Keeping our patient's information secure and confidential. What does it really mean?

Introduction

- Susan Martin, RN, JD, CIPP/G, CPHIMS

Disclaimer – No conflicts of interest to disclose

Objectives

- The nurse informaticist will understand common network and application security controls for the protection of sensitive medical and personal information in the electronic health record (EHR).
- The nurse informaticist will learn best practices for safeguarding health information, securing mobile platforms accessing patient information at the bedside and securing the information available via the organization’s patient portal.

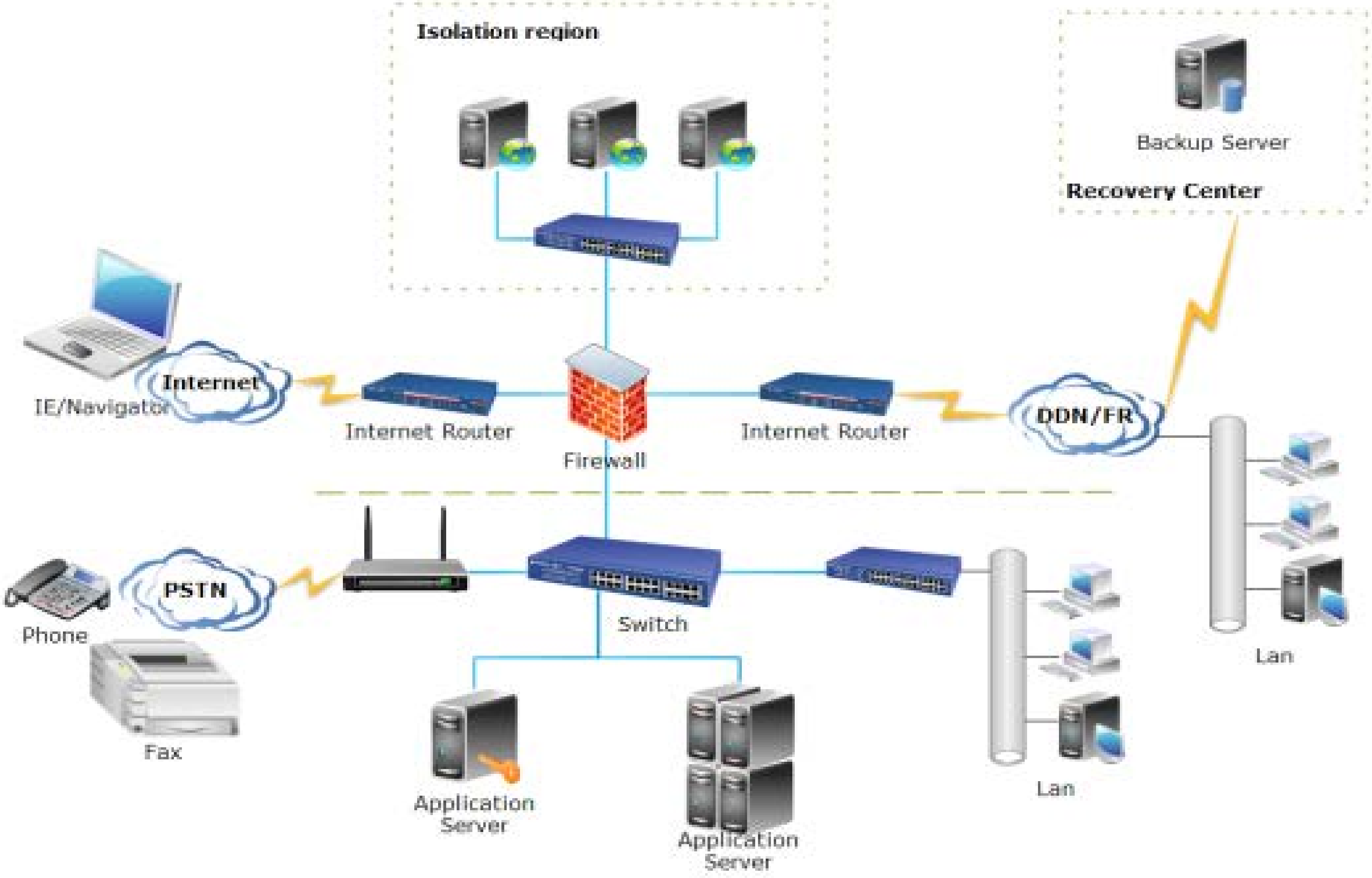
Getting started

- Ensuring the accuracy and confidentiality of sensitive medical information is vital to what we do every data as clinical informaticists.
- It takes a village of IT professionals contributing to the protection of data in its information systems.
- Security engineers practice a concept of “Defense in Depth,” building multiple security controls to protect sensitive data systems

Network Administrator

- This role includes designing perimeter and internal security through the configuration of firewalls, virtual private networks (VPN) concentrators and security appliances for access to vital business applications.
- Wired local area network (WLAN) with multiple VLANs separating clinical systems and medical devices
- Wireless network (Wi-Fi)
- HTTPS, Wi-Fi Protected Access encryption
- Virtual private network (VPN) to protect data from interception during transmission, internal or remote
- Patient Portal
- Demilitarized Zone (DMZ)

Information Center Network



System Administrator

- This role is responsible for the configuration, upkeep and reliable operation of computer systems, especially multi-user computers such as servers in the healthcare setting. Activities include:
- Building security into systems by configuring security protocols
- Installing operating system security patches and updates
- Reviewing system logs of user logins/actions and reporting malicious or suspicious activity to the information security official (ISO)
- Creating system accounts for server access or system services – system vs. Active Directory (AD) account
- AD managed environment use group policy objects (GPOs) to provide centralized management and configuration of the operating system (OS), applications and user settings
- Generating and retaining application backups

Application Administrator

- This role is responsible for the administration of one of more clinical applications. Application Administrators aren't developers but they are critical to keeping the applications each healthcare organization relies on running. Activities include:
- Working with system administrator to set up servers that satisfy security and vendor requirements
- Installing, updating, tuning, diagnosing, and monitoring performance of both internal and third-party applications associated with the clinical system
- Loading organization specific data into the system and generally keeping it up and running
- Performing initial troubleshooting of errors and working with vendor technicians to correct any problems
- Creation and maintenance of user accounts and user groups – privacy concept of “least privilege”
- Providing user support

Information Security Official (ISO) * required by HIPAA

- The ISO oversees the compliance with information security requirements of the HIPAA Security Rule and other regulatory frameworks like the Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) special publications for operational, technical, and management safeguards used to maintain the integrity, confidentiality, and security of data contained in IT systems. Responsibilities include:
- Performing a risk assessment of the EHR
- Designing security measures to reduce risks and close vulnerabilities
- Developing and implementing policies and procedures to prevent, detect, contain and correct security violations or weaknesses
- Information security is very important to help protect against data theft from internal threats as well as cybersecurity threats

Privacy Official * required by HIPAA

- The privacy official is responsible for developing privacy policies and procedures. This includes:
- Developing and maintaining the organization’s notice of information practices
- Implementing the patients right to access, right to review, and request amendment to their health records: request additional protection for confidential communications (email or phone) related to particularly sensitive health information
- Overseeing the management of business associates agreements with third parties that process ePHI for business operations
- Training the organization’s workforce on HIPAA’s privacy and security requirements for accessing patients and identifiable patient information
- Investigating complaints from patients about suspected HIPAA violations and responding to complaints submitted to HHS Office for Civil Rights

Best Practices for Safeguarding Health Information

- The HIPAA Security Rule and the HIPAA Privacy Rule provide guidance for large and small healthcare entities

https://www.hhs.gov/hipaa/for-professionals/security/index.html

- HHS Health IT.gov website provides another tool entitled *CyberSecurity 10 Best Practices for Small Healthcare Environment*

https://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf

- The Office of the National Coordinator for Health Information Technology (ONC) SAFER Guides enable healthcare organizations to address EHR safety in a variety of areas. The guides identify recommended practices to optimize the safety and safe use of EHRs.

https://www.healthit.gov/topic/safety/safer-guides

CyberSecurity 10 Best Practices for Small Healthcare Environment

The checklist lists the recommended practice and questions that will help organizations assess compliance with best practices. 9 areas of focus include:

Recommended Checklist	Questions from the Checklist
Practice 1 - Password	
Practice 2 – Anti-virus	
Practice 3 - Firewall	
Practice 4 – Access Control	
Practice 5 – Physical Access	
Practice 6 – Network Access	
Practice 7 – Backup & Recovery	
Practice 8 - Maintenance	
Practice 9 – Mobile Device	

Practice 1: **Password**	• Does organization have password policies and trained staff on the requirements? • Does staff have unique username and passwords that are strong, not shared, written down, or displayed on the screen? • Are passwords changed routinely and not re-used? • Are default passwords changed during product installation?
Practice 2: **Anti-Virus**	• Does organization have policies requiring the use of anti-virus software and trained staff on recognizing the symptoms of viruses or malware on their computer, what to do to avoid virus/malware infections, and how to report it? • Is anti-virus software installed and operating effectively on each computer and receiving automatic updates from the manufacturer? • Do handheld or mobile devices that support anti-virus software have it installed and operating?

SAFER Guides by Group

Foundational Guides	•High Priority Practices* •Organizational Responsibilities*
Infrastructure Guides	•Contingency Planning* •System Configuration* •System Interfaces*
Clinical Process Guides	•Patient Identification* •Computerized Provider Order Entry with Decision Support* •Test Results Reporting and Follow-Up* •Clinician Communication*

Security of Patient Portals

❑Requires a privacy notice that describes the personal information collected from patients, its intended uses and describes how the organization will secure the patient

❑Requires an independent vulnerability assessment of the patient portal application to ensure security weaknesses are addressed

❑Best practice includes locating the webservers in a demilitarized zone (DMZ) to limit direct access to the electronic medical record behind network firewalls

❑A proxy may be configured to authenticate the patient log on before displaying the patient’s medical record

Questions?