HIPAA CONFIDENTIALITY & SECURITY
WHAT IS HIPAA?

• **Health Insurance Portability and Accountability Act.** The Privacy Rules were effective April 2003 and the Security Rules in April 2005.

• Established national standards for safeguarding the privacy and security of protected health information (PHI).

• Requires “covered entities” (health care providers, health insurers, and health care clearinghouses) to keep PHI confidential and secure.*

• Covered entities must inform each patient of all the possible uses and disclosures of their health information.

• Covered entities must inform each patient of their rights under HIPAA

* The American Recovery and Reinvestment Act of 2009 (ARRA) expanded the coverage to include other non-covered entities that handle PHI such as regional health information organizations, personal health record vendors, and others that electronically store or transmit PHI.
WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

• HIPAA definition of “individually identifiable health information”
  • Any subset of health information, including demographic information, that identifies the individual and…
    – Is created or received by a health care provider, health plan, or health care clearinghouse
    – Relates to the past, present, or future physical or mental health or condition of an individual.

Individually identifiable health information = Protected Health Information (PHI).
PRIVACY RULES

• In general, a covered entity may not use or disclose PHI unless it is for treatment, payment, or health care operation purposes. All other uses or disclosures require the patient’s authorization.

• The covered entity must provide the patient with a Notice of Privacy Practices (NPP) which details the many uses and disclosures that may occur with their health information.

• The NPP also must provide a description of the many rights that the patient has and how to exercise these rights.
USES AND DISCLOSURES OF PHI WITHOUT AUTHORIZATION

• Reporting required by law
  – suspected abuse, neglect, or domestic violence
  – certain types of wounds or injuries e.g. gunshot wounds
  – communicable diseases

• Court Orders (not subpoenas)

• Research

• Workers’ Compensation
PATIENT RIGHTS

• Inspect and/or request a copy of their PHI.
• Request restrictions on certain uses and disclosures of PHI.
• Receive confidential communications of PHI.
• Request amendments to PHI.
• Receive an accounting of disclosures of PHI.
SECURITY RULES

• Consists of administrative, physical, and technical requirements that are intended to safeguard the integrity, confidentiality, and availability of PHI.
  – Unique identifiers and complex passwords
  – Automatic log-offs
  – Encryption
  – Data back-up and disaster recovery
  – Proper disposal of computers and storage devices
CONFIDENTIALITY AGREEMENTS
• I will maintain the confidentiality of protected health information.

• I acknowledge that during the course of my work I will have access to protected health information and I will view and use it only as necessary to perform my job.

• I will not disclose protected health information except in accordance with policies and procedures.

• I agree not to disclose my personal password(s) used for entry to information systems.
• I agree not to enter any of the information systems under any other account name and password other than my own or to allow another person entry under my account name and password.

• I acknowledge that my access to and use of protected health information may be monitored and that my access privileges are subject to periodic review and revision.

• I acknowledge that my improper access or my improper disclosure of protected health information may result in disciplinary action up to and including termination from the program.

• I acknowledge that my obligations for confidentiality of protected health information under this agreement will continue after the termination of my education.
HOW DO YOU PROTECT PHI?

• Be aware of the policies of the entity where you have your clinical rotations.
• Keep all information confidential. Be aware of your surroundings and do not discuss patients in areas where others can overhear.
• If you are using patient cases in a class presentation, do not use patient identifiers of any kind e.g. name, birth date, address, etc.
• If you are allowed to make copies of information, ensure that all identifiers have been removed.
• Do not store any information on removable media such as thumb or flash drives.
• View and enter information only under your personal user ID and password. Log-off as soon as you have completed your work. Access only the information necessary to perform your assignments.
Mary-j Waterstraat, MPA, RHIA, CPC

HealthTeam Compliance and Privacy Officer
D130 West Fee Hall
355-1822