Northwestern Medicine®

Information Security Overview

1. Information Security Overview
2. Patient Data Privacy
3. Common Threats and Risks
4. Best Practices for Protecting Information
5. Data Handling and Confidentiality

Information Security

Overview

Information security in healthcare is not just about IT systems. It's about protecting patient information from all types of threats, ensuring its confidentiality, integrity, and availability.

- **Confidentiality:** Keeping patient information private.
- **Integrity:** Ensuring the accuracy and completeness of data.
- **Availability:** Ensuring that data is accessible when needed by authorized individuals.

Information Security

Patient data privacy

Patient data privacy is the right of a patient to have their personal health information kept secure and not disclosed without their consent.

- **HIPAA** (Health Insurance Portability and Accountability Act) is the cornerstone of patient data privacy, setting the standards for protecting sensitive patient data.
- **HITECH Act** extends HIPAA's requirements with increased penalties for non-compliance.

Information Security

Common threats and risks

Threats to patient data can be external or internal and range from sophisticated cyber-attacks to simple human error. Common threats include:

- **Phishing Attacks:** A common threat where attackers trick students or employees into revealing sensitive information, thereby compromising the security of sensitive data.

  Example: Replying to a seemingly authentic email by disclosing your password.

- **Ransomware:** Malicious software that encrypts data and demands ransom, disrupting patient care and posing significant safety risks.

  Example: Clicking a link that appears to verify account information, seemingly from a trustworthy source – but it's not.

- **Insider Threats:** Risks from within the organization, either through intentional misuse or accidental mishandling of sensitive information, leading to data breaches.

  Example: Walking away from an unlocked computer while logged into a sensitive system.

Information Security

Best practices for protecting information

Protecting information is everyone's responsibility. Best practices include:

- **Personal Data Hygiene:** Adopt strong personal data hygiene habits, such as creating strong passwords, using multi-factor authentication (MFA), not sharing login credentials, and understanding the importance of logging out of systems when not in use.
- **Personal Device Security:** Ensure that any personal devices used for academic or clinical purposes are secured with strong passwords, disk encryption, antivirus, and are kept updated with the latest security patches.
- **Professionalism in Digital Spaces:** Exercise professionalism on social media and online forums, being careful not to share any patient information, even inadvertently.
- **Exercise Caution with Online Tools and AI Platforms:** Understand that platforms like ChatGPT or Grammarly are not designed to handle sensitive patient data. It is critical never to input or discuss any identifiable patient information on such platforms.

Information Security

Data handling and confidentiality

Proper data handling is vital. This includes:

- **Secure Communications:** Always use approved and secure channels with end-to-end encryption for discussing patient information electronically, such as emails and messages, to ensure that only intended recipients can access it.
- **Secure Note-Taking:** Develop habits for secure note-taking and storage, in both digital and physical forms, and learn proper disposal methods for these notes. This includes regularly cleaning up digital notes and ensuring that any deleted files are irrecoverable.
- **Adherence to Policies:** Familiarize yourself with and adhere to the Feinberg School of Medicine and Northwestern University policies regarding data handling and confidentiality.
- **Reporting Security Incident:** Learn the appropriate steps to take if a security incident or breach is suspected, including whom to contact and how to document the incident.

Information Security

Reporting incident

Immediately contact Feinberg IT or Northwestern IT Information Security to report a suspected breach:

- Call the Northwestern IT Service Desk at 847-491-4357 (1-HELP)
- Email Feinberg IT at fsmhelp@northwestern.edu
- Email Northwestern IT Information Security Office at security@northwestern.edu

Any incidents involving online harassment or physical theft of a device, including personally-owned, should be reported to University Police:

- In an emergency, dial 911
- For non-emergencies:

Chicago Campus

Phone: 312-503-3456 (or dial 456 from any campus phone)
TDD Phone: 312-503-3999 (TDD)
211 East Superior Street, Chicago, IL 60611

Evanston Campus

Phone: 847-491-3456 (or dial 456 from any campus phone)
TDD Phone: 847-467-7883 (TDD)
1201 Davis Street, Evanston, IL 60208

Information Security

Relevant policies

Appropriate Use of Electronic Resources
https://www.it.northwestern.edu/about/policies/appropriate-use-of-electronic-resources.html

Student Handbook
https://www.northwestern.edu/communitystandards/student-handbook/