

Working with HIT Systems

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



This material was developed by Johns Hopkins University, funded by the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology under Award Number H224DC000013.

Physical Safeguards

Facility Access Controls



Images: MS Clip



Component 7/Unit 7

Health IT Workforce Curriculum
Version 2.0/Spring 2011

2

Physical Safeguards

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

Component 7/Unit 7

Health IT Workforce Curriculum
Version 2.0/Spring 2011

3

Physical Safeguards

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

Component 7/Unit 7

Health IT Workforce Curriculum
Version 2.0/Spring 2011

4

Technical Safeguards

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



Image Source: MS Clip

Component 7/Unit 7

Health IT Workforce Curriculum
Version 2.0/Spring 2011

5

Technical Safeguards

- Audit Controls
- Integrity



Image: MS Clipart

Component 7/Unit 7

Health IT Workforce Curriculum
Version 2.0/Spring 2011

6

Technical Safeguards

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




Image: MS Clipart

Component 7/Unit 7
Health IT Workforce Curriculum
Version 2.0/Spring 2011
7

Technical Safeguards

- Transmission Security
 - Integrity controls
 - Encryption




Image Source: MS Clip

Component 7/Unit 7
Health IT Workforce Curriculum
Version 2.0/Spring 2011
8

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
Health IT Workforce Curriculum
Version 2.0/Spring 2011
9

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



Image: MS Clipart

Component 7/Unit 7

Health IT Workforce Curriculum
Version 2.0/Spring 2011

10

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.



Image Source: MS Clip

Component 7/Unit 7

Health IT Workforce Curriculum
Version 2.0/Spring 2011

11

References

- American Health Information Management Association. Available from: <http://www.ahima.org>
- Ensuring Security of High-Risk Information in EHRs c2008. Available from: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_03_9956.hcsp?dDocName=bok1_039956
- HIPAA Security Series: Security 101 for Covered Entities .c2004 Available from: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf>
- Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. c2008. Available from: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf
- Scribd, Mobility Infrastructure Solution Design Guide. c2008. Available from: <http://www.scribd.com/doc/24975115/Procurve-Wifi-Network-Design-Guide>
- U.S. Department of Health and Human Services. Available from: <http://www.hhs.gov>

Component 7/Unit 7

Health IT Workforce Curriculum
Version 2.0/Spring 2011

12
