Informatics: Confidentiality and Security

Beth Vottero PhD, RN, CNE
Objectives

1. Understand the basics of health information privacy and security
2. Explain techniques to maintain the privacy of health information in the specific health care setting
Vulnerability

- Cyber threats and malware continue to threaten electronic data
  - Ongoing process to secure and protect vital health electronic data
  - Knowledge of what constitutes a cyber threat, malware, virus is crucial

- Health care workers must know how their interactions with technology, specifically electronic medical records, can help protect sensitive health data
Description

- **Cyber threat** is the possibility of a malicious attempt to damage or disrupt a computer network or system.

- **Malware** is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.
Protection

Most facilities employ safeguards against cyber threats and malware

- Intranet
- Firewalls
- Contained internet access
- Multiple ‘behind the scenes’ processes designed to eliminate potential threats
Closer look

A nurse is looking for information about a patient’s diagnosis. Accessing a university’s library databases for quality information seems reasonable and appropriate. The nurse clicks on the library database and the screen becomes distorted. Before the nurse can close the screen, a message is displayed that the computer is shutting down due to a virus attack.
Closer look

- Even ‘reputable’ websites or emails from someone you know can have malicious viruses and malware
  - Web pages are created to look identical to reputable sites
  - Can be used to gain access to the computer and the data stored in the network
  - Typical signs include
    - Website performance is not normal
    - Misspelled words or poor grammar
Sensitive data

- Safeguards must provide adequate security for personal information

- Primary threats involve data that is altered, destroyed or disclosed

- Multiple levels of safeguards for personal health data employed by health care facilities
  - Required by law
Protecting health data

Why is it important to protect health data?

- Medical records used for Medicare/Medicaid fraud
  - For credit cards, liability is limited. For insurance fraud, the patient remains liable
- Altered health records
- Costs patients an average of $13,500 to fix compromised medical record
- Medical records are not stolen for the medical information, in most cases it is for the patient identification information
Recent notable cases

- Community Health Systems operate hospitals in large and small markets with over 30,000 beds in total
  - Data breach affecting over 4.5 million patients
  - 2nd largest ‘hack’ in US history
  - Data stolen used to open credit cards, secure loans, etc.
- Anthem is one of the country’s largest health insurers
  - 80 million current and former member’s data stolen
Code of ethics

Provision 3 of the ANA Code of Ethics states that:

Associated with the right to privacy, the nurse has a duty to maintain confidentiality of all patient information. The patient’s well-being could be jeopardized and the fundamental trust between patient and nurse destroyed by unnecessary access to data or by the inappropriate disclosure of identifiable patient information.
<table>
<thead>
<tr>
<th>Code of ethics</th>
</tr>
</thead>
<tbody>
<tr>
<td>The rights, well-being, and safety of the individual patient should be the primary factors in arriving at any professional judgment concerning the disposition of confidential information received from or about the patient, whether oral, written or electronic. The standard of nursing practice and the nurse’s responsibility to provide quality care require that relevant data be shared with those members of the healthcare team who have a need to know.</td>
</tr>
</tbody>
</table>
Code of ethics

Only information pertinent to a patient’s treatment and welfare is disclosed, and only to those directly involved with the patient’s care. Duties of confidentiality, however, are not absolute and may need to be modified in order to protect the patient, other innocent parties, and in circumstances of mandatory disclosure for public health reasons.
Code of ethics

Information used for purposes of peer review, third-party payments, and other quality improvement or risk management mechanisms may be disclosed only under defined policies, mandates, or protocols. These written guidelines must assure that the rights, well-being, and safety of the patient are protected. In general, only that information directly relevant to a task or specific responsibility should be disclosed.

*When using electronic communications, special effort should be made to maintain data security.*
Code of ethics

Access your organization’s policy on the use of protected health information. Read the policy with the following questions in mind:

- When is it appropriate to share protected health data?
- How does your facility define ‘need to know’?
- Does your facility define ‘mandatory public health reasons’ for sharing protected health information?
HIPAA
Health Information Privacy and Security Act of 1996
Some highlights

Describes standards for

- Unique individual identifiers and the use of such identifiers
  - Code words
  - Security passwords

- Security standards for electronic health information
  - Training of those who access health information
  - Technical abilities to maintain records
  - Audit trails in computerized systems
Closer look

A patient provides the security word, ‘John’ to his nurse for use by family members when calling to ask about the patient’s condition. The patient tells the family that the word is the name of his only son, whose name is ‘Tom’. The wife calls that night to ask about the patient’s condition. When she gives the security word ‘Tom’, the nurse tells her that it is wrong but gives her the patient’s information anyway.
Closer look

- The nurse knows the wife and was present when the patient gave the security word to the nurse. Is the nurse wrong to deny patient information to the wife because the security word was wrong?
- What could the nurse do to help the wife receive the requested information?
- What would you do if this occurred and you were friends with the patient and family?
Safeguards

- To ensure the integrity and confidentiality of the information
- To protect against any reasonably anticipated—
  - threats or hazards to the security or integrity of the information; and
  - unauthorized uses or disclosures of the information; and
- otherwise to ensure compliance with this part by the officers and employees of such person
Penalties
IN GENERAL.--Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.
Wrongful disclosure of health information

OFFENSE--A person who knowingly and in violation of this part--
- uses or causes to be used a unique health identifier;
- obtains individually identifiable health information relating to an individual; or
- discloses individually identifiable health information to another person,

PENALTIES
- be fined not more than $50,000, imprisoned not more than 1 year, or both;
- if the offense is false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
- if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.
Closer look

Could the nurse be liable for any monetary punishment based on the previous scenario where the nurse released patient information to the wife?

Is this a simple yes or no question? Why?
Emails

- Private Health Information (PHI) cannot be shared over non-encrypted emails
- This includes lab results, information about health status, tests, etc.
- Encrypted emails must be set up on the side of the health care provider
Vulnerability of workstations

Ways to protect your workstation computer:

- Password protected screensaver
- Privacy screen
- Log off and shut down when not in use
- Time out for computer screens
- Locked access
- Password changed per organization protocol
### Important terms

**Privacy:** Freedom from unauthorized and unwarranted intrusion. Personal health data is always considered private.

**Security:** Measures taken to limit access to information and protect it from attack or theft. Data can be secure, but not private.

**Data Integrity:** Assurance of reliability and accuracy of information. Data can be private and secure, and yet have no integrity.
Closer look

A nurse protects the workstation by always logging off if leaving the computer for anything. Currently, the nurse is working on the patient’s assessment when called away. The last piece of data entered was a blood pressure of 20/8 although it was supposed to be 120/80. The nurse logs off the assessment screen.

- Is the data secure?
- Is the data private?
- Does the data have integrity?
Closer look

Consider the following:

- How do you ensure that the personal health information you work with is kept private?

- How do you ensure that the personal health information is secure?

- How do you maintain the integrity of data you work with?
Resources

HIPAA and Health Information Technology (HIT)

Personal Health Records (PHR) and HIPAA
Social media

Social media consists of websites, applications and web-based tools that connect users to engage in dialogue, share information and media, collaborate and interact. Types include:

- Blogs
- Social networking sites (i.e., Facebook, LinkedIn)
- Video and photo sharing sites (i.e., Snapchat, Vines, Instagram)
- Virtual worlds
- Web-based communities and hosted services
National Council of State Boards of Nursing (NCSBN)

- The NCSBN created ‘A Nurse’s Guide to the Use of Social Media’
- Clearly explains the intricacies of using social media for nurses

https://www.ncsbn.org/NCSBN_SocialMedia.pdf
Closer look

Your family member was changing a light bulb and fell off a ladder breaking an ankle. The injury required surgery. You started a ‘Go Fund Me’ account as a surprise to help with the medical expenses. You posted the ‘Go Fund Me’ page on your Facebook web page.

- What might happen if the family member did not want their injury exposed to the public?
- What are the potential ramifications of your well-meaning gesture?
Social media cautions

Never
- Talk about a patient care encounter on social media
- Discuss a patient or care encounter
- Reveal a patient’s identification or anything that could be construed as a patient identifier
- Post pictures taken at a health care facility
  - Many health care organizations do not want facilities pictures posted, no matter how well-meaning they may be
Best tactics

- If it doesn’t feel right, it isn’t
- Do not allow others to use your login or password, EVER
- Logoff or use a password protected screen saver when leaving a work computer
- Never discuss a patient on social media
More information

ANA Social Policy Statement
https://ananursece.healthstream.com/Pages/Product.aspx?ID =ea27473c-ea5a-e011-9261-001517135351

Guidelines for Social Media

HIPAA and Nursing
http://www.nursingworld.org/MainMenuCategories/ANAMark etplace/ANAPeriodicals/OJIN/TableofContents/Volume102005 /No2May05/tpc27_116017.html