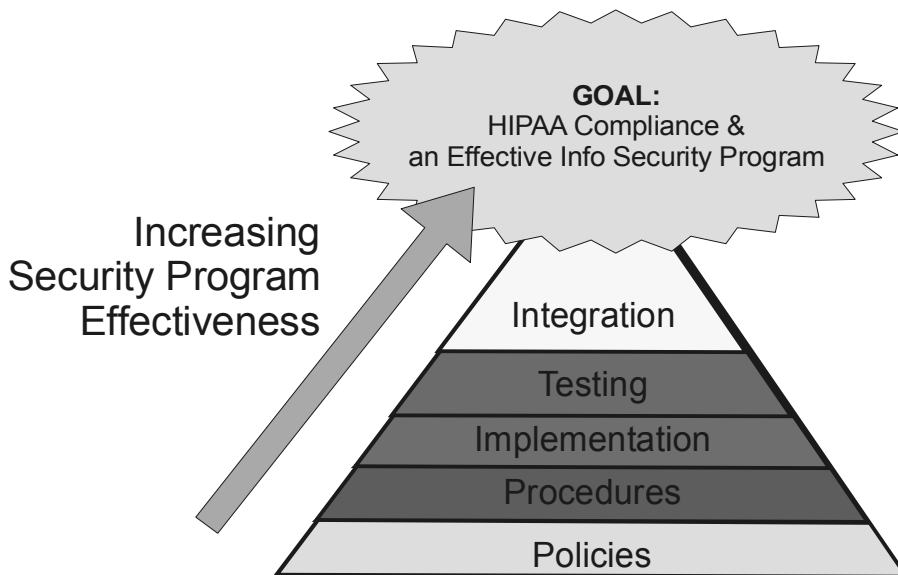
- Privacy & Security concerns
- Organization's Privacy policies & procedures
- Organization's
 - Security Policies,
 - Security Procedures
 - Technical security services
 - Technical security mechanisms

➤ **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 to those permitted by contract
 - Destroy or return any health data to the organization when permitted activity is complete or relationship ceases
 - Maintain safeguards to protect health data and agrees to security, inspection & reporting requirements necessitated by organization's security program
 - Report to organization the use or disclosure of any health data by BA that was not otherwise addressed by contract

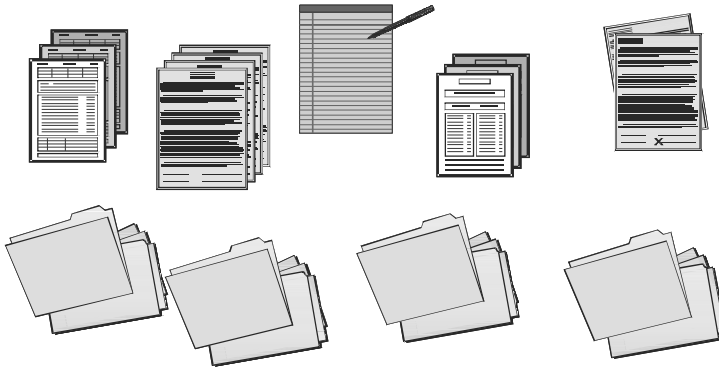
➤ **Step 5: Establish on-going audit & review process**

- 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

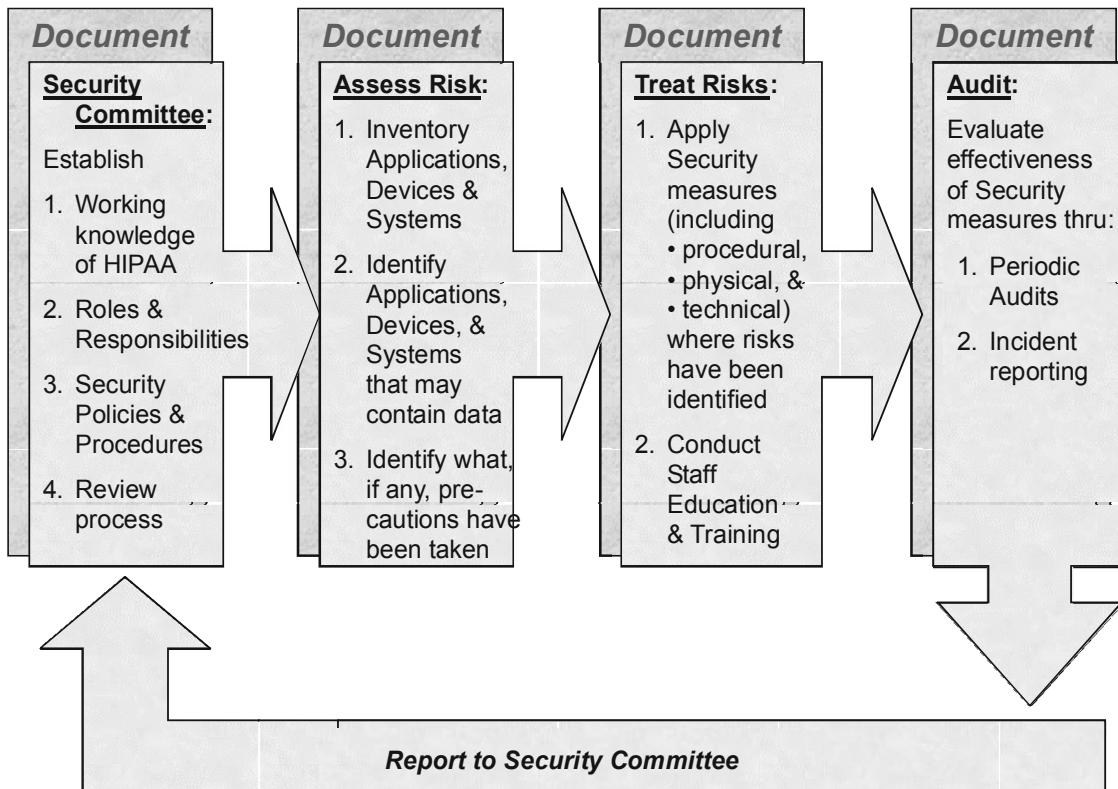


HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

➤ **Step 6: Document, Document, Document**



➤ **HIPAA Security Risk Assessment**



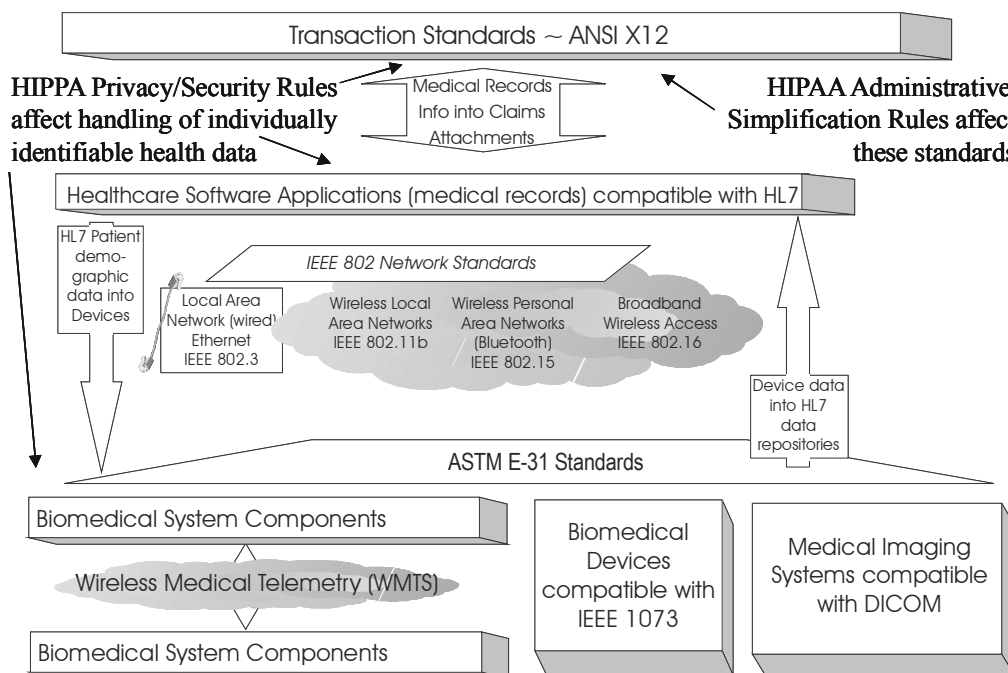
HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

Technology Standards for Medical Device/System Manufacturers

➤ **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
- **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 ~ WPAN (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

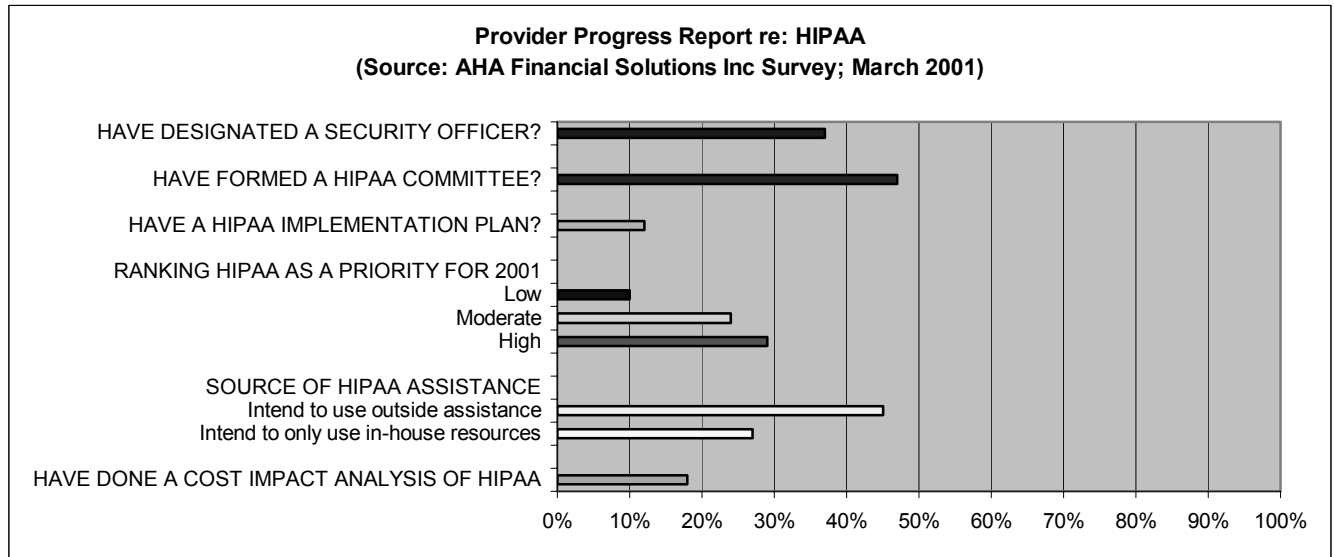
Relationship Between Standards



HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

Other HIPAA Issues

➤ **Provider Progress Report**



➤ **HIPAA Strategy for Providers**

- Don't wait for final HIPAA disposition. Formal, comprehensive information security program for every healthcare provider is inevitable
- "Writing is on the wall" ... changes will come whether decreed by regulation (i.e., HIPAA) or market forces
- Choice is to embrace security, take lead ... or delay and face a Herculean project only months or a year down the line
- Experience with Y2K shows delay only results in:
 - Outlay of more effort (i.e., delay = inefficiency)
 - A compressed timeline to adopt necessary compliance efforts
 - Significantly larger expenditures (resources will be scarce and those that are available will come at a higher premium as compliance "deadline" approaches)
- Delaying implementation of security
 - Postpones (i.e., loses) savings gained by efficiencies inherent in HIPAA mandated security processes ..
 - Results in competitive disadvantage ...
 - ✓ Healthcare providers must, as other industries have, consider e-commerce (and e-health) in their business plans in order to stay current and remain competitive.
 - ✓ A comprehensive information security program like that required by HIPAA 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 or "end date"
 - ✓ Compliance required was technology-based solutions
 - ✓ 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 "end-date")
 - ✓ Compliance involves organizational & procedural changes as well as some technology changes ... no such thing as "HIPAA-compliant" technology ... only "HIPAA-friendly"
 - ✓ Like Y2K, also requires coordinated effort across functional and organizational lines

HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

- **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” that are implemented thru organizational & technical procedures designed to support those specific Policies

- **HIPAA’s Impact ~ Broad & Substantial**

HIPAA will lead to tangible and intangible benefits by:

 - Standardizing EDI format ~
Reduce complexity associated with multiple standards, data 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 (*projected at \$240 billion annually*) ~ a flood of new e-health applications will be considered that would have been impossible to implement without standardized, secure & private data systems

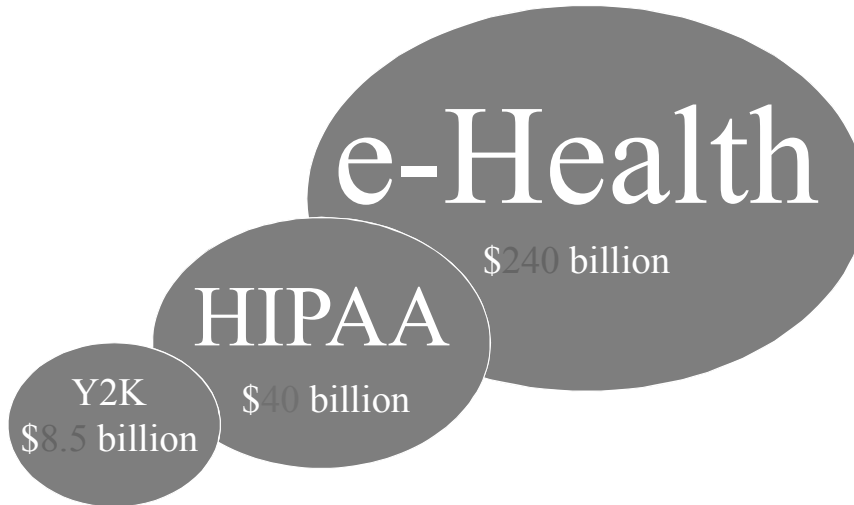
- **HIPAA will enable the Future of Healthcare:**

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 diagnostic & 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!



- **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/optho scopes

HIPAA Summit West ~ San Francisco, CA
HIPAA Security: Impact on Biomedical Device & Systems ~ by S. L. Grimes, TiM
Friday, June 22, 2001 @ 10:45am

➤ **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)

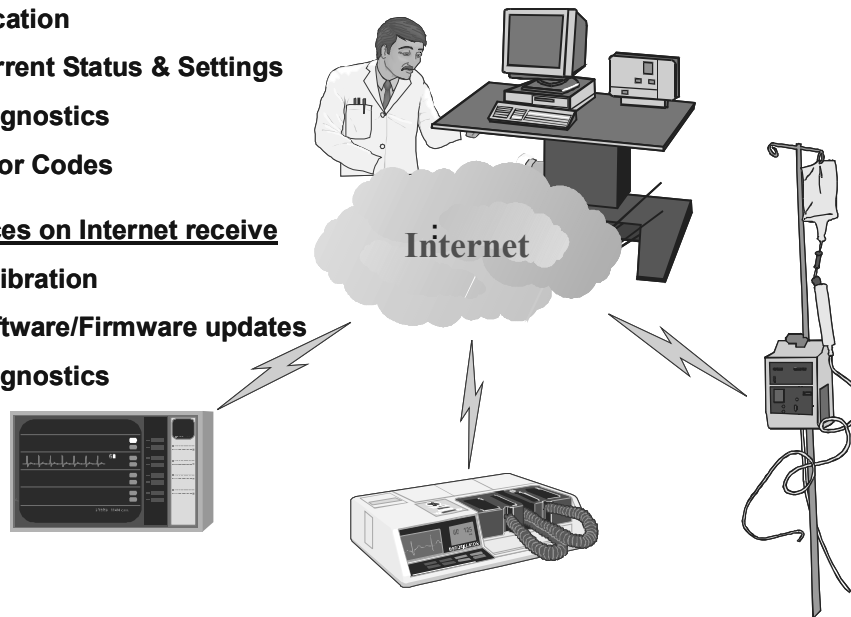
**Equipment Management with
Internet-connected Medical Devices**

Devices on Internet transmit:


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

Devices on Internet receive

- **Calibration**
- **Software/Firmware updates**
- **Diagnostics**

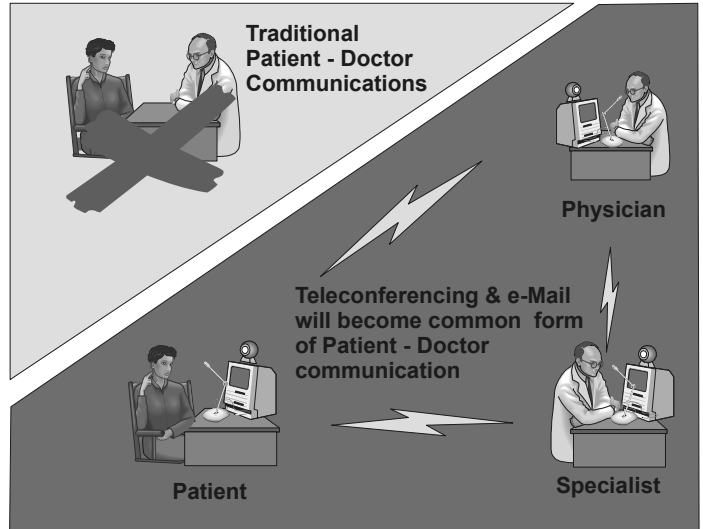


Implications for Future of Healthcare Technology & e-Health



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

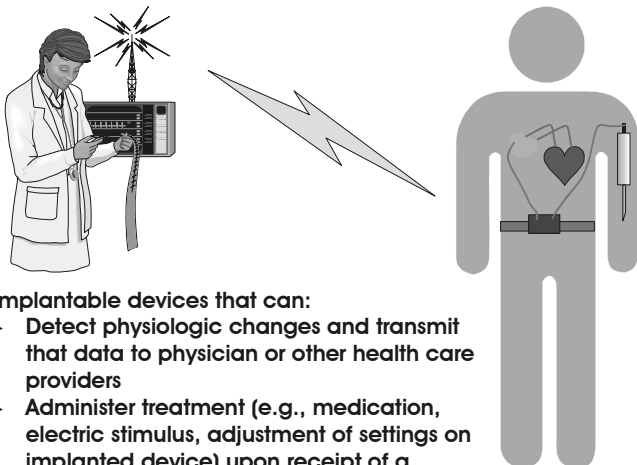
- Send/receive e-mail with patients and other members of healthcare team
- Obtaining patient status reports, test results
- Issuing prescriptions (less error prone) & orders



Traditional Patient - Doctor Communications

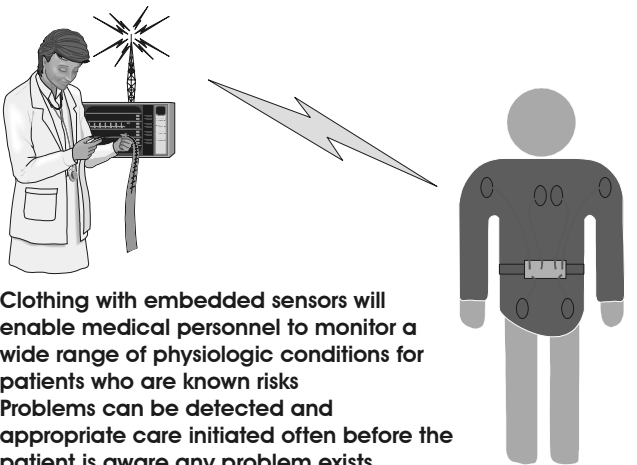
Teleconferencing & e-Mail will become common form of Patient - Doctor communication

Labels: Patient, Physician, Specialist



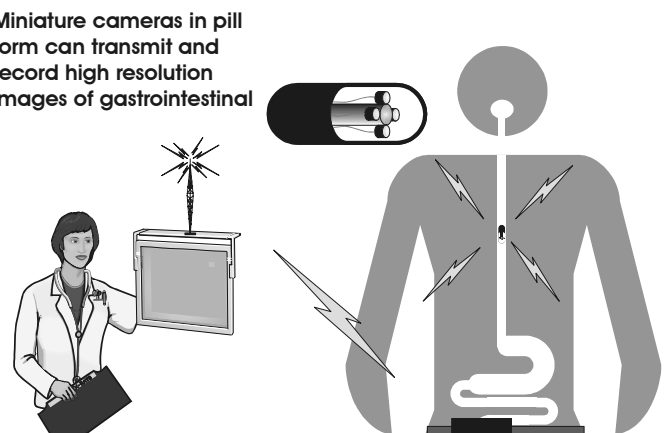
Implantable devices that can:

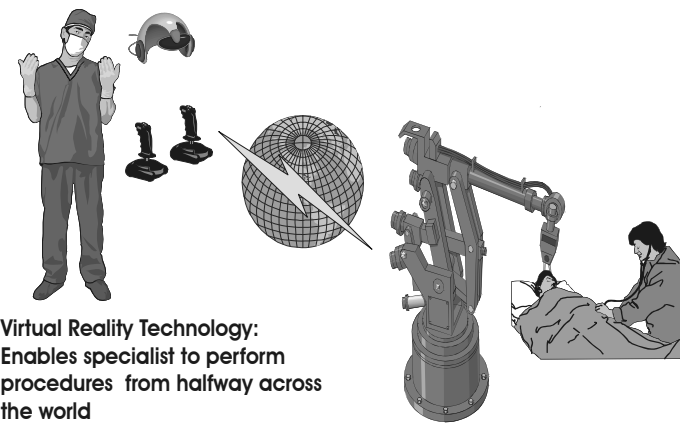
- ▶ Detect physiologic changes and transmit that data to physician or other health care providers
- ▶ Administer treatment (e.g., medication, electric stimulus, adjustment of settings on implanted device) upon receipt of a signal from a remote healthcare provider



- 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

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





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

HIPAA Summit West – June 22, 2001
HIPAA Security: Impact on Biomedical Technology, Devices & Systems
HIPAA Security Matrix

1. Administrative Procedures

These elements include documented, formal practices to:

- Manage the selection and execution of security measures
- Protect data
- Define conduct of personnel in relation to the protection of data

The *Administrative Procedures* required elements include:

Security Elements	Implementation features
a. Certification	
b. Chain of trust partner agreement	
c. Contingency plan	All of the following are <i>required</i> : (1) Applications & data criticality analysis (2) Data backup plan (3) Disaster recovery plan (4) Emergency mode plan (5) Testing and revision
d. Formal mechanism for processing records	
e. Information access control	All of the following are <i>required</i> : (1) Access authorization (2) Access establishment (3) Access modification
f. Internal Audit	
g. Personnel security	All of the following are <i>required</i> : (1) Assure supervision of maintenance personnel by authorized, knowledgeable person (2) Maintenance of record of access authorizations (3) Operating, and in some cases, maintenance personnel have proper access authorization (4) Personnel clearance procedure (5) Personnel security policy/procedure (6) System users, including maintenance personnel, trained in security
h. Security configuration management	All of the following are <i>required</i> : (1) Documentation (2) Hardware/software installation & maintenance review and testing for security features (3) Inventory (4) Security testing (5) Virus checking
i. Security incident procedures	All of the following are <i>required</i> : (1) Report procedures (2) Response procedures
j. Security management process	All of the following are <i>required</i> : (1) Risk analysis (2) Risk management (3) Sanction policy (4) Security policy
k. Termination procedures	All of the following are <i>required</i> : (1) Combination locks changed (2) Removal from access lists (3) Removal of user accounts(s) (4) Turn in keys, token or cards that allow access
l. Training	All of the following are <i>required</i> : (1) Awareness training for all personnel (including management) (2) Periodic security reminders (3) User education concerning virus protection (4) User education in importance of monitoring log in success/failure, and how to report discrepancies (5) User education in password management

HIPAA Summit West – June 22, 2001
HIPAA Security: Impact on Biomedical Technology, Devices & Systems
HIPAA Security Matrix

2. Physical Safeguards

These elements relate to the protection of physical devices and systems (and supporting equipment & buildings) from:

- Natural & environmental hazards (i.e., fire, floods, storms)
- Intrusion

The *Physical Safeguards* required elements include:

Security Elements	Implementation features
a. Assigned security responsibility	
b. Media controls	All of the following are <i>required</i> : (1) Access control (2) Accountability (tracking mechanism) (3) Data backup (4) Data storage (5) Disposal
c. Physical access controls (limited access) (all listed implementation features must be implemented)	All of the following are <i>required</i> : (1) Disaster recovery (2) Emergency mode operation (3) Equipment control (into and out of site) (4) Facility security plan (5) Procedures for verifying access authorizations prior to physical access (6) Maintenance records (7) Need-to-know procedures for personal access (8) Sign-in for visitors and escort, if appropriate (9) Testing and revision
d. Policy/guideline on work station use	
e. Secure work station location	
f. Security awareness training	

3. Technical Security Services

These elements include processes that are put in place to

- Protect information access and
- Control & Monitor information access

The *Technical Security Services* required elements include:

Security Elements	Implementation features
a. Access control	(1) Encryption (<i>optional</i>) (2) Procedure for emergency access (<i>required</i>) <i>One of the following 3 is required</i> (3) Context based access (4) Role-based access (5) User-based access
b. Audit controls	
c. Authorization control	<i>One of the following 2 is required</i> (1) Role-based access (2) User-based access
d. Data Authentication	
e. Entity authentication	<i>One of the following 5 is required</i> (1) Biometric (2) Password (3) PIN (4) Telephone callback (5) Token <i>Both of the following are required:</i> (6) Automatic logoff (7) Unique user identification

HIPAA Summit West – June 22, 2001
HIPAA Security: Impact on Biomedical Technology, Devices & Systems
HIPAA Security Matrix

4. Technical Security Mechanisms

This element includes processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network

The *Technical Security Mechanisms* required elements include:

Security Elements	Implementation features
a. Communication/network controls	<p>If using a network, the <i>following</i> are required</p> <ul style="list-style-type: none"> (1) Alarm (2) Audit trail (3) Entity authentication (4) Event reporting <p>Following are required if <i>communications</i> or networking employed</p> <ul style="list-style-type: none"> (5) Integrity controls (6) Message authentication <p>One of following 2 required if <i>communications</i> or networking employed</p> <ul style="list-style-type: none"> (7) Access controls (8) Encryption

In addition to the above four categories, HIPAA also requires adoption of the following security element whenever electronic signature is employed.

5. Electronic Signature

This element includes processes that must be used whenever a HIPAA specified transaction requires the use of an electronic signature

Security Elements	Implementation features
a. Digital signature	<p>If digital signature is employed, the following 3 are required</p> <ul style="list-style-type: none"> (1) Message integrity (2) Nonrepudiation (3) User authentication <p>The following are optional</p> <ul style="list-style-type: none"> (4) Ability to add attributes (5) Continuity of signature capability (6) Countersignatures (7) Independent verifiability (8) Interoperability (9) Multiple signatures (10) Transportability