HIPAA Privacy and Security

Course ID: 1020 - Credit Hours: 2

Author(s)

Kevin Arnold, RN, BSN

Disclosures

Clinical Specialist, Bard Access Systems

IVTAGS, LLC - Owner

Audience

All health care workers. HIPAA Privacy and Security addresses federal laws and guidelines for protecting and maintaining Protected Health Information.

Accreditation

KLA Education Services LLC is accredited by the State of California Board of Registered Nursing, Provider # CEP16145.

Course Objectives

After completion of this lesson, participants will be able to:

1. List 5 examples of protected health information (PHI).
2. List 3 Patient's rights.
3. List 3 examples uses of PHI.
4. List 3 example HIPAA violations.
5. Describe the consequences of HIPAA violations.
6. List 3 patient's right.
7. List 3 threats to PHI security.

Federal Law

- **HIPAA** is the Health Insurance Portability and Accountability Act of 1996.
- **HIPAA Privacy** – Protection for the privacy of Protected Health Information (PHI) effective
- **HIPAA Security** – Protection for the security of electronic Protected Health Information

- Protects the privacy and security of a patient's health information.
- Provides for electronic and physical security of a patient's health information.

HIPAA Privacy

Sample Protected Health Information (PHI)

- Name
- Address (any part)
- Name of employer
- Date of admission, birth
- Date of discharge, death
- Telephone and Fax numbers
- Electronic (email) addresses
- Social Security Number
- Medical Records
- Health Plan Beneficiary Info
- Account number
- Medical record number
- Any vehicle ID number
- Photographic Images
- Medical Hx or Tx
- IP (internet protocol) #
- Web URL
- Certificate / Licenses #
- Finger prints
- Any identifying data

- Do not access information unless it is needed to do your job.
- Do not share information with colleagues unless they need it to do their job.

Examples…

- Treatment of patient
  - –Direct patient care
  - –Coordination of care
  - –Consultations
  - –Referrals to health care providers

Examples…

- Operations
  - –Administrative activities
  - –Quality improvement
  - –Compliance
  - –Competency
  - –Training

Examples

- Payment of health care bills
  - Includes any activities required to bill and collect for health care services.

Examples…

- Disclosures required by law
- Public Health and other governmental reporting

Method of PHI Communication

- Verbal
- Paper
- Electronic

Verbal Communication

- When talking make sure you are:
  - Sharing with someone who needs PHI for their job.
  - Speaking where others can not hear.
  - Giving only the minimum PHI necessary

Paper Communication

- Nursing services may release a copy of a patients medical record to health care personnel transporting a patient to another health care facility.
- Physicians and Nurses may release some information to a patient

Paper Communication

- Typically releasing PHI is left to medical records departments.
- Dispose of PHI properly (shred)

Paper Communication

- Limit faxing to emergent situations
- Always include a cover sheet with a confidentiality notice
- Use secure fax locations
- Faxes sent to inadvertent locations should be reported

Paper Communication

- PHI should not be left on counters, in conference room, or anywhere it may be accessible to the public or staff that do not need to know the information.

Protecting Electronic PHI

- Ensure data is encrypted
  - Encryption assures PHI is unreadable to anyone but authorized devices.
- Create strong passwords
- Secure computers and other devices
- Avoid discussion on blogs/threads
  - Often contain malware, phishing software

Protecting Electronic PHI

- Malware is software designed to harm your computer (viruses, worms, spyware)
- Phishing is unwanted email or web site requests for confidential information
- Avoid suspicious emails

Protecting Electronic PHI

- Avoid storage of PHI on “Cloud” servers.
- Cloud servers store information over the internet (Dropbox, TheBox, Google Drive, Apple iCloud)

Example Violations…

- A medical chart left open at a nursing station
- A lost medical record
- PHI on a thumb drive that was lost and not password protected
- A PowerPoint presentation containing PHI given to a department of 20 employees with out proper authorization from the patient.

Example Violations…

- Informing a patient's family member of a patient medical diagnosis with out proper authorization.
- A physician and nurse discussing a case in the elevator with others present
- A smart phone containing PHI left on the counter with no pass word protection in place
- PHI on a computer left open and unattended

Reporting

- If you are aware or suspect a violation, report it to the appropriate supervisor or privacy officer.
- Failure to report is a violation.

Consequences

- $100 per violation, $25,000 for an identical violation within one year
- $50,000 for wrongful disclosure
- $100,000 and/or 5 years in prison for wrongful violation for obtaining PHI under false pretenses
- $250,000 and/or 10 years in prison if committed with intent to sell or transfer for commercial advantage, personal gain, or malicious harm, includes obtaining or disclosing.

Contacting Patients

- Before contacting a patient, make sure the patient does not have an approved request for an alternative method or location for communications.
- You should NOT leave PHI on answering machines, voice mails

Contacting Patients

- Appointment reminders made by telephone must be limited to:
  - Patient's Name
  - Caller's Name
  - Location
  - Date and Time of appointment
  - A call back number for further questions
- Do not disclose other details.

Patient's Rights

- The right to request restriction of PHI uses & disclosures
- The right to request alternative forms of communications
- The right to access and copy patient's PHI
- The right to an accounting of the disclosures of PHI
- The right to request amendments to information

Patient's Right to Opt Out

- Patients may opt out at the time of admission and at any time.
  - His/her information will not be shared with outside callers or visitors
  - The patient is not included in the patient list maintained by the Hospital telephone operators
  - If a patient “opts out” of the patient list, callers or visitors should be told, “I have no information available on that person.”
- All patients admitted to a Psychiatry service are typically automatically opted out.

What is okay?

- Typical Approved Disclosure to the Public
  - The patient's location
  - The patient's general condition "stable", "serious", or "critical"

Question?

- When Mr. Thomas is admitted, he signs a General Consent for treatment and does not choose to "opt out" of any areas. He calls her nurse upset because he just received a phone call from someone he did not want to know he was in the hospital.

- **Should this person's information have been disclosed?**

Answer…

- Since Mr. Thomas did not choose to “opt out” of the patient directory, callers inquiring about him by name would receive confirmation of his admission and general information about his condition.

Question?

- A patient drops by the nursing station as he is being discharged to get a copy of his medical records. Michelle, a business associate, accesses the patient's medical record and prints a complete copy for the patient to take with him.

- **Should Michelle have given the patient a copy of his medical record?**

Answer…

- NO, Michelle should have advised the patient to obtain a copy from the medical records office.

Question?

- Kathy calls a patient to remind them about and appointment.
  - " Hi, this is Kathy calling for James Henderson to remind you about your appointment tomorrow morning at 9:00AM. You may call me back at 555-1234 with any questions."

- **Was this message appropriate?**

Answer…

- Yes, Kathy did not identify the clinic or any sensitive medical information…only the necessary data for the appointment.

Question?

- Jack answers a phone call asking about the health status of Mrs. Owens. Jack looks up but does not see Mrs. Owens on the patient on the unit's roster. Jack knows Mrs. Owens is doing fine and about to be discharged from listening to the morning report. Jack tell the caller he can't say medial details, but she is doing okay.
- **Was this the appropriate response?**

Answer…

- NO, Jack should have known a patient not listed on the roster was a “no information patient.” Many patients “opt out” and do not want it known they are in the hospital. Jack should have said “I’m sorry but I have no information on that person.”

Question…

- You are an RN working in the MICU. One of your best friend's wife is in an auto accident and gets admitted to the Emergency Department. Your friend calls you to see if you look up her chart and make sure you agree with the treatment she is being given.

- **What can you do to help?**

Answer…

- You are only allowed to view information needed to do your job. Since you are not caring for this patient, you may not look up the chart or ask someone else to access it on your behalf.

HIPAA Security

Electronic Security of PHI

- Computer-based patient health information that is used, created, stored, received or transmitted.
- Information in an electronic medical record, patient billing information, digital images, etc.
- Ensure confidentiality (no disclosure) of PHI.
- Ensure integrity (no alteration) of PHI.

Usernames and Passwords

- Never share your username or password
- Never use someone else's username or password
- Change passwords often or per facility protocol

Email

- Use encryption
- Avoid use of personal email accounts

Work Areas

- Log off or lock work stations when unattended
- Make use of auto-lock features when possible
- Use screen savers or security screen protectors possible

Threats

- Suspicious emails
  - From names you do not recognize
  - Phishing links
  - Attachments

Threats

- Remote Access Trojans
  - –Remote uses may access your computer without your permission or with out you knowing
  - –May steal PHI from your computer

Threats

- Worms
  - –Viruses that take advantage of network security holes and spread throughout an internal network of computers

Threats

- Spyware
  - –Virus software that can monitor your computer usage and collect data to an external location. Often causes multiple out of control pop up advertisements.

Threats

- Keystroke Loggers
  - –Virus software that can record every keystroke on you computer and collected to an external location. Often serve as an attempt to record usernames and passwords.

Anti-Threat Measures

- Help to keep anti-virus software up to date
- Use of internet firewalls is recommended

Portable Devices

- Avoid long term storage of PHI on portable devices such as:
  - USB storage devices
  - Laptops
  - iPads
  - Smart phones
  - PDAs
- Destroy PHI when it is no longer needed.

References

- American Recovery and Reinvestment Act of 2009, Title XIII Health Information Technology for Economic and Clinical Health, Subtitle D, Privacy
- Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- NIST SP 800-30, Risk Management Guide for Information Technology System
- OCR website: Summary of HIPAA Privacy Rule
- OCR website: Summary of HIPAA Security Rule