HIPAA Education – Level One
For Volunteers & Observers

~ What does HIPAA stand for?
H – Health
I – Insurance
P – Portability
A – And Accountability
A - Act

The federal Health Insurance Portability and Accountability Act (HIPAA) of 1996, along with state law, mandates the privacy and security of Protected Health Information (PHI); the portability of health insurance and simplification of electronic billing.

~ Components of HIPAA
1.) Transactions (codes used in billing)
2.) Privacy
3.) Security

~ What is the purpose of HIPAA?
• Protects the privacy of an individual’s health information
• Ensures physical and technical security of an individual’s health information
• Governs the use and disclosure of an individual’s health information for treatment, health care billing, research, marketing and other functions.

~ What are the benefits of HIPAA?
• Privacy Notice – The University of Kentucky will be required to notify individuals in writing how their Protected Health Information may be used and disclosed.
• Accounting of Disclosures – A history of non-routine disclosures – those other than treatment, payment and health care operations, or those for which authorizations have been obtained – must be provided to individuals upon their request.
• Recourse – Individuals may file formal complaints with the University via the Privacy Officer or the Department of Health and Human Services Office of Civil Rights.
• Access – Individuals will be able to access, inspect and get copies of their medical records, and also may request amendments to those records.
• Restrictions – Individuals will have the right to request restrictions on the uses and disclosures of their information. The University of Kentucky may refuse such a request on grounds that we could not accommodate the request.
  Example: Mandatory reporting of gunshot wounds

~ Why do you have to take HIPAA training?
• Federal law requires this training. Observance of HIPAA regulations is the way we will conduct business in the future.
• This is the first stage of HIPAA training. You may require additional training specific to your area at a future date.
~ Who is required to comply with HIPAA?

All health plans, clearinghouses and health care providers who conduct business electronically, must comply with the standards. These groups are referred to as “Covered Entities.”

Covered Entities include:

- Hospitals, durable medical equipment suppliers, sole practitioners and Physician practice groups, dentists, pharmacies, home health agencies, and nursing homes, among others.
- Laboratories/departments conducting human research, financial offices, third party administrators, insurance carriers who deal with protected health information, internal audit, and legal counsel.
- Business associates who contract with the University of Kentucky.

The University of Kentucky is a “covered entity.”

~ What makes the University of Kentucky a “covered entity?”

The University of Kentucky is comprised of several groups that make it a “covered entity” including, University of Kentucky Chandler Medical Center, medical benefit plans, human research, dental clinics, student health services and athletics, among others.

~ The Privacy Rule

The HIPAA Privacy Rule establishes minimum safeguards to protect confidentiality of an individual’s health information.

STATE LAWS, WHICH PROVIDE STRONGER PRIVACY PROTECTIONS FOR INDIVIDUALS, WILL STILL APPLY INSTEAD OF THE FEDERAL PRIVACY STANDARDS.

The HIPAA Privacy Rule protects:
- An individual’s health information in all forms: electronic, paper, spoken, and whether past, present or future.
- The rule protects individuals, living and dead, and or groups in both the public and private sector.

~ What is Protected Health Information?

Protected Health Information is commonly referred to as PHI.

PHI is defined as facts about an individual’s past, present or future physical or mental health condition.

~ What information is included in PHI?

Use of any one of the 18 identifiers listed, when combined with information regarding a person’s health, is protected under HIPAA.

- Name
- Address
- Medical record #, account #
- Dates
- Social Security #
- Health plan beneficiary #
- Birth
- License or ID #
- Photographs
- Date of admission
- Drivers license #
- Fingerprints, voice prints
- Date of discharge
- Vehicle plate #
- Device identifiers & serial #’s
- Death
- Telephone #
- Full face photo/other images
- Certificate/license #
- Fax #
- Email/URL/IP address #
- Any other unique ID#, characters, or code

~ Under what conditions must you protect any of the previously mentioned pieces of information?

Whenever:
- The information relates to the person’s physical and mental health, provision of health care or payment for health care
- The information will identify, or could be used to identify, the subject of the information, and
- The information is transmitted or maintained in any form or medium.
  Examples: fax, computer files, paper records

ALWAYS REMEMBER…

All information regarding an individual’s health care is confidential. DO NOT share this information with your friends, family or neighbors. In other words, if you learned it through your work or other associations with UK, it is considered private.

You also must be careful about where and when and with whom you share information required to perform your job. Share information only with co-workers who HAVE a legitimate need to know for treatment, payment or health care operations. Hallways, break rooms, elevators, the shuttle and parking lots, for example, are not appropriate places to share PHI.

~ The Security Rule

What is information security?
- Maintains confidentiality, integrity, availability and privacy of employee, patient, physician, research subjects and University information

- Applies to all information – electronic, paper, or spoken-that is created, communicated, stored or processed by your office, department, hospital or school

~ UK and the Security Rule

Guidelines:
If you have access to written or electronic confidential health information, you may be asked as a condition of your affiliation with UK, to sign a confidential agreement.

~ “You” and the Security Rule

How do you secure the various types of protected health information you encounter on a regular basis?

PAPER
- Only authorized personnel generate or copy confidential documents.
- Confidential documents must not be left in areas accessible by unauthorized persons.
- Confidential documents must be disposed of in a confidential recycling bin, shredded, or rendered unreadable.
- Patient medical records must not be taken home or to any non work-related place.

If in doubt about confidentiality of a document, handle as if confidential.

COMPUTERS
- Use a unique password
- Do not share your password
- Store laptops, PDAs, floppy disks and CDs in a secure location when not in use
- Log out when leaving a workstation*
- Sign off applications WHEN leaving your workstation
- Use only password-protected portable computing devices
- Do not download unauthorized software from the Internet

* If you have an exception, contact the Compliance Office at 323-6044

TELECOMMUNICATIONS
- Devices such as cordless phones, cell phones, pagers, faxes and intercoms
- At UK confidential information can be communicated by phone and fax
- Use a cover sheet that includes a confidentiality statement to indicate who is to see the fax
- Prior to sending the fax, notify the person to whom the fax is being transmitted
- The sender is responsible for keeping receipts of fax transmissions

~ Securing the physical environment in which you work
- Keep records and protected health information in secure areas
- Dispose properly of confidential or protected health information (shredding or placing in secured recycle bins)
- Ensure that unauthorized individuals cannot see protected health information on your computer screen, fax machine, or in your work area

~ Why do we need to be so careful?
A New York State congressional candidate’s past suicide attempt was made public during the election. She won the election and sued the hospital for failing to maintain the confidentiality of her medical records.

An employee of a large Blue Cross/Blue Shield plan obtained unauthorized access to the medical records of a friend’s ex-wife and sent them to the friend.

A bank member of a state health commission accessed a list of local cancer patients and cross-referenced it to a list of his customers. He then called in their loans.

A Tampa, Florida man stole a list of 4,000 HIV-positive patients from a state health worker and sent the list to the Tampa Tribune, which did not publish it. The man was found guilty and sentenced to jail.

~ Why is this important to you?
You are responsible for securing PHI and keeping it private. If you don’t you may be liable!

The University of Kentucky will not be responsible for individual employee penalties if the breach was intentional or happened outside the scope of the individual’s job responsibilities.

~ What else do you need to know?
The University of Kentucky will facilitate compliance with the HIPAA regulations through electronic monitoring of computer access to PHI, and by conducting physical Inspections of University areas that handle confidential health information.

~ What are the penalties for non-compliance?
- Disciplinary action by the University of Kentucky: up to and including termination of employment or expulsion from the academic program
- Federal Civil penalties:
  - $100 per violation, up to $25,000 per person, per year, for each requirement or prohibition violated
- Federal Criminal penalties for knowing violations:
  - Up to $50,000 and one year in prison
  - Under “false pretenses” – up to $100,000, and up to five years in prison
- Intent to sell, transfer or use – up to $250,000 and up to 10 years in prison

~ What should you do if you see violations?
- Tell your supervisor or academic advisor, who will investigate the situation
- If you aren’t comfortable telling your supervisor or academic advisor, contact the Compliance Office at 323-6044 or by email at mches@email.uky.edu
- Violations also may be reported anonymously to the ComplyLine-(877) 898-6072
UK HealthCare HIPAA Test

In order to receive credit for HIPAA training-level one, you must complete the following questions with 100% accuracy as well as fill in the employee information at the end of the questions.

1. HIPAA (Health Insurance Portability Accountability Act) protects an individual’s health information.
   - True
   - False

2. HIPAA protects an individual’s health information in which of the following forms?
   - Electronic
   - Paper
   - Spoken
   - All of the above

3. Which of the following items of information are considered PHI (Protected Health Information) when combined with information about an individual’s health history, whether in the past or present?
   - Name
   - Social Security number
   - Date of birth
   - Full face photograph
   - All of the above are considered PHI

4. If you intentionally violate any of the provisions of the HIPPA law after receiving this training, you will NOT be covered by the University’s liability insurance and therefore will be personally responsible for any fines, penalties, or imprisonment.
   - True
   - False

5. The University of Kentucky is required to monitor itself for compliance with HIPAA regulations. Therefore periodic audits will be done of computer access to health information and observations of interactions of those involved in working with health information.
   - True
   - False

6. All information regarding any individual’s health care is confidential and must not be shared with anyone who does not have a legitimate need to know.
   - True
   - False

7. If you have access to written or electronic confidential health information, you may be asked as a condition of your affiliation with the University of Kentucky to sign a confidentiality agreement.
   - True
   - False
8. If you convey PHI to another person who does have a right to know, which method of communication is acceptable?
   - Send a fax without a cover sheet
   - Face to face communication in the elevator
   - Face to face in a room with a close door, and only occupied by others with a need to know
   - Message left on unsecured answering machine
   - All are acceptable methods

9. Which of the following actions is NOT acceptable when working with PHI on the computer?
   - Using a unique password
   - Sharing your password only with those whom you work or study
   - Logging out when leaving a shared workstation
   - Ensure that your computer is facing away from the public view
   - None are acceptable

10. I have reviewed and understand the HIPAA privacy rules restricting use and disclosure of protected health information. I further understand that I am required to comply with the HIPAA rules and that my compliance with them is a condition of my employment, enrollment or affiliation with the University of Kentucky. I understand that failure to follow the HIPAA rules may result in disciplinary action, including termination of my employment, enrollment or affiliation at the University.
   - Yes
   - No

Date ______________
First Name____________________
Last Name____________________
Last 4 digits of SSN_____________
Email Address__________________________________
Signature______________________________________

If you are under 18 years of age, please have your parent/guardian co-sign this HIPAA document.