



# Introduction to HIPAA Privacy and Security Regulations

2006



# Course Objectives

- **Overview of HIPAA Privacy/Security Regulations**
- **Provide awareness training to assist you in complying with the regulations**
- **Provide information on how to report issues/concerns.**



HIPAA stands for

# **Health Insurance Portability and Accountability Act**

HIPAA requires covered entities to

- **Protect the Privacy of Health Information**
- **Provide Security for Health Information**



# **HIPAA: Privacy & Security of Patient Information**

## **What is Protected Health Information (PHI)?**

- PHI is individually identifiable information that is maintained or transmitted in any form.
- PHI is any information, verbal or recorded, relating to the health, healthcare or payment for health care provided.
- The information does not have to be created by your organization to be considered PHI.



# HIPAA: Privacy & Security of Patient Information

## REMEMBER

- PHI comes in many forms: **electronic, paper & verbal.**
- PHI is not limited to a patient's clinical information. It includes any information that can identify the patient.

Examples: Name, MRN, Address, SS#, Date of Birth,  
Billing Information, Photos, Telephone #



# HIPAA

## Organizational Responsibilities

Covered entities (providers, payers, clearinghouses) are allowed to use and/or disclose PHI in the normal course of providing treatment, payment and health care operations.

**Treatment** is the coordination of health care or other services.

**Payment** includes billing, claims management, medical necessity, utilization review activities, determination of coverage.

**Health Care Operations** includes quality improvement activities, credentialing, training, underwriting, compliance services, business planning and development, business management and general administration.



# HIPAA

## Organizational Responsibilities

### Notice of Privacy Practices

- A document given to each patient at the first point of service
- Details how provider uses, discloses and protects PHI for purposes of treatment, payment and health care operations
- Defines the patient's rights under HIPAA
- Explains how provider uses PHI for Marketing, Fundraising and Research
- Explains how to file a complaint with provider or with the Department of Health and Human Services



# HIPAA

## Organizational Requirements

### Business Associate Agreements

**Business associates are persons or organizations that**

- Perform a service on behalf of the provider
- The Service requires the use/disclosure of patient's Protected Health Information

**A Business Associate Agreement is required to assure that the business associate will protect and secure PHI as required by HIPAA standards.**



# **HIPAA Authorization**

- **Instances where Authorization is required:**
  - If a covered entity wants to use PHI for its own uses, or for uses by others (other than treatment, payment or healthcare operations)
  - In most instances, prior to disclosing information contained in psychotherapy notes
  - Most marketing communications using health information
- **Patients have a right to revoke their authorization at any time.**
- **Instances where Authorization is not required:**
  - Health oversight release
  - Law enforcement
  - Public health activities
  - Workers compensation



# **Incidental Disclosures**

**HIPAA does not prevent hospitals from using**

- **Whiteboards on hospital floors**
- **Sign-in sheets or calling patients by name at the clinic desks, or**
- **Leaving messages on patient's answering machine**



# HIPAA Guidance

Although providers are not required to eliminate all “incidental disclosures”

Providers must:

- Have reasonable, common sense policies and procedures, AND
- Apply the **minimum necessary** standard



# Minimum Necessary

- Employees must take reasonable efforts to access, use and disclose only the minimum amount of health information necessary to complete their job.
- Minimum necessary also applies to when we are requesting or disclosing information to another health care provider.
- **DOES NOT APPLY TO TREATMENT SITUATIONS.**

**Use Professional Judgment**

**Already a Standard Practice**



# HIPAA – Patient Rights

HIPAA gives specific rights to patients. These rights give patients more control over how their health information is used/disclosed.

- **Right to Access PHI-**

- ✓ A patient can request to review or obtain copies of their PHI.
- ✓ STATE LAWS and HIPAA govern the review and release of PHI.
- ✓ Patients requesting access to their records should be directed to **Medical Records Release of Information Department (ROI)**.

- **Right to Request Restrictions**

- ✓ A patient has the right to request restrictions on the use and disclosure of their PHI.
- ✓ Such requests will be reviewed on a case-by-case basis.
- ✓ HIPAA does not require the provider to accommodate all requests.



# **HIPAA – Patient Rights**

HIPAA gives specific rights to patients. These rights give patients more control over how their health information is used/disclosed.

- **Right to an Accounting of PHI Disclosures**
  - ✓ A patient has a right to an account of the disclosures of their PHI that the provider has made without an authorization.
  - ✓ There are exceptions for the accounting. Disclosures that will NOT be listed in the accounting include disclosures for treatment, payment, health care operations or PHI released with a signed authorization.
- **Right to Request an Amendment to PHI**
  - ✓ A patient has the right to request an amendment to their medical record.
  - ✓ Requests for amendments will be reviewed by a health care professional. In most cases this will be the physician responsible for the documentation.



# HIPAA – Patient Rights

HIPAA gives specific rights to patients. These rights give patients more control over how their health information is used/disclosed.

- **Right to Request Confidential Communications**

- ✓ A patient can request that we communicate with them by an alternate means or at an alternate location.
- ✓ Provider must accommodate reasonable requests for the communications. Examples might be requests that information be sent to a work address/phone # rather than a home address/phone #.

- **Right to File a Complaint**

- ✓ A patient has the right to file a complaint if they believe their privacy rights have been violated.
- ✓ **To file a complaint with the US Dept of Health and Human Services, Office of Civil Rights (OCR), call toll free 1-800-368-1019.**



# **HIPAA Security**

## **General Requirements**

- 1. Ensure confidentiality, integrity and availability of e-PHI.**
- 2. Protect against threats or hazards**
- 3. Protect against inappropriate uses or disclosures**
- 4. Ensure compliance by the workforce**



# Security Definitions

**Privacy** – Right of an individual to control personal information

**Confidentiality** – Only the right people see it and use it

**Integrity** – The information is what it is supposed to be, no unauthorized alteration or destruction

**Availability** – The right people can see it when needed



# **HIPAA Security**

## **Password Management**

### **Create strong Passwords**

- at least 7 characters long
- use symbols (\*,%,@) and numbers
- do not use name of spouse, child, pet, etc.
- **Change your password at regular intervals**
- **Never write your password down**
- **Never share your password with others**



# **HIPAA Security**

## **Workstation Use and Security**

**Make sure doors, desks, files are locked as appropriate**

- Be aware of your surroundings. Pay attention to unauthorized persons**
- Locate computer screens so they are not viewable by the public**
- When leaving work area, log-off computer, turn-on screen saver & lock office door**



# **HIPAA Security**

## **Protect Your Computer**

- **Do not add or remove hardware or software on your computer unless authorized to do so**
- **Do not open any unknown attachments or emails**
- **Report all breaches of security or suspicious activity/emails to your supervisor or the Security Officer**

# **HIPAA Security**

## **Name Badges**

- **Badges must be worn at all times while on duty**
- **Should have name and picture fully visible**
- **No alternations**
- **Wear on upper torso**
  - **Do not attach to waist, shirt sleeve, pant leg**



# **HIPAA Mandates Education of Workforce**

- **Workforce will be trained regarding privacy/security policies and procedures with respect to PHI, as necessary and appropriate for the workforce to carry out their duties and responsibilities**



# Enforcement of HIPAA

- Office for Civil Rights (CMS) will enforce the Privacy Regulations
- Office of HIPAA Standards (CMS) will enforce the Security Regulations.
- Enforcement is “Complaint Driven”
- There are severe civil and criminal penalties for knowingly not complying





# **HIPAA and Sanctions**

- **HIPAA requires that the entity has defined sanctions for failure to follow policies and procedures**
- **Key elements of the sanction process are**
  - ✓ **consistent enforcement**
  - ✓ **imposition of fair and consistent disciplinary mechanisms**



# HIPAA Guidance

## Best Practices = Common Sense

- ❖ Be aware of public visibility of PHI on computer screens, paper records. Clear screens & sign off when you leave the work area.
- ❖ Never leave unattended medical information in a room with a patient or family member (i.e. paper record, computer screen).
- ❖ Shred documents containing PHI or discard in blue recycle bins.
- ❖ Be aware of and limit verbal communication involving patients in public areas (i.e. clinic desks, cafeteria, hallways, elevators, etc).
- ❖ Do not leave messages on answering machines regarding patient information or test results.
- ❖ Password protect your computer, handheld devices. Do not share, write down or post your password. Protect your password!
- ❖ Never leave laptops or handheld devices unsecured.



# HIPAA Guidance

## DO NOT Access PHI for Personal Reasons

The following information is not meant to be inclusive, but to give examples of MISUSE of PHI for personal reason.

- ❖ Accessing your own health information (Electronic/Paper)
- ❖ Looking up birth dates, addresses, appointments, test results for family, friends, neighbors
- ❖ Reviewing the record of a patient out of concern or curiosity
- ❖ Looking up a staff member's medical or financial information
- ❖ Discussing patient information with family, friends, other staff when it is not related to your job
- ❖ Reviewing patient record to use information in a personal relationship
- ❖ Compiling a mailing list from hospital records for any reason, except as defined by your job duties



# HIPAA

- For questions or concerns regarding privacy or security, contact:
  - Your instructor
  - The healthcare facility
    - Unit manager
    - Corporate Compliance Officer
    - Security Officer