

NATIONAL MINORITY AIDS EDUCATION & TRAINING CENTER

HIPAA SECURITY REQUIREMENTS TRAINING FOR CLINICAL DATA ENVIRONMENTS



NMAETC
National Minority AIDS
Education and Training Center

HIPAA SECURITY

DEFINITION/STANDARDS

FINAL RULE COMPLIANCE:

DATA INTEGRITY

DATA CONFIDENTIALITY

DATA AVAILABILITY

HIPAA SECURITY

IT SECURITY INITIATIVE DRIVERS & STANDARDS

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Federal Information Security Management Act (FISMA)

OMB Circular A-130, Management of Information Resources

Government Information Security Reform Act (GIRSA)

HIPAA SECURITY

IT SECURITY INITIATIVE DRIVERS & STANDARDS

**Information technology Management Reform Act of 1996
(Clinger-Cohen ACT)**

**National Institutes of Standards & Technology (NIST)
Special Publications (SP)**

**Federal Information Processing Standards (FIPS) 199
Standards for Security Categorization of Federal
Information and Information Systems**

HIPAA SECURITY

HIPAA COMPLIANCE DATES

April 14, 2003 Privacy

- all covered entities except small health plans

October 16, 2002 Health Care Transactions and Code Sets

- all covered entities except those who filed for an extension and are not a small health plan

October 16, 2003 Electronic Health Care Transactions and Code Sets

- all covered entities who filed for an extension and small health plans

HIPAA SECURITY

HIPAA COMPLIANCE DATES

April 14, 2004 Privacy- all small health plans

April 20, 2005 Security Standards

– all covered entities except small health plans

April 20, 2006 Security Standards

- all small health plans

HIPAA SECURITY

HIPAA SECURITY DEFINITIONS - PRIVACY vs. SECURITY

HIPAA Privacy –

Requirements that outline the methods to protect individual identifiable health data, referred to as Protected Health Information (PHI)

PHI is transmitted or maintained in any form or medium (e.g., electronic, paper, or oral) but excludes certain educational records and employee records

HIPAA SECURITY

HIPAA SECURITY DEFINITION- PRIVACY vs. SECURITY

HIPAA Privacy –

The Privacy Rule expressly permits disclosures with individual authorization by law to collect or receive the information for the purpose of preventing or controlling disease, injury or disability, including but not limited to public health surveillance, investigation and intervention

HIPAA SECURITY

HIPAA Security Definition- PRIVACY vs. SECURITY

HIPAA Security (Section 164.306) –

Defines the minimum requirements to ensure confidentiality, security and integrity of electronically stored and transmitted patient health information ePHI

Defines measures that help protect individual's health information, while permitting the appropriate access and use of that information, which ultimately promotes the use of electronic health information in the industry

HIPAA SECURITY

HIPAA Security Definition- PRIVACY vs. SECURITY

HIPAA SECURITY (Section 164.306)

ePHI is defined as patient health information that is strictly in “electronic media”, which is in turn defined as:

Electronic Storage – computer hard drives, any removable digital memory

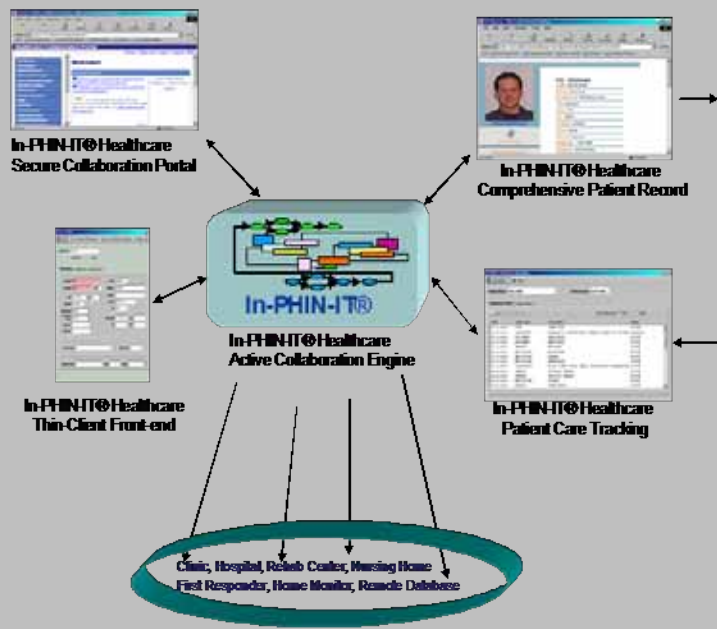
Information Exchange Transmission Media – Internet, extranet, leased lines, dialup lines and private networks

HIPAA SECURITY

EHR standard compatible patient health information systems

Saving Lives Through Collaboration!

In-PHIN-IT® Description and Advantages



Real time information capture, including phonetically searched voice objects, at the point of care. This includes access to information residing on existing computer systems and real time access to Food and Drug Administration (FDA) and Center for Disease Control (CDC) web sites for adverse drug interactions

AI workflow module to capture physician chromadose orders, a time sequence of procedures, and the measurement of the "quality of care" using a six sigma methodology, i.e., a process to reduce errors to 3.4 parts per million (3.4 errors per million events)

Automatic report generation and document management needed to meet Joint Commission on Accreditation of Healthcare Organizations (JCAHO) or Centers for Medicare and Medicaid Services (CMS) requirements

Low cost collaborative ASP work space and the introduction of best practices based on our transformation methodology that includes distance learning for training-the-trainer or direct interactive user training

HIPAA SECURITY

HIPAA DEFINITION- PRIVACY vs. SECURITY

HIPAA SECURITY (Section 164.306) –

Electronic Health Record (EHR) standards are being driven by HHS Office of the National Coordinator for Health Information Technology (ONCHIT)

Implementation will depend on clinics adopting sound HIPAA Security standards as they implement EHR standard compatible patient health information systems

HIPAA SECURITY

HIPAA Security Definition- Privacy vs. Security

In summary...

Privacy Rule

- Covers PHI in all forms
- Focuses on confidentiality
- Defines what should be protected
- Office of Civil Rights (OCR) oversees and enforces this regulation

Security Rule

- Covers PHI in electronic form only
- Focuses on confidentiality, integrity, and availability
- Defines how to protect it
- Center of Medicare and Medicaid (CMS) will oversee and enforce this regulation

HIPAA SECURITY

HIPAA Security - Final Rule Compliance

Covered Entities Must –

Ensure the confidentiality, integrity and availability of all ePHI the covered entity creates, receives, maintains or transmits

Protect against any reasonably anticipated threats or hazards to the security or integrity of such information

Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Final Security Rule

Ensure compliance by the workforce

HIPAA SECURITY

HIPAA SECURITY GENERAL CONCEPTS

Confidentiality- “Data or information which is not made available or disclosed to unauthorized persons or processes”

Integrity- “Data that has not been altered or destroyed in an unauthorized manner”

Authenticity: Third party can verify content has not been changed in transit

Non-repudiation: Origin or receipt of a specific message that is verifiable by a third party



HIPAA SECURITY

HIPAA SECURITY GENERAL CONCEPTS

Availability- “Data is in the place needed by the user, at the time the user needs them, and in the form needed

HIPAA SECURITY

HIPAA SECURITY - Final Rule Standards

- **Administrative Safeguards**
- **Physical Safeguards**
- **Technical Safeguards**

HIPAA SECURITY

HIPAA SECURITY - Final Rule Standards

Administrative Safeguards

Actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect ePHI

HIPAA SECURITY

HIPAA SECURITY

Final Rule Standards

Physical Safeguards

Each covered entity is required to address the following physical safeguard standards that concern the physical protection of data systems and data from intrusion and from environmental or natural hazards.

The physical safeguard standards are:

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

HIPAA SECURITY

HIPAA SECURITY -

- Final Rule Standards

Technical Safeguards

The technical safeguard standards address the technology and the policies and procedures for its use that protect ePHI and control access to it.

The technical safeguard standards are:

Access Controls

Audit Controls

Integrity

Person or Entity Authentication

Transmission Security

HIPAA SECURITY

HIPAA SECURITY -

■ Sanctions for Noncompliance

- **Violations of the Final Security Rule can result in:**
 - Penalties of up to \$100.00/person/violation
 - Penalties of up to \$25,000 for violation of a single standard during a calendar year
 - Penalties for knowing violations of up to \$50,000 and one year in prison

HIPAA SECURITY

HIPAA SECURITY -

■ Sanctions for Non compliance

- **Violations of the Final Security Rule can result in:**
 - **Penalties for knowing violations under false pretenses up to \$100,000 and up to five years in prison**
 - **Penalties for knowing violations with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm up to \$250,000 and 10 years in prison**

HIPAA SECURITY

HIPAA SECURITY -

- Sanctions for Noncompliance

- **Use of “De-identified” Information**

- **De-identified information is data that has identifiable health information stripped off which could identify individual subjects**
- **De-identified information is NOT covered under the Security Rule as it is no longer classified as ePHI**

HIPAA SECURITY

HIPAA SECURITY ePHI PROTECTION AWARENESS

- **What we will cover:**
 - **FMCS IT Security and Use of Technology Policy**
 - **HIPAA Security Risk Assessment**
 - **HIPAA Security Risk Management**
 - **FMCS Logins and Passwords**

HIPAA SECURITY

HIPAA Security ePHI Protection Training

- **Why are we concerned:**
 - **Jacksonville, Florida**

A woman brought her teenage daughter to work at a hospital, and left her unattended at a logged in computer. The girl looked up patient phone numbers and phoned to tell them that they'd tested positive for HIV. One patient attempted suicide.

HIPAA SECURITY

HIPAA Security ePHI Protection Training

- **Why are we concerned:**

- **Rapid City, South Dakota**

A medical student took home copies of patients' psychiatric records to work on a research project. When finished, he disposed of the material in the dumpster of a fast food restaurant, where they were found and given to a newspaper reporter.

HIPAA SECURITY

HIPAA Security ePHI Protection Awareness

- **Why are we concerned:**

- **Missoula, Montana**

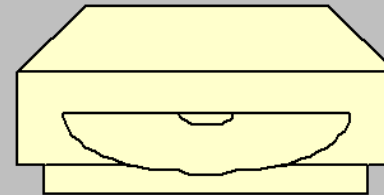
A hospital posted the psychiatric records of dozens of children on its public website, where they remained for weeks until discovered by a newspaper reporter.

HIPAA SECURITY

HIPAA Security ePHI Protection Awareness

IT Security & Use of Technology Policy

- ePHI data must be stored in computer based storage systems- ex. DVD, CD, tape, zip disk



HIPAA SECURITY

HIPAA Security ePHI Protection Training

IT Security & Use of Technology Policy

- **All removable electronic media must be secured from unauthorized access when out of the clinical record room and/or cabinet**
- **All computer systems and screens should be password protected**
- **All screens should be cleared before they are left unattended**



HIPAA SECURITY

HIPAA Security ePHI Protection Training

- **IT Security & Use of Technology Policy**
 - **Computer and client files should be positioned to prevent access by unauthorized persons**
 - **All diagnostic reports, such as laboratory and radiology reports, should be treated with the same degree of confidentiality as a full clinical record**
 - **Permission should be granted by a client to leave lab results on an answering device or with a family member-this must be clearly documented in the clinical record**

HIPAA SECURITY

HIPAA Security ePHI Protection Training

- **IT Security & Use of Technology Policy**
 - **FMCS adheres to Federal regulations, 42 CFR Part 2, that restricts disclosure of information or clinical records for clients receiving treatment for alcohol and other substance abuse**
 - **Clients must be advised of their rights under these regulations at the time of intake and prior to signing a Release form**
 - **When sending ePHI to another provider, FMCS staff must authenticate the end point to ensure that the entity receiving the client information has a legitimate email address and uses 128 bit encryption technology**

HIPAA SECURITY

IT Security & Use of Technology Policy

128 bit Encryption

Sophisticated scrambling method which prevents unauthorized eavesdropping on electronic data

Works by taking a piece of information and processing it with a mathematical formula (algorithm) that converts it into meaningless information.

HIPAA SECURITY

IT Security & Use of Technology Policy

- 128 bit Encryption
 - The statement, “This is a secret” when encrypted looks like, “as03xx1a79x!dqt”
 - These digital characters take different paths over internet and arrive at the destination where they are “decrypted”
 - Both ends must employ 128 bit encryption

HIPAA SECURITY

HIPAA Security ePHI Protection Awareness

- **The FMCS IT Security & Use of Technology Policy**

All client information will be retained for 6 years from the date of the last entry...or longer if required by state

HIPAA SECURITY

HIPAA Security ePHI Protection Awareness

- **The FMCS HIPAA Security Risk Analysis**
 - **Requirements:**
 - **Identify all electronic health data**
 - **Ensure that the analysis covers all health data areas**
 - **Define the system boundaries**
 - **Networked devices**
 - **Same management control**
 - **Same function or objective**
 - **Same characteristics and security needs**
 - **Same operating environment**

HIPAA SECURITY

HIPAA Security ePHI Protection Awareness

- **The FMCS HIPAA Security Risk Analysis**
 - **Determine most likely risks and vulnerable areas:**
 - Define the “System” – related assets
 - What are the threats to those assets
 - What are our vulnerabilities
 - What is the probability of a loss from a threat?
 - What is the cost of the loss?

HIPAA SECURITY

Family Medical & Counseling



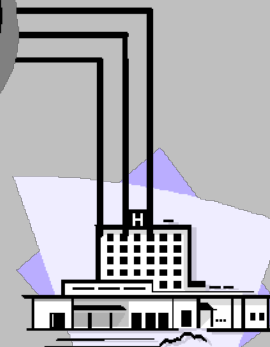
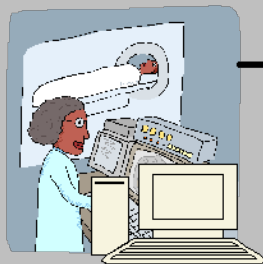
Transmission of ePHI



Internet Access

Internet

Internet Access



Children's Hospital

HIPAA SECURITY

HIPAA Security ePHI Protection Awareness

■ The FMCS HIPAA Security Risk Management

- **Protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification**
 - Reasonable and appropriate
 - Level or degree of risk may change over time

HIPAA SECURITY

HIPAA Security ePHI Protection Awareness

HIPAA Security Risk Management

- **Seven cents of every revenue dollar is at risk due to lack of information security**
- **Many clinics spend less than ten cents of each IT dollar on security**
- **Risk is significant: The average company had over 4,000 attacks over the last two years**

HIPAA SECURITY

HIPAA Security ePHI Protection Awareness

■ HIPAA Security Risk Management

- It is getting much worse: The average will soon be over 8,500 attacks
- 70% of networked computers are infected each year (viruses, spy ware, etc)
- More than half of the damage done is unintended employee action

HIPAA SECURITY

HIPAA SECURITY RISK MANAGEMENT

- **Computer data encryption – yes**
- **Strong Passwords - yes**
- **Firewalls - yes**
- **Data filters - yes**
- **Modem control - yes**
- **PBX devices (phone system) - yes**
- **Data backup and recovery - yes**
- **Diagnostic and testing - no**
- **Training - ongoing**

HIPAA SECURITY

HIPAA SECURITY RISK MANAGEMENT

When is Risk Acceptable

- Finding the “sweet spot”
 - Greatest protection per dollar
 - Meets the commonsense test
 - Countermeasures address more than one risk where possible
 - Remaining risk is “acceptable”
 - Further reduction would cost more than the benefits gained



HIPAA SECURITY

In summation:

Risk Analysis and Management are required

No clear standard for “reasonable and appropriate”

Return on Investment Analysis most common approach

The earlier the better

Make guesses and use common sense

