

# Health Insurance Portability & Accountability Act (HIPAA)

*. . . a training module for all students and employees involved in the use, management and handling of personal health information*

Austin Community College ©2005



# What is HIPAA?

- The Health Insurance Portability and Accountability Act of 1996 was signed into law on August 21, 1996, by President Bill Clinton.
- The Department of Health and Human Services (DHHS) administers the Act.



# What is HIPAA?

The primary objectives of the law are to:

- ensure health insurance *portability* (ease of movement) for workers and families when they change or lose their jobs
- *reduce healthcare fraud* and abuse
- guarantee *security and privacy of healthcare information*
- enforce *standards for health information*
- set *standards for electronic data interchange transactions.*

# Why Should I Know about HIPAA?

- For me as a student, HIPAA helps protect my patients.
- For me as an employee, it protects the privacy and security of my health care information and that of my coworkers.
- For me as a supervisor, HIPAA outlines my responsibilities and boundaries related to healthcare information.

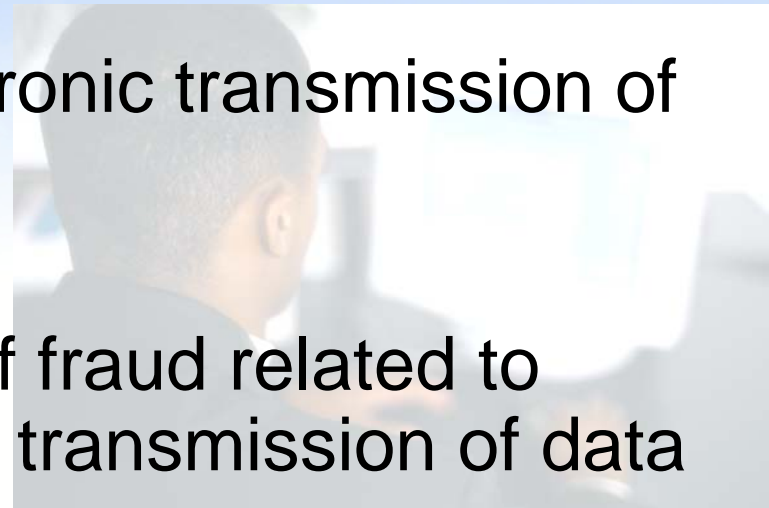
# Why is HIPAA Needed?

- **Advancements in Technology Have**

- Allowed greater access to protected health information (PHI)

- Increased use of electronic transmission of patient data

- Increased possibility of fraud related to electronic storage and transmission of data



# Why is HIPAA Needed?

## *For Example ...*

- An Atlanta truck driver lost his job in early 1998 after his employer learned from his insurance company that he had sought treatment for a drinking problem.



# Why is HIPAA Needed?

- The late tennis star Arthur Ashe's positive HIV status was disclosed by a healthcare worker and published by a newspaper without his permission.



- Tammy Wynette's medical records were sold to *National Enquirer* by a hospital employee for \$2,610.

# Why Comply with HIPAA?

**Protect  
Patient  
Information**



*We all want our  
personal health  
data kept safe  
and secure.*

- **Civil fines** include: - \$100 per person per violation - up to \$25,000/year

# Why Comply with HIPAA?

## **Criminal penalties include:**

- Up to \$50,000 and 1 year in jail for intentional violations
- Up to \$100,000 and 5 years in jail for obtaining PHI with intent to sell, use for personal gain or to cause material harm
- Up to \$250,000 and 10 years in jail for obtaining PHI with intent to sell, transfer, use for personal gain or cause material harm



# Enforcement of HIPAA

- Primary responsibility for the HIPAA Privacy Standards falls on the Office of Civil Rights (OCR), which is an agency within the U.S. Department of Health and Human Services (DHHS).
- The OCR or DHHS will not randomly inspect covered entities for compliance.

# Enforcement of HIPAA

A covered entity will only be investigated after DHHS/OCR receives a legitimate complaint from a consumer. The individual, supervisor and agency can all be held liable.



- Current state laws remain in force that are more stringent in the area of privacy and security of personal information than the standards found in HIPAA.

# Enforcement of HIPAA at ACC

- The HIPAA Sanctions Officer, a member of the ACC HIPAA Task Force, is responsible for investigating any breaches of HIPAA and facilitating the sanctions process following ACC's progressive discipline process.
- The Sanctions Officer will involve an employee's supervisor or the student's faculty member in the discipline process should a serious breach of HIPAA be identified.
- Termination of the student's status in a program or of the employee's employment status could result if it is established that a student or employee of ACC has committed a serious breach of HIPAA regulations.

# Who is Covered by HIPAA?

- All healthcare providers, including hospitals, clinics, nursing homes, physicians, dentists, chiropractors and suppliers
- Entities that furnish, bill, or are paid for healthcare services in the normal course of business (healthcare plans)
- Entities that transmit health information in electronic form in connection with specific transactions (healthcare vendors or clearinghouses, etc.)



# Who is Covered by HIPAA?

- Educational institutions are not specifically addressed in the law, however ACC *is* a covered entity based on the following ...
- **Business Associate:** person/entity to whom the clinical agency discloses PHI, for example, students in ACC courses who have access to PHI in the clinical setting

# Who is Covered by HIPAA?

- **Hybrid Provider:** entity that may be covered as both a Business Associate and a primary covered entity, for example, an educational institution that places students in clinical settings, provides healthcare services to the community (i.e., the ACC Dental Hygiene Clinic), and/or manages staff PHI (i.e., the management of insurance benefits by Human Resources staff)

# When Do We Have to Comply with HIPAA Regulations?

- **April 2003** – all covered entities must be in compliance with Electronic Data Interchange (EDI) requirements
- **April 2004** – must be in compliance with Privacy Rule
- **April 2005** – must be in compliance with Security Rule
- **Business Associates** – must comply with all requirements when requested by covered entity

# 3 Major Focus Areas of HIPAA

## 1) Electronic Data Interchange (EDI)



Focuses on establishing national privacy and security standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers

# 3 Major Focus Areas of HIPAA

## **2) Security**

Focuses on administrative, physical, and technical safeguards that keep patient information safe



# 3 Major Focus Areas of HIPAA

## **3) Privacy**

Focuses on defining boundaries for medical record use and release, penalties for misuse of patient information, appropriate and inappropriate disclosures of information, and appropriate access for information about self

# What is Protected Health Information (PHI)?

- Information that can be communicated orally, in written form, or through other media and is “individually identifiable” about an individual’s past, present, and future, including information about:
  - physical and mental health of a patient
  - provision of healthcare to the patient
  - payment for the patient’s healthcare

# What is Protected Health Information?



Name

Date of birth

Social Security  
number

Address

Phone number

Patient account  
number

E-mail address

Date/location of  
healthcare service  
delivery

Diagnosis,  
treatment,  
medication

Photo or other  
identifiable image

Lab results, etc...

*Basically ...any health related information that can be traced back to the individual!*

# What is Protected Health Information (PHI)?

***NOTE:***

Employee health information is not subject to the Texas Open Records Act and may not be released to the public.

# Use and Disclosure

**Use** – Sharing protected health information (PHI) within the entity that maintains the information (i.e., in the clinical environment or within a specific department of the college)

**Disclosure** – Release or transfer of PHI, providing access to or divulging PHI in any other manner outside the entity holding the information (i.e., outside the clinical environment or from an ACC department to the greater college or to a source outside the college)

# De-identified PHI is...



- Health information that does not identify an individual, and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual, is not individually identifiable health information.
- De-identified information may be disclosed for certain purposes (i.e., educational purposes).

# De-identified PHI

All of the following specific identifiers need to be removed before PHI is considered de-identified:

Name

Address/city/county/  
precinct/zip code

Date of birth

Admission date/discharge  
date

Date of death

Telephone numbers/fax  
numbers, email address

Social Security number

Medical record number

Account numbers

Certificate/license numbers

Vehicle identification  
numbers

Device identifiers and serial  
numbers

URLs/IP addresses

Finger and voice prints

Full face photographic  
images and any  
comparable images

Unique identifying number,  
characteristic or code.

# Minimum Necessary Rule

- Pertains to the use, disclosure and/or request for the minimum amount of PHI needed to accomplish a necessary job/task (treatment, healthcare operations and payment)
- Based on the role/task of the person involved in handling the PHI (i.e., the student in a clinical rotation)

***Note:*** *If it is not within the employee's job description and/or regular job duties (i.e., supervisors, faculty, etc.) to have access to PHI of any kind, then that employee should not have access to or handle such PHI.*

# Minimum Necessary Rule

- *Reasonable Effort* must be used to ensure that only the minimum amount of PHI is handled.
- No identifiable data may be removed from any assigned clinical placement area.
- Only that information needed to meet patient care and learning needs should be used by the student in the clinical setting.
- Does not apply to disclosures...
  - required by law
  - to the individual, or pursuant to an authorization by individual allowing disclosure
  - for treatment purposes in which limiting information may impede treatment

# Minimum Necessary Rule

- Only that information needed by a supervisor to deal with sick leave or employee leave requests should be handled.
- The collection of information not necessary for the administration of requests as outlined above, even by a supervisor, is a potential breach of HIPAA.
- Documents related to the health information of employees should be maintained by HR Benefits, unless otherwise secured by the supervisor.

# Protecting Access to PHI - *Things to Consider ...*

- **Access:** who (employees, patients, students, etc.), what (type of info), when
- **Storage:** how (paper and electronic), where (filing systems, PDAs, laptops, networks, etc.)
- **Disclosure:** who, what, when, how (verbal, fax, e-mail, etc.)
- **Disposal/destruction:** how, when, who (notes made during clinical practice; employee insurance support information)

# Oral Communications are PHI

- The *Privacy Rule* applies to protected health information ***in all forms***, including electronic, written, oral, and any other.
- Coverage of spoken protected health information ensures that this information retains protections when discussed or read aloud from a computer screen or written document.

# Oral Communications are PHI

- The *Privacy Rule* **is not** intended to prohibit providers from talking to each other and to their patients.
- Provisions require implementation of ***reasonable safeguards*** that reflect particular circumstances.

# Email Guidelines

- The Information Technology department recommends that faculty and staff include a statement regarding confidentiality at the end of outgoing email messages.

*For example:*

*“This message may contain confidential and/or privileged information. If you are not the intended recipient or have received this message in error, please notify the sender immediately and destroy this message.”*

# Email Guidelines

- Senders ultimately have no control over how recipients handle email messages they receive.
- Once sent, email cannot be “unsent.”
- ACC faculty and staff should communicate only via their ACC email addresses for college related business.
- It is best to reply to incoming email rather than risk typing incorrect email addresses.

# Faxes - Another Example of PHI

- A form of written communication
- Students are not allowed to fax any type of PHI in the normal course of their program.
- Faxes will be allowed only under the supervision of the instructor, and only when absolutely necessary.
- When a fax is used, a privacy statement must be placed on the cover page, and the sender must ensure that the receiver expects the fax and is ready to receive the fax securely.

# Consent for Release

- Covered entities do not need to obtain consent from the *patient* for use or disclosure of PHI, as long as that use/disclosure follows the *minimum necessary rule*.
- A consent can be put in place if an individual wants to limit the use of their PHI more than the HIPAA standards allow.

# How HIPAA Applies to Education

- It applies to any student who, in the course of the educational process, is involved in a patient's care and/or has access to PHI (within the clinical environment, as well as associated activities outside the clinical environment).
- In the course of education, a patient's PHI (including photos/images) must not be disclosed or used in any way *without the patient's authorization/consent*.
- *Reasonable Effort* must be made to ensure that only de-identifying PHI is used for educational purposes.

## ***NOTE:***

- A serious breach of HIPAA rules, as determined by the HIPAA Sanctions Officer, can result in...
  - ... the removal of a student from a course or program
  - ... disciplinary action for an employee, up to and including dismissal
  - ...depending upon the seriousness of the breach

# In General, Students Need To ...

- Be aware of HIPAA policies for their specific clinical setting by completing HIPAA training for the facility.
- Sign the ACC HIPAA Acknowledgement.
- Ensure that *reasonable effort* is being used to prevent misuse of PHI.
- Report to the faculty member/instructor any breaches in HIPAA rules they observe or participate in (intentionally or unintentionally).
- Ensure disclosure of only de-identified PHI.

# Responsibilities of All ACC Employees (Faculty and Staff Members)

- Must be a role model by
  - Respecting the rights of patients, students, and employees with regard to privacy
  - Supporting the clinical agency's privacy policies
  - Refraining from the collection and/or distribution of PHI from other ACC employees/students when not absolutely necessary to their ACC role

# Responsibilities of All ACC Employees (Faculty and Staff Members)

- Must be knowledgeable about and understand HIPAA law and compliance regulations
  - Staff, students, patients
- Must be an enforcer of HIPAA regulations
  - Enforce clinical agency's policies
  - Adhere to student discipline requirements
  - Follow through on breaches by reporting them to supervisor and HIPAA Privacy Officer



# **Proceed to Post-Test**

Leave this PowerPoint window open, so that you may refer back to its content while completing the Post-Test.