Health Insurance Portability and Accountability Act (HIPAA)
What is HIPAA?

- The acronym HIPAA stands for the Health Insurance Portability and Accountability Act. It requires “covered entities” to protect the privacy and security of individuals’ personal health information.

- This means that individually identifiable information about a person’s physical or mental health or healthcare in any written or oral form—including computer records—is protected from unauthorized disclosure.

- The law provides regulations on privacy of health information, security of health information, notification of breaches of confidentiality, penalties for violating HIPAA.
Since more and more health information is being computerized, many people are concerned that they might be losing control over their personal health information. In some cases, before HIPAA was enacted, physicians, pharmacies, and pharmaceutical companies were guilty of breaches of confidentiality.

In an effort to allay these fears, federal rules governing the use and disclosure of health information were enacted under HIPAA. HIPAA is a civil rights law which gives the patient control over the use of their health information. As of April 2003 all healthcare providers across the nation are required to comply with it.
HIPAA imposes restrictions on the use and disclosure of protected health information. It gives patients greater protection of their medical records and provides them with greater peace of mind regarding the security of their information.

It also means that a healthcare worker has obligations to protect a patient’s protected health information and can only release it in very specific circumstances.

After HIPAA was passed, the Department of Health and Human Services issued two separate regulations referred to as the Privacy Rule and the Security Rule.
The Privacy and Security Rules require healthcare providers to adopt processes and procedures to protect patient confidentiality. These processes include administrative, physical, and technical safeguards to ensure that medical information is stored, transmitted, and received in a secure manner.

HIPAA regulations are broad in scope and affect many entities that have access to personal health information. These include hospitals, medical practices, radiologists, pharmacies, insurance companies, healthcare clearinghouses, and business associates such as auditors, lawyers, consultants, data and billing firms, and others covered entities work with.
Covered Entities

- HIPAA regulations discuss covered entities. The term covered entities in this case means healthcare providers or business associates who transmit any health information in connection with carrying out healthcare-related financial or administrative activities.
- These entities are required to establish policies and procedures addressing the use and disclosure of protected health information.
Disclosure

- The term disclosure means revealing information to someone outside the healthcare entity holding the information. That means HIPAA does not ban an employee of a covered entity from revealing information to his or her supervisor or to another management official who has a need to know.

- Here are several additional definitions that are important to know when discussing HIPAA and its requirements. They are follows:
  - **Privacy**: this is defined as the state of being concealed or secret.
  - **Confidentiality**: defined as that which contains secret information such as a medical record. When a patient provides their personal information to you, the healthcare provider, they should be able to do so without fear of anyone other than those involved in their care finding out their personal health information.
Disclosure cont.

- **Authorization**: this term means giving permission for or to grant power to someone. For example, an individual could grant authorization for a spouse or adult child to have access to their medical information.
PHI

- Information protected under the regulation is referred to as protected health information, or PHI. When a patient gives personal health information to a healthcare provider it becomes PHI. The Privacy and Security Rules protect individually identifiable health information transmitted or maintained by a covered entity no matter what form it takes.

- PHI is any individually identifiable health information including anything:
  - Created or received by a healthcare provider, health plan, or healthcare clearinghouse.
  - Relating to the past, present, or future physical or mental health or condition of an individual including information related to payment for healthcare.
  - Transmitted in any form or medium—paper, electronic, and verbal communications.
PHI cont.

- Information is protected if it directly or indirectly identifies someone.
  - Direct identifiers include individual’s name, Social Security number, driver’s license numbers, etc.
  - Indirect identifiers include information about an individual that can be matched with other available information to identify the individual

- Individually identifiable health information includes demographic information such as the following unique identifiers:
  - Name
  - Address
  - Date of Birth/Admission/Discharge/Death
  - Telephone
  - Email address
  - Medical record
  - Health plan number
  - Social Security Number
  - Account Number
  - Photographic images
  - Financial information
These identifiers provide information by which the identity of a patient can be determined with reasonable accuracy and speed, either directly or by reference to other publicly available information. If any direct or indirect identifiers are present, the information is PHI and subject to HIPAA protection.
How HIPAA Protects PHI

- HIPAA helps protect Protected Health Information (PHI) in several ways including:
  - Limiting who may use or disclose PHI.
  - Limiting the purposes for which PHI may be used or disclosed.
  - Limiting the amount of information that may be used or disclosed.
  - Requiring the use of safeguards over how PHI is used, stored, and disclosed.
Permitted Disclosure

There are some permitted uses for PHI. These are for treatment, payment, and healthcare operations and for specified public policy exceptions such as public health and law enforcement. Any other use requires individual written authorization.

**Treatment:** In the course of providing, coordinating, and managing healthcare, you may access PHI as needed to provide treatment. This includes:

- Direct treatment of patient.
- Consultation among healthcare providers.
- Indirect treatment (for example, laboratory testing).
- Patient referral from one provider to another.
Payment: If your job requires it, you may access relevant PHI during the course of activities to obtain reimbursement for healthcare. Activities covered by this include billing, eligibility or coverage determination, medical necessity determinations. Also allowed are activities by those working for a health plan in order to pay claims.
Permitted Disclosure cont.

- **Healthcare Operations:** If your job requires it, you may access PHI in the course of activities directly related to healthcare operations such as treatment and payment, credentialing, auditing, utilization review, quality assessment, and training programs. Other instances where you may access PHI, is when performing supporting activities, such as computer systems support or administrative and managerial activities, such as business planning, resolving complaints, and complying with HIPAA.
Minimum Necessary Rule

- The use or disclosure of PHI should be limited to the minimum amount necessary to perform a task. You must always ask yourself, what is the minimum amount of information needed to enable me to do my job?

- The only exception to this rule is with regard to treatment of a patient since knowing the entire patient history is important when making diagnoses and developing treatment plans. When it comes to treatment, you can access whatever information you need for treatment purposes.
Minimum Necessary Rule cont.

- When working with Protected Health Information (PHI), keep in mind the following:
  - Do not access PHI that you do not need
  - Do not discuss PHI with individuals who do not need to know it
  - Do not provide PHI to anyone not authorized to receive it
  - Leave records accessible to patients or others who do need to see them
Good Practice for Information Disclosure

- You should only share information with someone who needs to know that information to perform their job. Never discuss personal health information in public areas such as cafeterias or elevators.
- Also, be careful when speaking so that others—including patient family members and friends—don’t overhear.
- Finally, only give the minimum amount of information necessary.
There are some exceptions to an individual giving written consent to disclose his or her health information. There are some specific circumstances where you are authorized to disclose PHI without patient permission. In these specific circumstances, you are protected as a whistleblower. Let’s look at some of these circumstances.

A covered entity’s employees or business associates may disclose protected health information to a public health authority (such as federal OSHA or a state agency operating under a federal OSHA-approved state plan that is authorized to investigate a covered entity’s conduct), to an attorney retained to deal with a case involving such conduct, or to a healthcare accrediting organization.
When Can PHI be Disclosed cont.

- These disclosures are permitted as long as the employee believes in good faith that the conditions he is reporting are unlawful or endanger employees, among other things.

- Employees who are crime victims may also disclose protected health information to a law enforcement official if the information is about the suspected perpetrator and the information is limited to that listed in the privacy regulation.

- Also, an employee may report a serious and imminent threat to the health and safety of a person if the recipient of the report is reasonably able to prevent or diminish the threat. Such recipients include law enforcement, OSHA, and union officials.
An employee is protected from retaliation for making disclosures authorized by HIPAA in connection with an occupational safety or health complaint.
Computer Safety

- You also have a responsibility to protect information stored electronically.
- You should always follow safe practices for your computer system ID and password. Always use a strong password. Password requirements may vary depending on your employer, but generally strong passwords contain a mix of numbers, symbols, and upper and lowercase letters.
- Remember, keep your user ID and password confidential and secure and don’t allow anyone else to access the computer system under your ID.
- Never leave the computer station unattended without locking it first.
Many security breaches occur as a result of phishing attempts. Phishing, a type of social engineering, is a high-tech scam that uses email to deceive individuals into disclosing personal information or unknowingly providing access to a computer or computer network.

By tricking just one person into opening an email and clicking on an attachment or a link, an attacker can succeed in gaining access to the entire network.

The two primary attack methods used with phishing emails are embedded hyperlinks and file attachments. These can be used by an attacker to install malware and direct users to bogus web sites.
To avoid or minimize the phishing threat, you must be able to recognize phishing attempts to avoid being scammed by them. There are some things which can help you identify phishing attacks and learn how to recognize and avoid malicious hyperlinks and attachments. These include:

- You don’t know the sender or the sender’s email address doesn’t match the “friendly” name displayed
- The email is not similar to what you have received from the sender in the past
- Includes a link or an attachment you weren’t expecting or that is out of context for the sender
Minimizing the Threat of Phishing cont.

- Includes information that may have been found on social media or refers to a current news event
- Immediate action is required
- Requests sensitive information about yourself or the Department
- Contains poor grammar, misspellings, and punctuation errors
Considerations for Materials Containing PHI

In addition to avoid phishing attempts, there are other commonsense precautions you can employ when dealing with materials that contain PHI.

Some of these precautions include the following:

◦ Do not unnecessarily print or copy PHI
◦ When faxing PHI, use a fax cover page
◦ Do not send PHI in email unless first cleared by your supervisor
◦ Dispose of PHI when it is no longer needed
◦ Use shredding bins for paper records
◦ When retiring electronic media used to store PHI, ensure the media is “cleansed” according to your employer’s IT Department standards
Since social media is such a big part of the way we communicate with friends and family today, it is sometimes easy to forget that it is a public forum and sharing any PHI is strictly prohibited.

Some tips to keep in mind when using social media include:
- Keep your personal social media accounts separate from any business ones that might be used in the workplace
- Don’t ‘friend’ patients
- HIPAA lists 18 personal identifiers including photos, neighborhoods, birth dates and vehicle identifiers so never post any of this information on social media as it relates to patients
Social Media cont.

- Even if a patient posts information pertaining to their own treatment, it doesn’t mean you can also share it or even re-share or retweet it.
- Never post photos of a patient on a social media site.
- If photos are taken at the workplace, ensure that no patient files or photos are visible.
- Report any breaches of privacy or confidentiality committed by a co-worker.
- Don’t refer to the patient in a disparaging manner, even if the patient is not identified.

Remember that even if you delete a post, it still exists on a server somewhere and would be discoverable in a court of law.
Consequences for PHI Breaches

- Misusing PHI can result in disciplinary action, legal penalties, or imprisonment, not to mention the loss of trust of the public.
- If a patient feels that their rights have been violated, they may complain to the Privacy Officer or to the Director of Health and Human Services.
Any complaint, breach or discovered violation can initiate mandatory investigations. Consequences for a HIPAA violation are:

- Disciplinary action up to and including termination of employment.
- Civil penalties of up to $1,500,000 per year per violation.
- Criminal penalties of up to $250,000, imprisonment of up to ten years, or both.
- Lawsuits for invasion of privacy or negligence.