Curriculum Development Centers Program

Awardee of The Office of the National Coordinator for Health Information Technology

Component 8 Installation and Maintenance of Health IT Systems

Unit 6b
System Security Procedures and Standards

This material was developed by Duke University, funded by the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology under Award Number IU24OC000024.

Technical Safeguards: Intrusion Detection System (IDS)

- Monitors networks or systems for malicious activities or policy violations.
- Logs such activity and notifies administrator.
- Takes preemptive actions to stop activities.
- NOT a firewall (and vice versa).

Technical Safeguards: Audit Logging

- Hardware/software/procedural mechanisms to record & examine access & other activity
- Data to be logged can vary depending on level of access controls to ePHI data.
- In general, servers should use OS system logging tools to track:
  - Who accessed (or tried to access) server.
  - What data/databases were accessed, any changes made.

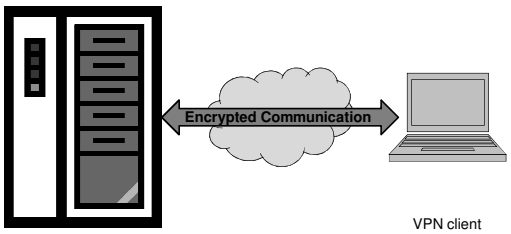
Technical Safeguards: Audit Logging (cont'd)

- EHR should also support logging:
  - User access
  - Patient data accessed
  - Sign-on failures
  - Data changes made
- Periodic proactive audits (sampling)
  - Consider for higher-risk patient populations (e.g., employees) or after publicized events
  - To deter abuse, make users aware.
- Reactive audits triggered by defined event

Technical Safeguards: Offsite Access

- Should be tightly regulated.
- Utilize Virtual Private Network (VPN) and encryption at all times.
- VPN
  - Uses encryption, authentication, authorization, Network Access Quarantine Control to protect data.
  - Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol/Internet Protocol security (L2TP/IPSec)

What is a Virtual Private Network (VPN)?



Server & Computer Security Tips

- Install firewall, IDS, & monitoring tools to monitor & protect all servers using/storing ePHI.
- Strong policies for use of ePHI.
- Rename local administrator & guest accounts; strong passwords; disable unused accounts.
- NTFS file system (Windows servers)
- Antivirus software, with updates
- Attack surface reduction tool: turn off unneeded server applications & reduce attack surface.
- Configure server correctly, with vendor
- Create security baseline; tools available.
- Install service packs within 48 hours of release.
- Lock down database applications, regularly install updates.

Contingency Plans

- Critical data backed up and stored
- Emergency call list
- Plan to restore systems
- Plan to move into temporary office
- Secure offsite storage
- Situations that may activate contingency plan

Contingency Plans (cont'd)

- Written plans
  - Risk analysis/assessment
  - Database backup
  - Database secure storage
  - Data restore plan
  - Disaster recovery plan
  - Critical incident response plan
- Software inventory
- Hardware inventory
- Logs: transmission points

Data Backup Policy

- Data integrity just as important as confidentiality.
- Backing up critical files, including patient or EHR databases, helps ensure data recovery after catastrophic failure or security breach.
- Determine procedures, hardware, and software required for reliable & efficient backup of production databases.

Secure Data Storage & Restore Policies

- Data most susceptible to corruption or loss in state of rest (90% of the time).
- Databases need particularly thorough analysis for risks.
- Detailed guidelines for securing and safely restoring data stored on network.

Disaster Recovery & Critical Incident Response Plans

- Address emergencies requiring immediate intervention to protect network or restore operational status after catastrophe.
- Based on original risk analysis.
- Outlines elements, procedures, & people needed to restore network or mitigate imminent threat in timely manner.

Hardware & Software Inventories

- Hardware inventory
  - Loss of hardware can mean a loss much greater than just replacement cost.
  - Helps ensure equipment properly locked down and secure.
- Software inventory
  - Provides insight to manage/mitigate risks to network from software vulnerability.
  - Facilitates proper software management practices, patching.

Logs: Transmission Points

- Effective logging and monitoring strategy is critical to network security.
- Logs can be overwhelmingly large. Determine which data need stringent monitoring (e.g., who is accessing); begin by concentrating efforts there.
- Written plan of what is logged & why, with procedures for auditing & record of accountability to ensure compliance.

Summary

- Security measures to be implemented on your network will largely depend on:
  - Federal, state, & local requirements
  - Organizational requirements
  - Network type topology & operating system (OS)

Reference

- University of Wisconsin-Madison HIPAA Security Best Practices Guidelines, #3 Audit Controls, 4D
  - http://hipaa.wisc.edu/docs/auditControls.pdf