

Working with HIT Systems

Unit 7 Protecting Privacy, Security, and Confidentiality in HIT Systems

Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

Objectives

By the end of this unit the student will be able to:

- Explain and illustrate privacy, security, and confidentiality in HIT settings.
- Identify common threats encountered when using HIT.
- Formulate strategies to minimize threats to privacy, security, and confidentiality in HIT systems.

Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

Electronic Health Information Risks and Opportunities

- Access to electronic vs. paper records
- Public apprehension around digitization of health information
- Success of HIT systems depends on ensuring patient privacy
- Security can facilitate patient-centered care

Component 7/Unit 7

Component 7/Unit 7

Privacy, Confidentiality, Security Defined

- · Privacy: patient is in control
- Confidentiality: only authorized individuals are allowed access
- Security: controls/safeguards that ensure confidentiality

Component 7/Unit 7

Health IT Workforce Curriculur Version 1.0/Fall 2010

Security Management System Standards

- ISO 27001
- NIST 800-53
- HIPAA



Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

HIPAA and PHI

- Health Insurance Portability and Accountability Act of 1996
- Privacy Rule (effective 2003)
- Security Rule (effective 2005)
- HITECH Act of 2009

Name	Swepter	SANOR Posterii	(share Passell	(Mon Potari	(Aur.)	Number
SATTONE MODEL MODEL						
Nava ampuna	Manages the four-last instruction of salarit information second perceptation, recovered, contacts, salarists, colors of state.					
Smarts Carbellation	Range to spice occuping it peer adversion, mixing defens applices an operar adversion less. By mixing desert inches for 'over exactor' mixe.					
(heliumpione (11)	Allow the princips is add the symptoms, problem, condition, dispersion, physician recommendate dispersion draws from that is the based for a feed or exception.					
Natry of present these (MP)	Allow the provider is order privately of the preparation of subspirated by traders, southy assuming desirate foreign contact, marking factors and associated spirates in					
Constitutement	Provide currence for act this other in the contractor man interior maps angle that present pate represen- ant patent appears.					
Nacioni, economicos, Piri	Processor for the collection of all repeats of your family and count family from reference counter framework progenition, illustrate and provincements, promp others.					
Name of April 1997 (1997)	Albas for the reporting or developed symplectic or all participal garbons. Most systems include an addity in deep of symplectic or depts upon if self-only to other solicity, colouphon.					
(Irrae sales	Equation for the characters, such as destinated by the department and project (COP), reduced translating a potential consistent the potential study.					
SIR only allow	Astrophylip provide SSR cole; basel or of major colected surg (1, 50), as the majority prior both entering atta, principle and democing					
Trape in the state	A registrary to information that is presented the other form states assess, as and it is a state to done register from charts, or sign, all resolution as only other graphs of specifical frontiers.					
Smart on A strawing	Allow the preview is star or understall cognitive or lights private and control from a fire public record. Plan caper depots private and control from a fire public record.					

Component 7/Unit 7

Types of Security Safeguards

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards



Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

Administrative Safeguards

- Security Management Process
 - Risk Analysis
 - Risk Management
 - Sanction Policy
 - System Activity Review



Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

Administrative Safeguards

- Assigned Security Responsibility
 - Security officer



Component 7/Unit 7

Component	7/Unit 7
-----------	----------

Administrative Safeguards

- Workforce Security, Information Access Management
 - Who can and who cannot have access
 - Who determines who can have access and how
 - Employee turnover
 - Contractors
 - User roles



Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

10

Administrative Safeguards

- Security Awareness and Training
 - Training
 - Security reminders
 - Log-in monitoring
 - Password management



Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

Administrative Safeguards

- Security Incident Procedures
- Contingency Plan
 - Data backup
 - Disaster recovery
 - Emergency operation plan



Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010 12

Administrative Safeguards

- Evaluation
- Business Associate Agreements



Component 7/Unit 7

alth IT Workforce Curricu Version 1.0/Fall 2010

Physical Safeguards

• Facility Access Controls



Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

Physical Safeguards

- Workstation Use
- Workstation Security
- Device and Media Controls (e.g., media disposal, access to backup and storage media)



Component 7/Unit 7

n IT Workforce Curriculum Version 1.0/Fall 2010	15

Physical Safeguards

- Device and Media Controls
 - media disposal
 - access to backup and storage media



Component 7/Unit 7

Health IT Workforce Curriculun Version 1.0/Fall 2010

Technical Safeguards

- Access Control
 - Unique user identification
 - Emergency access
 - Automatic logoff
 - Encryption/decryption



Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

Technical Safeguards

- Audit Controls
- Integrity



Component 7/Unit 7

Component	7/Unit 7	7	

Technical Safeguards

- Person or Entity Authentication
 - Password/Passphrase/PIN
 - Smart card/token/key
 - Biometrics
 - Two factor authentication



Component 7/Unit 7

Health IT Workforce Curriculur Version 1.0/Fall 2010

19

Technical Safeguards

- Transmission Security
 - Integrity controls
 - Encryption



Component 7/Unit 7

Health IT Workforce Curriculum Version 1 0/Fall 2010

Risk Analysis and Management

- Analysis
 - Gather data on potential threats and vulnerabilities
 - Assess current security measures
 - Determine likelihood, impact and level of risk
 - Identify needed security measures
- Management
 - Develop a plan for implementation
 - Evaluate and maintain security measures

Component 7/Unit 7

Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

21

Meaningful Use

- Criteria for meaningful use of EHRs related to privacy, security and confidentiality meant to align with HIPAA
- Emphasizes need to conduct a risk analysis
- Some specific requirements for EHR vendors

Component 7/Unit 7

Health IT Workforce Curriculur

22

Summary

- Privacy, security, and confidentiality in HIT settings
- Common threats encountered when using HIT
- Strategies to minimize threats to privacy, security, and confidentiality in HIT systems.



Component 7/Unit 7

Health IT Workforce Curriculum Version 1.0/Fall 2010

23