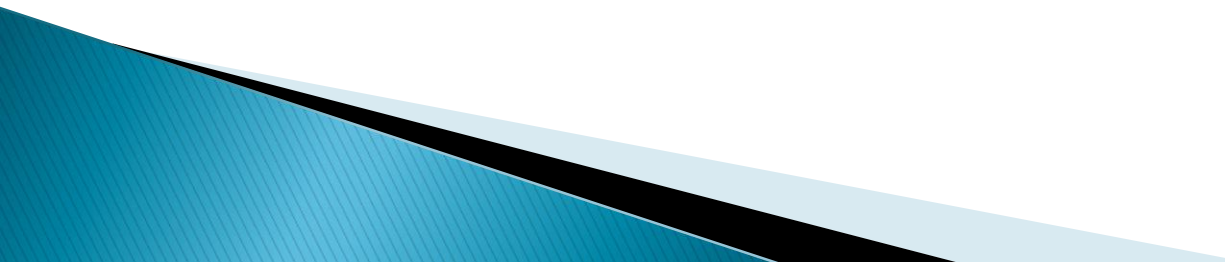


# Health Insurance Portability and Accountability Act (HIPAA)

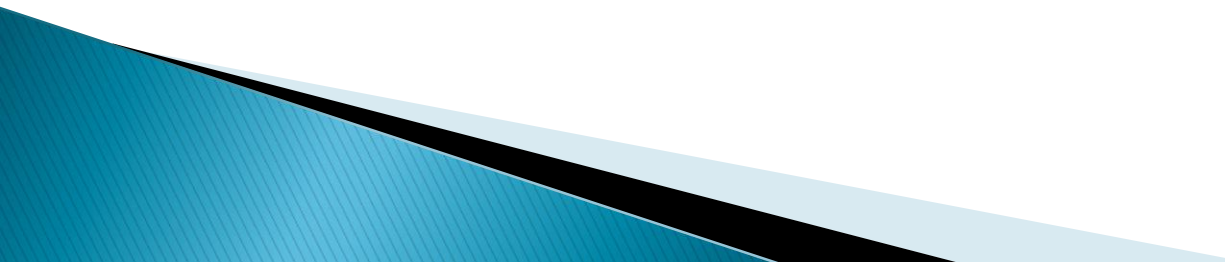
- ▶ This presentation contains important information about the laws and regulations that affect the healthcare industry, our organization and you.
- ▶ Upon completion of this course, you should:
  - Have a basic understanding of HIPAA - the law that protects patient health information

# Key Points: Health Insurance Portability and Accountability Act (HIPAA)

- ▶ HIPAA imposes penalties on covered entities and individuals who fail to keep patient information confidential in accordance with the law.
  - ▶ HIPAA's confidentiality rules fall under two main umbrellas:
    - *Privacy Rule*— grants individual rights with regard to their health information and imposes obligations on covered entities to protect all type of health information
    - *Security Rule*—requires covered entities to safeguard *electronic* health information
- 

# What is Protected Health Information (PHI)?

(PHI) is information that:

- Identifies or can be used to identify a specific individual
  - Relates to the individual's health, health care, or payment for care (past, present, or future) is protected.
  - Includes personal information like name, date of birth etc.
  - Includes information relating to diagnosis and/or method of injury
- 

# What questions might patient's ask about their PHI?

- How will my PHI be used?
  - The hospital may use or disclose your information for treatment, payment, or healthcare operations and when specifically permitted or required by law. The Notice of Privacy Practices describes these uses and disclosures in more detail. Any other releases require your authorization.
- How will the hospital limit the use of my PHI?
  - The hospital only permits those employees who have a need to know to access your health information. For example, clinicians who are treating you are allowed to access your information. Billing clerks are allowed to access your information to submit claims for payment.

## *What questions might patient's ask about their PHI?*

- How will the hospital prevent someone else from accessing my PHI?
  - All hospital computers are password protected and have other safeguards. Paper with sensitive information must be filed in the patient record or placed in a secure bin to be shredded. The Hospital also limits access to medical records and imposes disciplinary actions for inappropriate access.
- What are my rights as a patient?
  - Patients have many rights under HIPAA, including the right to request access to their medical record, an amendment to their medical record, and an accounting of the disclosures that have been made.

# Key Points: PHI

- PHI includes information in any format, including:
  - ✓ Spoken
  - ✓ Paper
  - ✓ Telephone
  - ✓ Electronic
  - ✓ Mail
  - ✓ Fax
- In general, patients over 18 years of age have control over their PHI.
  - ✓ Parents have the right to access their minor children's health information (child under age 18). There are some exceptions to this rule, such as when the minor has the legal authority under state law to consent to certain health care services, or if the minor is emancipated.

# Key Points: PHI – Public Health Reporting

- ▶ The hospital may report PHI to meet state or federal law public health reporting requirements, without patient authorization. For example, the following types of reports are commonly required by state law:
  - ✓ Child Abuse or Neglect
  - ✓ Certain infectious diseases (such as HIV and TB)
  - ✓ Vital statistics – births and deaths
- ▶ \*Note that many reporting obligations are state law specific\*

# Minimum Necessary Rule

- ▶ When using or disclosing PHI, you should always follow the Minimum Necessary Rule:
  - ✓ The Minimum Necessary Rule means only accessing or disclosing PHI needed to do your job.
- ▶ Ask yourself:
  - ✓ Do I need to access this information for a work-related task I am assigned to do?
  - ✓ What is the minimum amount of information I need to get the job done? (Note: this question does not apply if the use is for treatment purposes)
- ▶ Remember: You may not access information that you do not have a business need to know. Access to PHI may be recorded, monitored and audited by the hospital.



# Incidental Disclosures

- ▶ In the course of routine communications, PHI may sometimes be mistakenly disclosed.
  - In a busy ER, a discussion between a patient and a doctor may be overheard by another patient. This is considered an incidental disclosure and is not a HIPAA violation, so long as reasonable safeguards were in place.
    - Safeguards include speaking with a lowered voice or using privacy curtains when available.
- ▶ Incidental disclosures should be minimized and PHI should never be discussed in public areas, such as elevators.

# Incidental Knowledge

- ▶ Friends/family may be hospitalized without your knowledge. Throughout your experience you may run across someone you know. If you find yourself in this situation, you may not disclose this to anyone without the patient's permission.
  - If you do not have the chance to ask permission or if the patient does not give you permission, you must keep this information to yourself.
- ▶ Although this rarely happens, it is a reality and one that must be addressed. Our patient's deserve the utmost privacy.

# Reasonable Or Not?

## Permissible Uses and Disclosures –

Reasonable	Not Reasonable
Two health care professionals speaking with lowered voices in a treatment area.	Talking loudly with a patient in a public area.
Access PHI to perform a job-related function	Reading a medical record for curiosity.
Sign-in sheet with only name and arrival time.	Discussing a patient's condition/background in a public area. This includes how/where they were injured or the specific types of injuries they have. This includes inside and outside the hospital.
	Alerting family/friends of a patient's admission to the hospital without the patient's permission.

# Key Points: Security

## ▶ Environment Security

- ✓ Paper containing PHI must either be filed in the correct record or placed in a secure, locked bin to be shredded.
- ✓ Computer screens should not be viewable by the public.

## ▶ Facility Security

- ✓ All employees and contractors should display a security badge while on hospital premises.
- ✓ All visitors must be accompanied by staff when in sensitive or restricted areas, such as Pediatrics, Nursery, Operating Room, or IT Department.
- ✓ Do not allow non-employees to follow you into sensitive or restricted locations.
- ✓ Do not hesitate or be afraid to question individuals not wearing a security badge or who appear suspicious.
- ✓ Do not hesitate to contact Security if you see any unusual or suspicious individuals or activities.

# Key Points: Reporting

- ▶ You should *always* feel empowered to report any privacy issues. Depending on your hospital policies, this may include:
  - ✓ Your direct supervisor
  - ✓ Human Resources
  - ✓ The Compliance Officer
  - ✓ The Privacy Officer
  - ✓ Hospital Legal Counsel
  - ✓ The anonymous Compliance Hotline
- ▶ There is a non-retaliation policy for reporting any complaint or concern in good faith.