Installation and Maintenance of Health IT Systems

Unit 6b

System Security Procedures and Standards

Technical Safeguards - Access Control

- Use an Intrusion Detection System (IDS), which:
  - Monitors networks or systems for malicious activities or policy violations.
  - Logs such activity and notifies the administrator.
  - Can take preemptive actions to stop detected activities.
  - Is NOT a firewall (and vice versa).

Technical Safeguards – Logging

Implement adequate audit logging:

- What NEEDS to be logged can vary depending on the level of access controls to the ePHI data.
- In general, your servers should use the OS system logging tools to log:
  - Who accessed, or tried to access, the server
  - What data/databases were successfully accessed and any changes made

Technical Safeguards – Logging

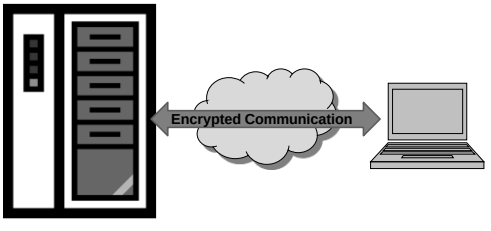
Your EHR software should also support logging:

- User access
- Patient data accessed
- Sign-on failures
- Any changes that were made to the data

Technical Safeguards – Offsite Access

- Offsite access of ePHI should be tightly regulated.
- Virtual Private Network (VPN) and encryption should be utilized at all times.

What is a Virtual Private Network (VPN)?



Server and Computer Security

- Install a firewall, IDS, and monitoring tools to monitor and protect all servers using/storing ePHI.
- For Windows servers, use NTFS file system.
- Install and maintain reliable antivirus software.
- Rename the local administrator and guest accounts, use strong passwords, and disable any accounts not in use.
- Use an attack surface reduction tool to turn off unneeded server applications and reduce the attack surface.
- Install the latest service packs, no later than 48 hours after release.
- Protect your database applications by locking them down and regularly installing application 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

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

Summary

The security enhancement you implement on your network will largely depend on:

- Network type topology and operating system (OS)
- Federal state and local requirements
- Organizational requirements
- User needs