Chris Nicholson MT (ASCP) CLS
Program Director
Phlebotomy U
San Diego, California

Philip Rey CPT
Phlebotomy Instructor
Phlebotomy U
San Diego, California

The Health Insurance Portability and Accountability Act (HIPAA) for Healthcare Professionals

Purpose and Objectives:

The purpose of this course is to provide you with information about the HIPAA law and its guidelines. This course covers various aspects HIPAA, including confidentiality, communication, record keeping and how it applies to caring for patients. The course also contains useful information about how to manage encounters with Protected Health Information (PHI) in relation to HIPAA and compliance. It also reviews the most common causes for a HIPPA violation.

After successful completion of this course, the healthcare professional will be able to:

1. Describe what HIPAA is and what portion of the law applies to their role in the healthcare system.

2. Identify who is obligated to maintain patient confidentiality.

3. Identify what type of patient communication and information sharing requires compliance under HIPAA.

4. Describe what PHI is and why it is important.

5. Understand the most common causes for a HIPPA violation.

6. Describe the penalties for non-compliance with HIPAA requirements.

HIPAA Case Study:

Lisa works at a large metropolitan healthcare system. She is a Certified Phlebotomy Technician (CPT) and is the supervisor of a large outpatient blood collection center. She has 12 employees reporting to her. Lisa has worked at the healthcare system for 10 years. Jim is a CPT that works for Lisa at the same blood collection center. Lisa hired Jim 7 years ago. Jim is an outstanding employee. He is dependable, reliable, and he is a highly skilled phlebotomist. The patients all like Jim and often request for him to collect their blood sample. Lisa is an outstanding supervisor. She is thoughtful and kind to her staff. She recognizes and rewards great work by using the healthcare system's employee appreciation program. Under Lisa's leadership her team has above average patient satisfaction scores and exceptional employee satisfaction scores. Lisa recently became concerned about Jim. He didn't look well and had been out sick more than usual. On Monday Lisa got a note from Jim's doctor placing him on a medical leave for six weeks. The physician is an Oncologist at the healthcare system where Lisa and Jim both work. Lisa was so worried about Jim she decided to look up Jim's medical record in the healthcare system's Electronic Health Record (EHR). Will is the manager of all of the healthcare system's blood collection centers. Lisa reports to Will. On Wednesday Will was contacted by the healthcare system's Privacy Officer. The Privacy Officer told Will that the healthcare system's compliance monitoring software (Snoop Ware) had detected on Monday an employee looking up Protected Health Information (PHI) on another employee. The Privacy Officer said that on Monday Lisa logged into the EHR and looked at Jim's PHI. An investigation of the incident was started.

Was this a HIPPA violation?

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Maintaining the privacy and confidentiality of patient information is a cornerstone of the health care practice, and all medical professionals must follow ethical and legal standards which protect this information. In 1996 the U.S. Congress passed legislation to help combat waste, fraud, and abuse in the healthcare field, recognizing that the ever-increasing use of electronic communications posed a risk for privacy breaches.

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. Specifically, it requires healthcare practitioners to obtain a patient's written consent before disclosing private medical information to unauthorized parties. Prior to giving consent, patients must be informed of their rights involving the release of PHI and how the information will be used.

This law seeks to facilitate the flow of healthcare information necessary for effective patient care, while safeguarding the privacy of all personal information. HIPAA compliance is regulated by the Department of Health and Human Services (HHS) and enforced by the Office for Civil Rights (OCR).

Communication and Information Sharing which Requires HIPAA Compliance

Protected Health Information (PHI) is defined as any demographic information which could be used to identify a patient or client of a *covered entity* (a HIPAA-regulated entity). Examples include a patient's name, date of birth, address, telephone number, email, social security number, medical diagnoses, test results, and health insurance details. Any information classified as PHI is protected by HIPAA. It must be kept confidential and cannot be disclosed to unauthorized parties without the patient's consent.

HHS lists the following as protected under HIPAA:

- Information doctors, nurses, and other health care providers put in the medical record

- Conversations a doctor has about patient care or treatment with nurses and others

- Patient information in the health insurer's computer system

- Patient billing information at the clinic

- Most other health information about patients held by those who must follow these laws

In certain situations, HIPAA allows covered entities to use and disclose PHI *without obtaining permission* from individuals:

- Disclosure to the individual (if the information is required for access or accounting of disclosures, the covered entity *must* disclose to the individual)
- Treatment, payment, and healthcare operations
- Opportunity to agree or object to the disclosure of PHI
    - An entity can obtain informal permission by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object
- Incident to an otherwise permitted use and disclosure
- Limited dataset for research, public health, or healthcare operations
- Public interest and benefit activities—The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, for *12 national priority purposes*:

1. When required by law
2. Public health activities
3. Victims of abuse or neglect or domestic violence
4. Health oversight activities
5. Judicial and administrative proceedings
6. Law enforcement
7. Functions (such as identification) concerning deceased persons
8. Cadaveric organ, eye, or tissue donation
9. Research, under certain conditions
10. To prevent or lessen a serious threat to health or safety
11. Essential government functions

12. Workers' compensation

In such cases, healthcare professionals are required to sign a confidentiality and nondisclosure agreement stating they understand and will abide by HIPAA regulations.

Who is Obligated to Maintain Patient Confidentiality

In 2000, HHS published the HIPAA *Privacy Rule*, a federal law which set national standards for the protection of individually identifiable health information by covered entities. It also set standards for individuals' rights to understand and control how their health information is used.

According to HHS, covered entities are those which must follow HIPAA regulations. These entities are categorized into three types: health plans, health care clearinghouses, and most health care providers.

Health plans include health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid. The CDC notes an exception, wherein a group health plan with fewer than 50 participants that is administered solely by the employer that established and maintains the plan is *not a covered entity*.

Health care clearinghouses are entities that receive nonstandard health information from another entity and process it into a standard electronic format (or data content), or vice versa.

Health care providers (including doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists) who provide patient care and/or process standard health care transactions electronically (such as electronic billing of health insurance) must abide by HIPAA regulations.

In 2003, HHS published the HIPAA *Security Rule*, which sets national standards for protecting the confidentiality, integrity, and availability of *e-PHI* (Electronic Protected Health Information, meaning PHI that is transmitted, stored, or accessed electronically). Information shared verbally or in writing is not covered under the Security Rule. HHS provides organizations with a *Security Risk*

Assessment Tool to help them understand security regulations and provide guidance in assessing risk and implementing protocols.

The HIPAA *Breach Notification Rule* requires covered entities *and* their business associates to provide notification following a breach of unsecured protected health information. A *breach* is defined as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.

Business Associates are outside persons and companies that are not employees of a covered entity but whom need to have access to patients' health information when providing services to the covered entity. HHS gives the following examples:

- Billing companies and companies that process health care claims
- Companies that help administer health plans
- Outside lawyers, accountants, and IT specialists
- Companies that store or destroy medical records

According to HHS, "covered entities must have contracts in place with their business associates, ensuring that they use and disclose health information properly and safeguard it appropriately. Business associates must also have similar contracts with subcontractors. Business associates (including subcontractors) must follow the use and disclosure provisions of their contracts and the Privacy Rule, and the safeguard requirements of the Security Rule."

Organizations that *do not have to follow* the Privacy and Security Rules include:

- Life insurers
- Employers
- Workers' compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies

- Many municipal offices

Penalties for Non-compliance with HIPAA Requirements

According to HHS, “since 2003, OCR's enforcement activities have obtained significant results that have improved the privacy practices of covered entities. The corrective actions obtained by OCR from covered entities have resulted in systemic change that has improved the privacy protection of health information for all individuals they serve”.

Complaints of possible HIPAA violations are investigated by the OCR. When entities are found to be non-compliant, they may voluntarily make changes to resolve the issue. They may also be required by OCR to take specific corrective actions. These include revision of existing policies, development and implementation of new policies and procedures, creation of new HIPAA-compliant documents or PHI safeguards, modification of workspaces, equipment installation, and employee training.

Aside from undergoing disciplinary action, non-compliant entities can also face civil monetary or criminal penalties. If a civil violation is not corrected within 30 days, fines range from $100 to $50,000 per violation (up to $25,000 annually for repeat violations), as determined by the HHS secretary. Covered entities may be directed to issue refunds to individuals for inappropriate billing transactions.

A civil violation deemed as willful neglect that is corrected within the required time has a penalty of $10,000 to $50,000 per violation (up to $250,000 annually for repeat violations). If willful neglect is not corrected within the required time, the penalty is $50,000 per violation, with an annual maximum of $1.5 million.

Complaints that could involve a criminal violation are referred to the Department of Justice for investigation. Deliberate PHI disclosure has a penalty of up to $50,000 with imprisonment for up to a year, and offenses committed under false pretenses have penalties of up to $100,000 fine, with up to 5 years’ imprisonment. Selling (or the intent to sell) PHI for commercial advantage

personal gain, or for malicious purposes can lead to fines of up to $250,000 with imprisonment for up to 10 years.

Employee Snooping is the Most Common Cause of HIPAA Security Breaches

A study asked healthcare providers about the security breaches their organizations had suffered, with 70% of the survey respondents claiming to have experienced at least one security breach. 35% of those respondents attributed the breaches to unauthorized access by employees.

Snooping was the largest single cause of exposure of patient health information according to the survey with 27% of having experienced a breach when an employee viewed medical records of friends and family, while 35% occurred when employees checked the medical records of their work colleagues.

The survey was conducted on medium to large healthcare organizations; however, there is no reason to suggest that small healthcare organizations do not suffer data breaches of a similar nature.

Employee Snooping is a HIPAA Violation

Accessing of patient records without authorization may not make headline news, but the breach is still likely to be reported and could potentially trigger an investigation by the Office for Civil Rights (OCR). There have been documented cases where covered entities have incurred a HIPAA violation financial penalty even when only one or two individuals' PHI has been accessed without authorization or when the individuals' rights under HIPAA have been violated.

Generally, covered entities should report snooping to the OCR and must communicate the breach to the individual(s) whose records were accessed, unless it is established that the employee accessed the records in good faith and within the scope of the workforce member's authority, or the records were accessed by accident.

All patient records must be protected, and the appropriate administrative, technical and physical safeguards must be employed to keep all PHI secure and away from prying eyes. While it may not be possible to prevent unauthorized accessing of medical records in all cases, a monitoring system should be in place and access logs should be regularly reviewed to ensure that if PHI is accessed by an unauthorized individual, rapid action can be taken to limit the harm caused and

prevent further records from being accessed. All too often employees are discovered to have accessed health records, without authorization, multiple times over a period of several months or years before the snooping is identified.

Meaningful Use

One of the most significant advancements in healthcare is the use of electronic health records (EHRs). The U.S. government introduced the Meaningful Use program as part of the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, to encourage health care providers to show "meaningful use" of a certified EHR. In doing so, eligible providers who do so receive incentive payments. The overall goal of the Meaningful Use program is to promote the widespread adoption of electronic health records systems, ultimately creating an infrastructure that improves the quality, safety, and efficiency of patient care in the United States. Meaningful Use means that electronic health record technology is used in a "meaningful" way and that it ensures health information is shared and exchanged to improve patient care. According to the CDC, there are five "pillars" of health outcomes that support the concept of Meaningful Use:

- Improving quality, safety, and efficiency while reducing health disparities
- Engaging patients and families
- Improving care coordination
- Improve public health
- Ensure privacy for personal health information

Steps Healthcare Organizations Can Take to Prevent Snooping

Organizations compliant with Meaningful Use must ensure that the ePHI of patients is secured. HIPAA also requires the implementation of adequate physical, administrative, and technical safeguards to protect electronic health data. The starting point for assessing security risks in an organization is to conduct a Privacy and Security Audit. Only by thoroughly assessing all IT systems, procedures and policies can potential security threats be identified and eliminated. **When a Privacy and Security Audit is conducted, healthcare organizations must complete a four-step procedure as detailed below:**

1. Conduct a full risk analysis of all IT systems.
2. Review and update risk management policies and procedures.
3. Devise an employee sanction policy following HIPAA breaches and ensure it is communicated to all staff.
4. Ensure logins and data access are logged and access logs are checked regularly; any irregularities found must be investigated promptly.

If individual employees are required to have access to patient health records in order to perform their duties, there is little that can be done to prevent those individuals from accessing such data. It is therefore essential for the staff to be advised of their obligations under Meaningful Use and HIPAA and be informed of the consequences of accessing ePHI without authorization.

Case Study continued:

Will met with Lisa to see if and why she looked at Jim's PHI. Lisa admitted to looking at Jim's PHI. She said that she was just trying to be a good supervisor to see if she could help and support Jim. It was confirmed that Lisa had completed her annual HIPAA competency training three months before the incident. Following the investigation of the incident, Jim was notified that a breech had occurred with his PHI. The breech was reported to the OCR. The results of the investigation were submitted to Human Resources for appropriate action. According to the healthcare systems "zero-tolerance" policy on violating HIPPA, Lisa's employment with the healthcare system was terminated.

Examination Questions: (Score of 80% is required for passing)

1. The most common cause of a HIPPA security breach is?
   a. Snooping on co-worker or family member.
   b. A mis-directed fax.
   c. Posting PHI on social media.
   d. Talking to co-workers in a public place about PHI.
2. Protected Health Information (PHI) protected under HIPPA includes, but is not limited to:
   a. The patient's name, address, telephone number, age, diagnosis, surgery, date of procedure and medications.
   b. Any medical history information, results of physical examinations, laboratory and other diagnostic results.
   c. Billing records and claim forms. Any information that could be used to identify the patient.
   d. All of the above.
3. What could happen to a covered entity if it violates HIPPA regulations:
   a. Disciplinary Action and Termination.
   b. Civil Penalties.
   c. Criminal Penalties.
   d. All of the above.
4. What government agency enforces HIPPA?
   a. CLIA
   b. CMS
   c. FDA
   d. OCR
5. A phlebotomist working at a blood collection center calls out in a busy waiting room "Ms. Smith, I'm ready to draw your blood for your lithium level."
   Is this a HIPPA Violation or Acceptable Practice?
   Yes or No

Violation: There was no need to announce the name of the test. This is a violation of the patient's privacy.

References:

Centers for Medicaid & Medicare Services (CMS) (2012). HIPAA - General Information. Updated August 23, 2012 from: http://www.cms.gov/Regulations-andGuidance/HIPAAAdministrativeSimplification/HIPAAGenInfo/index.html?redirect=/hipaaGenInfo/

Hartman's Complete Guide for the Phlebotomy Technician (2020) page 9

Department of Health and Human Services. HIPAA for Professionals. Updated May 17, 2021 from: https://www.hhs.gov/hipaa/for-professionals/index.html

Department of Health and Human Services. Your Rights Under HIPAA. Updated January 19, 2022 from: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

Department of Health and Human Services. Case Examples. Updated June 7, 2017 from: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html

Compliancy Group. What is HIPAA Compliance? ©2022 from: https://compliancy-group.com/what-is-hipaa-compliance/

Centers for Disease Control. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Updated June 27, 2022 from: https://www.cdc.gov/phlp/publications/topic/hipaa.html

American Medical Association. HIPAA Violations and Enforcement. © 19915 – 2022 from: https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

athenahealth. What is Meaningful Use? from: https://www.athenahealth.com/knowledge-hub/practice-management/what-is-meaningful-use/what-is-meaningful-use#:~:text=The%20U.S.%20government%20introduced%20the,Electronic%20Health%20Record%20(EHR)

RegisteredNursing.org. What is Meaningful Use? from: https://www.registerednursing.org/articles/meaningful-use/

Survey

1. What category best describes your title or position? Select all that apply.

   - o Medical/Technical (CLS/MLS/MT, MLT, lab, or medical personnel)
   - o Non-Medical/Technical (lab administrative staff)
   - o Supervisor/Manager (Medical/Technical)
   - o Phlebotomist (CPT)
   - o Other (please specify): _____

2. Rate your expertise in this subject matter prior to this presentation.

   - o None
   - o Poor
   - o Fair
   - o Good
   - o Excellent

3. To what extent were the learning objectives achieved?

   - o Describe what HIPAA is and what portion of the law applies to their role in the healthcare system.
     Poor o Fair o Good o Excellent o
   - o Identify who is obligated to maintain patient confidentiality.
     Poor o Fair o Good o Excellent o
   - o Identify what type of patient communication and information sharing requires compliance under HIPAA.
     Poor o Fair o Good o Excellent o
   - o Describe what PHI is and why it is important.
     Poor o Fair o Good o Excellent o
   - o Understand the most common cause of a HIPPA violation.
     Poor o Fair o Good o Excellent o
   - o Describe the penalties for non-compliance with HIPAA requirements.
     Poor o Fair o Good o Excellent o

4. How would you rate the quality of the presentation?

- o Poor
- o Fair
- o Good
- o Excellent

5. Do you feel there was any commercial bias or service promoted in this presentation?

- o Yes
- o No

6. Please provide us with any additional comments you may have.

_____

_____

_____