PREPARED BY MICHELLE BROOMFIELD RN

**PURPOSE**

The purpose of this course is to review Health Insurance Portability and Accountability Act (HIPAA) and the recommended practices within the workplace, to educate and reinforce the knowledge of nurses; ARNP, RN, LPN and CNA/HHA who are working in the health care environment, as well as other students, individuals regarding Health Insurance Portability and Accountability Act (HIPAA).

**OBJECTIVES/ Goals:**

After successful completion of this course the students will be able to:

1. Define Health Insurance Portability and Accountability Act (HIPAA)
2. Discuss the purpose for Health Insurance Portability and Accountability Act (HIPAA)
3. Describe Confidentiality of patients' information
4. Discuss Protected Health Information (PHI)
5. Discuss the use of computerized documentation systems
6. Describe practices that protect the security of electronic Protected Health Information
7. Describe the responsibility of the HHS' Office for Civil Rights

## HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The Health Insurance Portability and Accountability Act (1996) is a Federal regulation which requires healthcare providers, healthcare plans, healthcare clearing houses and other entities to make sure that the privacy, protection and security of the patient medical information is maintained.

Confidentiality of patients' information
HIPAA violations involves both civil and criminal penalties which include fines and imprisonment. The fines can range from $100 for each violation of the law to a limit of $25,000 per year for multiple violations. For misusing or disclosing any of the patient's information, criminal sanctions carry fines of 50,000 to 250,000 and one to ten years imprisonment.

Always maintain confidentiality of patients' information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules:

The Office for Civil Rights enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

The HIPAA Privacy Rule provides Federal protections for individually identifiable health information held by covered entities and their business associates and give the patient an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it allows the disclosure of health information needed for patient care and other important purposes.

**Protected Health Information (PHI)**

The HIPAA Privacy Rule protects most individually identifiable health information held or transmitted by a covered entity or its business associate, in any form; electronic, on paper, or oral. The Privacy Rule calls this information protected health information (PHI). Protected health information is information, including demographic information, which relates to:

- the person's present, past, or future physical, mental health or condition,
- the provision of health care to the individual, or
- the present, past, or future payment for the provision of health care to the individual, and that identifies the person or for which can be used to identify the individual.

Protected health information includes many common identifiers such as name, address, Social Security Number, date of birth when they can be associated with the health information.

A medical record, hospital bill or laboratory report, would be Protected health information because each document would contain a patient's name and the other identifying information associated with the health data content.

Some of HIPAA's privacy and security protections for health information includes the following:

- Allows patients to ask for a copy of their electronic medical record in an electronic form,
- Allows patients to instruct their provider not to share information about their treatment with their health plan when they pay by cash,
- Reduces burden by streamlining individuals' abilities to authorize the use of their health information for research purposes, and
- Clarifies that genetic information is protected under the HIPAA Privacy Rule and prohibits most health plans from using or disclosing genetic information for underwriting purposes.

## CONFIDENTIALITY

Confidentiality is defined as a set of rules or a promise that limits access or place restrictions on certain types of information. Within the health care setting, confidentiality is a major issue in patient/resident care. Certified nursing assistants as well as everyone who works with the patient has to maintain confidentiality of patient information. For example: you cannot talk about the patient with others who are not working with the patient and you cannot leave patient's chart at the bedside for unauthorized personnel to view. Legally, you can be fined or imprisoned; if you talk about the patient or share patient information. HIPAA laws must be followed and maintained.

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. To date, the implementation of HIPAA standards has increased the use of electronic data interchange. Provisions under the Affordable Care Act of 2010 will further these increases and include requirements to adopt:

- operating rules for each of the HIPAA covered transactions
- a unique, standard Health Plan Identifier (HPID)
- a standard and operating rules for electronic funds transfer (EFT) and electronic remittance advice (RA) and claims attachments.

In addition, health plans will be required to certify their compliance. The Act provides for substantial penalties for failures to certify or comply with the new standards and operating rules.

## Uses and Disclosures for Treatment, Payment, and Health Care Operations

The HIPAA Privacy Rule establishes a foundation of Federal protection for personal health information, carefully balanced to avoid creating unnecessary barriers to the delivery of quality health care. As such, the Rule generally prohibits a covered entity from using or disclosing protected health information unless authorized by patients, except where this prohibition would result in unnecessary interference with access to quality health care or with certain other important public benefits or national priorities.

Ready access to treatment and efficient payment for health care, both of which require use and disclosure of protected health information, are essential to the effective operation of the health care system. In addition, certain health care operations—such as administrative, financial, legal, and quality improvement activities—conducted by or for health care providers and health plans, are essential to support treatment and payment. Many individuals expect that their health information will be used and disclosed as

necessary to treat them, bill for treatment, and, to some extent, operate the covered entity's health care business.

To avoid interfering with an individual's access to quality health care or the efficient payment for such health care, the Privacy Rule permits a covered entity to use and disclose protected health information, with certain limits and protections, for treatment, payment, and health care operations activities.

**How the Rule Works**

**Treatment, Payment, and Health Care Operations**

The core health care activities of Treatment, Payment, and Health Care Operations are defined in the Privacy Rule at 45 CFR 164.501.

- Treatment generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

- Payment encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:

  - Determining eligibility or coverage under a plan and adjudicating claims;

  - Risk adjustments;

  - Billing and collection activities;

  - Reviewing health care services for medical necessity, coverage, justification of charges, and the like;

  - Utilization review activities; and

  - Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

- Health care operations are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities, which are limited to the activities listed in the definition of “health care operations” at 45 CFR 164.501, include:

  - Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;

  - Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;

  - Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims

  - Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;

  - Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and

  - Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. General Provisions at 45 CFR 164.506.

A covered entity may, without the individual's authorization:

- Use or disclose protected health information for its own treatment, payment, and health care operations activities. For example:

  - A hospital may use protected health information about an individual to provide health care to the individual and may consult with other health care providers about the individual's treatment.

  - A health care provider may disclose protected health information about an individual as part of a claim for payment to a health plan.

  - A health plan may use protected health information to provide customer service to its enrollees.

A covered entity may disclose protected health information for the treatment activities of any health care provider (including providers not covered by the Privacy Rule). For example:

  - A primary care provider may send a copy of an individual's medical record to a specialist who needs the information to treat the individual.

  - A hospital may send a patient's health care instructions to a nursing home to which the patient is transferred.

- A covered entity may disclose protected health information to another covered entity or a health care provider (including providers not covered by the Privacy Rule) for the payment activities of the entity that receives the information. For example:

  - A physician may send an individual's health plan coverage information to a laboratory who needs the information to bill for services it provided to the physician with respect to the individual.

  - A hospital emergency department may give a patient's payment information to an ambulance service provider that transported the patient to the hospital in order for the ambulance provider to bill for its treatment

A covered entity may disclose protected health information to another covered entity for certain health care operation activities of the entity that receives the information if:

- Each entity either has or had a relationship with the individual who is the subject of the information, and the protected health information pertains to the relationship; and

- The disclosure is for a quality-related health care operations activity (i.e., the activities listed in paragraphs (1) and (2) of the definition of "health care operations" at 45 CFR 164.501) or for the purpose of health care fraud and abuse detection or compliance. For example: A health care provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, provided that the health plan has or had a relationship with the individual who is the subject of the information.

- A covered entity that participates in an organized health care arrangement (OHCA) may disclose protected health information about an individual to another covered entity that participates in the OHCA for any joint health care operations of the OHCA. For example:

- The physicians with staff privileges at a hospital may participate in the hospital's training of medical students. Uses and Disclosures of Psychotherapy Notes. Except when psychotherapy notes are used by the originator to carry out treatment, or by the covered entity for certain other limited health care operations, uses and disclosures of psychotherapy notes for treatment, payment, and health care operations require the individual's authorization. See 45 CFR 164.508(a)(2).

**Minimum Necessary**

A covered entity must develop policies and procedures that reasonably limit its disclosures of, and requests for, protected health information for payment and health care operations to the minimum necessary. A covered entity also is required to develop role-based access policies and procedures that limit which members of its workforce may have access to protected health information for treatment, payment, and health care operations, based on those who need access to the information to do their jobs. However, covered entities are not required to apply the minimum necessary standard to disclosures to or requests by a health care provider for treatment purposes.

## CONSENT

A covered entity may voluntarily choose, but is not required, to obtain the individual's consent for it to use and disclose information about him or her for treatment, payment, and health care operations. A covered entity that chooses to have a consent process has complete discretion under the Privacy Rule to design a process that works best for its business and consumers. A "consent" document is not a valid permission to use or disclose protected health information for a purpose that requires an "authorization" under the Privacy Rule (see 45 CFR 164.508), or where other requirements or conditions exist under the Rule for the use or disclosure of protected health information.

## RIGHT TO REQUEST PRIVACY PROTECTION

Individuals have the right to request restrictions on how a covered entity will use and disclose protected health information about them for treatment, payment, and health care operations. A covered entity is not required to agree to an individual's request for a restriction, but is bound by any restrictions to which it agrees. See 45 CFR 164.522(a). Individuals also may request to receive confidential communications from the covered entity, either at alternative locations or by alternative means. For example, an individual may request that her health care provider call her at her office, rather than her home. A health care provider must accommodate an individual's reasonable request for such confidential communications. A health plan must accommodate an individual's reasonable request for confidential communications, if the individual clearly states that not doing so could endanger him or her. See 45 CFR 164.522(b).

# NOTICE

Any use or disclosure of protected health information for treatment, payment, or health care operations must be consistent with the covered entity's notice of privacy practices. A covered entity is required to provide the individual with adequate notice of its privacy practices, including the uses or disclosures the covered entity may make of the individual's information and the individual's rights with respect to that information.

## COMPUTERIZED DOCUMENTATION SYSTEMS

Computerized documentation systems often incorporate nursing diagnoses into the system, which produces lists of interventions and expected outcomes. More institutions are utilizing computerized systems for documentation. These computerized systems however vary from one facility to another; however security is a common factor for all systems.

Training has to be provided for the staff, which usually includes:

- Securing patient information from unauthorized persons whether the computer is at the nurses' station or at the bedside,
- Security of password information; no one is allowed to share their password with their co-worker etc.

Computer systems usually track the use of the system, therefore it is documented who is logged on and time and date.

There has to be training regarding how to correct errors when an entry error is made.

Computerized documentation systems have many advantages, including but not limited to:

- Eliminates handwritten orders,
- The records are legible; no need to worry about unclear handwriting,
- Enters signatures automatically,
- Security of patient information; need password to log in to access patient information,
- Orders can be automatically transmitted to pharmacy and medication is ordered quickly,
- Reduction in errors,
- Prevents tampering of the medical record,
- Difficult to delete information from the record.

Computerized documentation systems may include:

**Electronic medical record (EMR)**

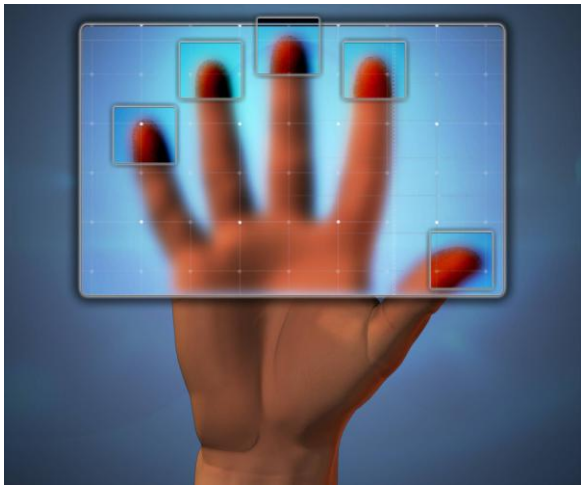
Electronic medical record is the computerized patient medical record. With the use of the computerized documentation system, computer terminals may be located in the patient's room, therefore healthcare providers / workers, professionals have to be educated/ trained regarding the importance of logging off the computer system so that persons who are not authorized will not be able to access and view the patient's information. The computerized documentation system usually has computerized physician order entry, clinical decision support system; therefore the notes can be entered electronically.

**Clinical decision support system (CDSS)**

Clinical decision support system refers to the interactive software systems which has evidence based medical information. Clinical decision support system can be used for different purposes such as providing diagnosis and treatment options when the symptoms are imputed into the computer system. Clinical decision support system may also monitor the orders and the treatments to prevent repetitions or duplications.

**Computerized physician or provider order entry (CPOE)**

Computerized physician or provider order entry (CPOE) refers to the interactive software application that automates ordering for medications or treatments. Orders must be entered in a prompted format that eliminates many errors. These systems usually include Clinical decision support system to provide alerts if there is an inaccurate dose or duplication order. Computerized physician or provider order entry eliminates handwritten orders and the information is automatically transmitted to the pharmacy, reducing errors and medication is ordered quickly.



# OFFICE FOR CIVIL RIGHTS (OCR)

On July 27, 2009, the Secretary of Health and Human Services (HHS) delegated to the Director of Office for Civil Rights (OCR) the authority to administer and enforce the HIPAA Security Rule. This action by Secretary Sebelius was expected to improve HHS' ability to protect individuals' health information by combining the authority for administration and enforcement of the Federal standards for health information privacy and security called for in the HIPAA legislation.

The transition of authority for the administration and enforcement of the Security Rule from the Centers for Medicare & Medicaid Services (CMS) was seamless with no interruption in the management or processing of any complaints filed prior to the

transition. New security complaints should be sent directly to the Office for Civil Rights (CMS 2013).

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security.

At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information (CMS 2013).

# HIPAA ENFORCEMENT

Health and Human Services (HHS) Office for Civil Rights is responsible for enforcing the Privacy and Security Rules. Enforcement of the Privacy Rule began April 14, 2003 for most HIPAA covered entities. Since 2003, OCR's enforcement activities have obtained significant results that have improved the privacy practices of covered entities. The corrective actions obtained by Office for Civil Rights from covered entities have

resulted in systemic change that has improved the privacy protection of health information for all individuals they serve.

# ENFORCEMENT PROCESS

**Office for Civil Rights enforces the Privacy and Security Rules in several ways:**

- by investigating complaints filed with it,
- conducting compliance reviews to determine if covered entities are in compliance, and
- performing education and outreach to foster compliance with the Rules' requirements.

OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA.

# BIBLIOGRAPHY

Florida Board of Nursing (2014) Licensing and Registration. Retrieved from http://floridasnursing.gov/licensing/

Florida Board of Nursing (2015). Certified Nursing Assistant (CNA). Retrieved from http://floridasnursing.gov/renewals/certified-nursing-assistant/

Florida Department of State. (2010) Florida Administrative Code and Administrative Registry. Division 64B9 Board of Nursing. Retrieved from https://www.flrules.org/gateway/Organization.asp?OrgNo=64b9

Florida Statues (2014) Chapter 456 HEALTH PROFESSIONS AND OCCUPATIONS: GENERAL PROVISIONS Retrieved from http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0400-0499/0456/0456.html

Florida Statues (2014) Chapter 464 Title XXXII Regulations of Professions and Occupations, Nursing, Nurse Practice Acts, Certified Nursing Assistant. Retrieved from http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0400-0499/0464/0464.html

HHS.gov. (2015) Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#protected

Lippincott Nursing Center (2010) The Legalities of Nursing Documentation. Retrieved from http://www.nursingcenter.com/journalarticle?Article_ID=959265

U.S. Department of Health and Human Services (2015) Health Information Privacy. Retrieved from http://www.hhs.gov/ocr/privacy/

www.cms.gov (2013) HIPAA General Information. Retrieved from https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/index.html?redirect=/hipaageninfo

www.cms.gov (2016) Medical Privacy of Protected Health Information. Retrieved from https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/SE0726FactSheet.pdf

www.cms.gov (2013) Privacy and Security Standards. Retrieved from https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/PrivacyandSecurityStandards.html