Welcome to the
HIPAA, Privacy & Security
Training Module
Course Competencies

This training module addresses the essential elements of maintaining the privacy and security of sensitive information and protected health information (PHI) within the workplace.

During this course you will learn:

• about the Health Insurance Portability and Accountability ("HIPAA") Privacy and Security Rules;

• about the HIPAA identifiers which create protected health information ("PHI");

• how to recognize situations in which confidential and protected health information can be mishandled;

• about practical ways to protect the privacy and security of sensitive information, including PHI, and

• that employees will be held responsible if they mishandle confidential or protected health information.
Forms of Sensitive Information

Sensitive Information exists in various forms…

printed  spoken  electronic

It is the responsibility of every employee to protect the privacy and security of sensitive information in ALL forms.
Examples of Sensitive Information

- Social Security numbers
- credit card numbers
- driver’s license numbers
- personnel information
- research data
- computer passwords
- Individually identifiable health information

The improper disclosure of sensitive information presents the risk of identity theft, invasion of privacy, and can cause harm and embarrassment to staff, patients, and Louisville Metro. Breaches of information privacy can also result in criminal and civil penalties for the Department and for those individuals who improperly access or disclose sensitive information, as well as disciplinary action for responsible Metro employees.

Every LMPHW employee must protect the privacy and security of sensitive information.
HIPAA Privacy & Security Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law designed to protect a subset of Sensitive Information known as protected health information (PHI).

In 2009, HIPAA was expanded and strengthened when the American Recovery and Reinvestment Act was passed. This law is referred to as the HITECH Act (Health Information Technology for Economic and Clinical Health).

This training module focuses on two primary HIPAA rules, as amended by HITECH:

Section 1: The HIPAA Privacy Rule

Section 2: The HIPAA Security Rule

Note: There is also a Transaction Rule that is not covered in this course. Healthcare providers need to be aware that under this rule, treatment must be accurately billed using the prescribed code set for their profession.
Section 1A

HIPAA Privacy Rule Overview
Covered Entities Have a Duty to Protect PHI

A “covered entity” is any person or organization that furnishes, bills or is paid for health care services in the normal course of business. Pursuant to HIPAA, individually identifiable health information collected or created in a covered entity is considered “protected health information,” or PHI. Metro departments that use or disclose PHI are governed by HIPAA requirements.
**PHI defined**

**PHI** is generally defined as:

Any information that can be used to identify a patient – whether living or deceased and which relates to the patient’s past, present, or future physical or mental health or condition, including healthcare services provided and the payment for those services.

Employees may access PHI only when necessary to perform their job-related duties.
Any of the following are considered identifiers under HIPAA.

- Patient names
- Geographic subdivisions (smaller than state)
- Telephone numbers
- Fax numbers
- Social Security numbers
- Vehicle identifiers
- E-mail addresses
- Web URLs and IP addresses
- Dates (except year)
- Names of relatives
- Full face photographs or images
- Healthcare record numbers
- Account numbers
- Biometric identifiers (fingerprints or voiceprints)
- Device identifiers
- Health plan beneficiary numbers
- Certificate/license numbers
- Any other unique number, code, or characteristic that can be linked to an individual.
In general, HIPAA violations are enforced by the Department of Health and Human Services. However, the more recently enacted Health Information Technology for Economic and Clinical Health (HITECH) Act now permits state Attorneys General to bring civil actions AND for monetary awards to be shared with harmed individuals.

The Tufts Medical Center and an employee were sued by a patient who alleged the Center sent documents containing her protected health information to a shared office fax machine in her place of business without her consent, causing her great embarrassment. Although the PHI was related to the employee’s disability claim, it was sent to the wrong fax machine located in a common area of her office.

Confirm authorization instructions and verify telephone numbers before faxing AND use pre-programmed telephone numbers whenever possible.
A psychiatric clinic patient sued her doctor and his office manager after the doctor permitted the manager to access the patient’s protected health information without her authorization and shared the PHI with third parties.

Although the complaint was initially dismissed, the Court of Appeals reversed that decision, finding that HIPAA establishes a standard of care to which healthcare provider offices need to adhere, and liability for negligence may arise when that standard of care is breached.
Access Must be Authorized

An employee may only access or disclose a patient’s PHI when this access is part of the employee’s job duties.

If an employee accesses or discloses PHI without a patient’s written authorization or without a job-related reason for doing so, the employee violates LMPHW policy and HIPAA.
Unauthorized Access

It is never acceptable for an employee to look at PHI “just out of curiosity,” even if no harm is intended.

It also makes no difference if the information relates to a “high profile” person or a close friend or family member – ALL information is entitled to the same protection and must be kept private.

These rules apply to all employees, including health care professionals.

Be aware that accessing PHI of someone involved in a divorce, separation, break-up, or custody dispute may be an indication of intent to use information for personal advantage, unless the access is required for the individual to do his or her job. Such improper behavior will be considered by the Department when determining disciplinary action against violators.
Breaches

A breach occurs when information that, by law, must be protected is:

• lost, stolen or improperly disposed of (i.e. paper or device upon which the information is recorded cannot be accounted for);

• “hacked” into by people or mechanized programs that are not authorized to have access (e.g. the system in which the information is located is compromised through a “worm”), or

• communicated or sent to others who have no official need to receive it (e.g. gossip about information learned from a medical record).
In 2011, a UCLA Health System employee became the first person in the United States to receive jail time in a federal prison for a misdemeanor HIPAA offense. The employee used his employee access to the University’s electronic medical records system to view the medical records of his supervisors, co-workers, and high-profile patients. While none of the information was “used” or sold, the access was nonetheless illegal because the employee lacked a valid reason for looking at the records.

The ex-employee pled guilty to four misdemeanor counts of violating HIPAA. His sentence was four months in prison and a $2,000 fine.
Employees Must Report Breaches

Part of your responsibility as a LMPHW employee is to report privacy or security breaches involving PHI to your supervisor AND one of the following persons:

- the HIPAA Privacy Officer, or
- the HIPAA Security Officer.

Employees, volunteers, students, or contractors of the Department may not threaten or take any retaliatory action against an individual for exercising his or her rights under HIPAA or for filing a HIPAA report or complaint, including notifying of a privacy or security breach.

Reports of possible information privacy violations can be made to the HIPAA Privacy Officer by emailing:

Briana.Forsythe@Louisvilleky.gov

Reports may also be made via telephone by calling the HIPAA Privacy Officer at 502-574-6690.
Penalties for Breaches

Breaches of the HIPAA Privacy and Security Rules have serious ramifications for all involved. In addition to sanctions imposed by the Department, such breaches may result in civil and criminal penalties.

Statutory and regulatory penalties for breaches may include:

**Civil:** $50,000 per incident, up to $1.5 million per calendar year for violations that are not corrected

**Criminal:** $50,000 to $250,000 in fines and up to 10 years in prison

In addition, institutions that fail to correct a HIPAA violation may be fined up to $50,000 per violation.

Under the HITECH Act, the Department may be required to notify potentially affected individuals of breaches involving their PHI.
Breach Notification Requirements

Improper disclosures or breaches of PHI or other sensitive information may trigger notification requirements. Depending upon the nature of the disclosure or breach, notifications may have to be made to:

- the Department of Health and Human Services,
- the Kentucky State Attorney General,
- all individuals whose information was breached or disclosed, and
- the media.

Letters of explanation describing the circumstances, including responsible parties, may have to be sent. It is estimated that the cost to comply with notification requirements exceeds $200 per data set.
Brigham and Women’s Hospital recently announced the loss of a hard drive potentially containing the PHI of over 600 patients. This information could include patient names, medical record numbers, admission and release dates, and information about diagnosis and treatment.

Department employees should consult the LMPHW HIPAA Privacy & Security Policies on SharePoint or call the HIPAA Privacy Officer at 502-574-6690.
Quick Review

• Sensitive information exists in many forms: printed, spoken, and electronic.
• Sensitive information includes Social Security numbers, credit card numbers, driver’s license numbers, personnel information, computer passwords, and PHI.
• There are a number of laws that impose privacy and security requirements, including the HITECH Act.
• Two primary HIPAA regulations are the Privacy Rule and the Security Rule.
• When used to identify a patient and when combined with health information, HIPAA identifiers create PHI.
• An employee must have a patient’s written authorization or a job-related reason for accessing or disclosing patient information.
• Breaches of information privacy and security may result in both civil and criminal penalties, as well as Department sanctions. Employees must report such breaches.
Section 1B

HIPAA Privacy Rule

Program Components
Five HIPAA Program Components

Following is a brief overview of five HIPAA program components followed by Metro covered entities:

1. Individual (Patient) Rights

2. “Minimum Necessary” Information Standard

3. Procedures for Data Use in Research

4. Limits for Marketing and Fundraising Uses

5. Business Associates
1. Patient Rights

The first component sets forth the following individual rights for patients.

- To receive a copy of the Department’s Notice of Privacy Practices.
- To request restrictions and confidential communications of their PHI.
- To inspect and copy their healthcare records.
- To request corrections of their healthcare records.
- To obtain an accounting of disclosures (i.e., a list showing when and to whom their information has been shared).
- To file a complaint with a healthcare provider or insurer and the U.S. Government if the patient believes his or her rights have been denied or that PHI is not being protected.
2. Minimum Necessary

Under the HIPAA Privacy Rule, when the use or disclosure of PHI is permitted, only the **minimum necessary information** may be used or disclosed. However, this does **not** restrict the ability of doctors, nurses, and other healthcare providers to share information needed to treat patients, process payments, or to report public health concerns.

Otherwise, **patients must sign an authorization form** before their PHI may be released by the Department to outside parties such as a life insurer, a bank, or a marketing firm.
Disclosures of PHI

HIPAA regulations **permit** use or disclosure of PHI for:

- providing medical treatment
- processing healthcare payments
- conducting healthcare business operations
- public health purposes as required by law.

Employees **may not** otherwise access or disclose PHI **unless**:

- the patient has given written permission
- it is within the scope of an employee’s job duties
- proper procedures are followed for using data in research
- required or permitted by law
Imagine that you work with patients to help find ways to pay their medical bills. Through your work, you become aware of a family under substantial financial hardship. You believe that kindhearted members of the community would provide help “If they only knew” of these circumstances. In order to tell this story you must get specific written authorization, from the patients or their legal representatives, that identifies whom you will tell. In addition, you may communicate only the minimum amount of information necessary to describe the need.

Note: This type of “outreach” should be approved in advance by departmental managers and supervisors and must be consistent with institutional policy.
3. Research Data

HIPAA regulates how PHI may be obtained and used for research. This is true whether the PHI is completely identifiable or partially “de-identified” in a limited data set.

A researcher or healthcare provider is not entitled to use PHI in research without the appropriate HIPAA documentation, including an authorization or an institutionally approved waiver.

HIPAA requirements for accessing and using PHI in research are explained in the Department’s HIPAA Privacy & Security Policies.
Even if a researcher gets a signed “Informed Consent Form” from a research subject, if she does not also get a signed HIPAA Authorization form (or waiver), she may not use data she has collected for her research, presentations or publications.
4. Marketing & Fundraising

- Without an authorization, the Department may not use information about the medical treatment of an individual for targeted fundraising or marketing.

- The Notice of Privacy Practices and other general fundraising and marketing communications must advise patients of the right to “opt out” of being contacted for fundraising and marketing purposes.
5. Business Associates

An outside company or individual is a **HIPAA Business Associate** of the Department when providing services involving PHI maintained by the Department.

Pursuant to HIPAA, a **Business Associate** must:

- enter into a **Business Associate Agreement** (sometimes called a BAA) with the covered entity (LMPHW);

- use **appropriate safeguards** to prevent the use or disclosure of PHI other than as permitted by a contract with the covered entity;

- **Notify the covered entity** of any individual instances of a breach for which the Business Associate was responsible where PHI has been improperly accessed, used, or disclosed;

- ensure that their employees and/or subcontractors receive **HIPAA training**; and

- protect PHI to the same degree as a covered entity.

Speak with the Privacy Officer to decide if a Business Associate Agreement (BAA) must be established.

Business Associate Decision Tree

Is an outside person or entity providing a service or performing a function or activity for LMPHW?

NO

Will the outside person or entity access or receive and use Protected Health Information (PHI) in providing the service?

NO

YES

Does the health information being disclosed meet any of the exceptions noted at the right?

YES

NO

The person or entity is not a business associate and a business associate agreement is not required.

The person or entity is a business associate and a business associate agreement is required.

Health Information is:
- De-identified;
- For transport purposes (e.g. Postal service or courier);
- A claim sent to a health plan, payment to a provider; or a fund transfer to a financial institution;
- Going to a Health Oversight Agency as part of a federal or state program (e.g. Centers for Medicare and Medicaid Services);
- In response to a request from law enforcement or subpoena;
- Legally required to be reported; or
- For the purposes of research.
Quick Review

Under HIPAA, patients have the right to:

• receive a copy of the Department’s **Notice of Privacy Practices**

• inspect and copy their healthcare records

• ask for **corrections** of their healthcare records

• receive **accounting** of when and with whom their PHI has been shared

• **restrict** how their PHI is used and shared

• authorize **confidential communications** of their PHI to others

• file a HIPAA **complaint**
Quick Review

- The Department may use or share only the **minimum necessary information** to perform its duties.
- Patients must sign an **authorization form** before the Department can release their PHI to a third party not involved in providing healthcare, such as a bank or life insurer.
- A researcher or healthcare provider is not entitled to use PHI in research without the appropriate HIPAA documentation.
- The Department must obtain an individual’s **specific authorization** before using his or her PHI for **marketing or fundraising**.
- A contractor providing services involving PHI is called a **Business Associate**.
- A covered entity and business associate must enter into a **Business Associate Agreement** (“BAA”).
- Business Associates must ensure that their employees or subcontractors receive HIPAA training.
- HIPAA protections apply to a person’s protected health information even after they have died.
Section 2

HIPAA Security Rule
HIPAA Security Rule

The HIPAA Security Rule concentrates on safeguarding PHI by focusing on the confidentiality, integrity and availability of PHI.

**Confidentiality** means that data or information is not made available or disclosed to unauthorized persons or processes.

**Integrity** means that data or information has not been altered or destroyed in an unauthorized manner.

**Availability** means that data or information is accessible and useable upon demand only by an authorized person.
Security Standards/Safeguards

The Department is required to have administrative, technical, and physical safeguards to protect the privacy of PHI.

Safeguards must:

- **Protect PHI** from accidental or intentional unauthorized use/disclosure in computer systems (including social networking sites such as Facebook, Twitter and others), and work areas;

- **Limit accidental disclosures** (such as discussions in waiting rooms and hallways); and

- **Include practices** such as document shredding, locking doors and file storage areas, and use of passwords and codes for access.
A doctor at Westerly Hospital in Rhode Island was fired for posting information on Facebook about a patient she treated. Although the posting did not reveal the patient’s name, there was enough information that others could easily identify him or her, and indicated the patient had problems with alcohol and marijuana abuse.

The doctor was also reprimanded by the state medical board and fined $500.

Department employees should never disclose work-related sensitive information through social media such as Facebook, Twitter, and Google+.
Malicious Software

Viruses, worms, spyware, and spam are examples of malicious software, sometimes known as “malware.”

Employees should utilize antivirus and anti-spyware software, and update it regularly. (Metro IT automatically updates your computer’s antivirus and anti-spyware software).

Safe Internet browsing habits can also reduce the likelihood of an infection.

If the computer or mobile device you are using stores work-related sensitive information, personal use of the web is not recommended.
Viruses

A major threat to the Department’s information system and to your data is computer viruses.

- Viruses “infect” your computer by modifying how it operates and, in many cases, destroying data.
- Viruses spread to other machines by the actions of users, such as opening email attachments.
- Viruses can forward PHI to unauthorized persons by attaching themselves to documents, which are then emailed by the virus.
- Newer viruses have their own email engines, enabling them to send email without having to use an email client or server.
- Many viruses also install a “backdoor” on affected computer systems allowing for unauthorized access and collection of Sensitive Information.
Worms

Worms are programs that can:

• run independently without user action
• spread complete working versions of themselves onto other computers on a network within seconds
• quickly overwhelm computer resources with the potential for data destruction as well as unauthorized disclosure of sensitive information.
Spyware

Spyware is software that is secretly loaded onto your computer, monitors your activities, and shares that information without your knowledge.

Malicious websites can install spyware on every computer that visits those sites.
Spam is an unsolicited or “junk” electronic mail message, regardless of content.

Spam usually takes the form of bulk advertising and may contain viruses, spyware, inappropriate material, or “scams.”

Spam also clogs email systems.

Phishing is a particularly dangerous form of spam that seeks to trick users into revealing sensitive information, such as passwords. No official part of Metro government, including Metro IT, will ever ask you to disclose passwords, social security numbers or other sensitive information via email. Do not respond to any email request for this type of information by email. Contact the Metro IT Service Desk at 574-4444 if you receive any such requests.
Safe Browsing Habits

• **Safeguard sensitive information**
  Look for signs of security when providing sensitive information (i.e. the web address starts with “https” or a padlock icon is displayed in the status bar).

• **Keep browser updated and use security settings**
  • Stay current with browser updates and application updates such as Adobe Flash and Acrobat. Contact Metro IT at 574-4444 and they will assist you.
  • Enable browsing security settings to alert you to threats to your computer like popups, spyware, and malicious cookies.

• **Use security software**
  There are a number of software products to protect your computer from malware, spyware and virus threats. Metro IT automatically installs a variety of products on individual computers and devices.

• **Safe downloading & streaming**
  • When in doubt just don’t do it! If a download looks too good to be true it might be malware.
  • Downloaded files like software or other media can contain hidden malware.
  • Streaming media Web sites might seem harmless, but watching or listening to streaming media may require downloading a special media player that could contain malware.
Last year, Martin Memorial Center in Florida took disciplinary action against several employees for taking pictures of a shark attack victim with their cellular phones. Penalties for employees who took the photos ranged from written warnings and demotions to suspension.

Department employees should consult the LMPHW HIPAA Privacy & Security Policies on SharePoint or call the HIPAA Privacy Officer at 502-574-6690.
Peer to Peer (P2P)
File Sharing Programs

- P2P programs frequently contain spyware and are used to share files that contain malware.
- P2P file sharing programs such as Morpheus, Kazaa, and BitTorrent are commonly used to download unauthorized or illegal copies of copyrighted materials such as music or movies. They may also expose Sensitive Information to unauthorized individuals if not configured correctly.

Use of P2P programs on Department networks is prohibited in certain areas, especially those where PHI or PII (Personally Identifiable Information) is present.

Check with your HIPAA Privacy or HIPAA Security Officer before using P2P programs.
Safe Email Use

• Do not open email attachments if the message looks the least bit suspicious, even if you recognize the sender. “When in doubt, throw it out.”

• Do not respond to “spam” – simply discard or delete it, even if it has an “unsubscribe” feature.

• PHI may be transmitted by email to louisvilleky.gov addresses when appropriate. No additional action is required.

• Email should not normally be used to transmit PHI outside LMPHW. If you do have to transmit PHI via email you should:
  ◦ Not include PHI in the subject line.
  ◦ Type “[encrypt]” in the subject line
  ◦ Only use your Metro email account – do not use an outside account

• For further information, contact the Department HIPAA Security Officer, at 502-574-6690.
Password Control

Many security breaches come from within an organization – and many of these occur because of **bad password habits**.

- **Use strong passwords** where possible (at least 8 characters, containing a combination of letters, numbers, and special characters).

- **Change your passwords frequently** (45-90 days) to prevent hackers from using automated tools to guess your password.

- **It is a violation of Department Policy to share your password with anyone.** Electronic audit records track information based on activity associated with user IDs.
Against Department policy, a health clinic employee set his phone to “auto-forward” his Department messages to his Google account. In addition, his supervisor sometimes sent assignments to his Google address. Also, the phone was not password protected.

While on vacation, the employee’s phone “went missing”. Eventually the phone was returned by a travel office, but no one knows who may have had possession of the device while it was not in the employee’s control.

The employee violated HIPAA by housing and transmitting PHI to an unsecure device, creating a risk of breach that could require notification to each affected client/patient whose data was contained in the phone and possibly the government. There were also disciplinary actions taken against the employee and his supervisor.

Costs to the Department of a lost or stolen mobile device go far beyond the cost of replacing the device itself. The majority of expenses include:

- investigative costs
- reporting data breaches
- liability for data breaches (e.g. government penalties)
- restoring hard-to-replace information
- preventing further misuse of the data
- lost intellectual property
- lost productivity.

Report missing, lost, or stolen devices immediately to your Supervisor and the Metro Service Desk (574-4444). According to an Intel study, the faster an organization learns that a laptop is lost, the lower the average cost of response. "If a company discovers the loss in the same day, the average cost is $8,950. If it takes more than one week, the average cost rises significantly to approximately $115,849."
Mobile Devices

If you use mobile computing devices such as laptop PCs, PDAs such as iPads, iPhones, Palm Pilots, Blackberrys, Treos, or smart phones, or even regular cell phones to store and send information, be aware that Department policy requires written approval from a Director, Department Head, or ITS in order to store PHI or PII off campus. Department policy also requires that written approval be granted by a Director, Department Head, or IT before storing PHI or PII on mobile devices.

Employees are required to utilize the following security controls when storing and transmitting sensitive information:

- strong power-on passwords
- automatic log-off
- display screen lock at regular intervals while the device is inactive
- metro authorized data encryption software

Never leave mobile computing devices unattended in unsecured areas.

Immediately report the loss or theft of any mobile computing device to your supervisor and the Information Security Office.
Remote Access

All computers and mobile devices used to connect to Department networks or systems from home or other off-site locations should meet the same minimum security standards that apply to your work PC.

You should:

- Make use of the Virtual Private Network (VPN) at home or off-site, AND transmit PHI only to locations within the Department network. Otherwise, sensitive data must be encrypted.

- Run Windows Update or the update feature of the particular operating system that you are using. Don’t forget to also update your applications (e.g. QuickTime, RealPlayer, and your preferred web browser)!

- Keep virus definitions current by using the automatic updater from the antivirus software you are using.

**DO NOT** let your antivirus subscription expire.

Antivirus software is available to all Staff via Metro’s IT Department.

Call 502-574-4444 for assistance.
A professor at Bowling Green University lost a computer USB flash drive (memory stick) with students’ personal information in it. The files in the portable storage device contained Social Security numbers for about 200 students, together with names, grades, and university ID numbers for another 1600 students.

Whenever possible, avoid using external storage devices to store Sensitive Information. If you must use encryption and:

- Use only Metro approved USB devices
- Use portable storage media only for transporting information, and not to permanently store information.
- Once you’ve used the information, erase it from the device.
- Consider attaching your memory stick to your key ring -- you are less likely to lose your keys.
Employee Responsibilities

- Access information only as necessary for your authorized job responsibilities.
- Keep your passwords confidential.
- Report promptly to your supervisor and the Department’s HIPAA Privacy or Security Officer the loss or misuse of Department information.
- Initiate appropriate actions when problems are identified.
- Comply with the Department’s HIPAA Privacy & Security Policies.
- Avoid storing sensitive information on mobile devices and portable media, and if you must, make sure the device is encrypted.
- Always keep portable devices physically secure to prevent theft and unauthorized access.
Communications in Public Areas

Be aware of your surroundings when discussing Sensitive Information, including PHI. **Do not discuss sensitive information or PHI in public areas such as in hallways or bathrooms, while walking around the department, or while on work trips.**

Use caution when conducting conversations in:
- semi-private rooms
- waiting rooms
- corridors
- elevators and stairwells
- open treatment areas
Appropriate Disposal of Data

Observe the following procedures for the appropriate disposal of Sensitive Information, including PHI.

- Hard copy materials such as paper or microfiche must be properly shredded or placed in a secured bin for shredding later.
- Magnetic media such as diskettes, tapes, or hard drives must be physically destroyed or “wiped” using approved software and procedures. Contact the Metro Service Desk at 574-4444 for more information.
- CD ROM disks must be rendered unreadable by shredding, defacing the recording surface, or breaking.

Sensitive information and PHI should never be placed in the regular trash!
On several occasions sensitive materials have been left in file cabinets or office desks that have been turned in to the Metro Surplus department. The surplus staff found the sensitive materials and returned them to the Department before anyone picked up the furniture. If any of that furniture had been sold to the public before the sensitive materials were found, it would’ve been difficult and costly for the Department to retrieve the materials and manage the breach.

One can’t be too careful when disposing of desks, file cabinets and other office furniture that may hold documents in them. Please check them carefully and confirm that all documents have been removed and properly disposed of before sending furniture to the Metro Surplus department.
Physical Security

Equipment such as PCs, servers, mainframes, fax machines, and copiers must be physically protected.

- Computer screens, copiers, and fax machines must be placed so that they cannot be accessed or viewed by unauthorized individuals.
- Computers must use password-protected screen savers.
- PCs that are used in open areas must be protected against theft or unauthorized access.
- Servers and mainframes must be in a secure area where physical access is controlled.
What if there is a breach of confidentiality?

Breaches of the Department’s policies or an individual’s confidentiality must be reported to the employee’s supervisor AND one of the following persons:

- the HIPAA Privacy Officer, or
- the HIPAA Security Officer;

The Department is required to take reasonable steps to lessen harmful effects of any breach. This may include notifying the individual whose information has been breached. The HITECH Act requires that covered entities report breaches of PHI to the Secretary of Health and Human Services at least once a year.
Disciplinary Actions

Individuals who violate the Department’s HIPAA Privacy & Security Policies will be subject to appropriate disciplinary action as outlined in the Department’s personnel policies, as well as possible criminal or civil penalties.
Best Practice Reminders

• **DO** keep computer sign-on codes and passwords secret, and **DO NOT** allow unauthorized persons access to your computer. Also, use locked screensavers for added privacy.

• **DO** keep notes, files, memory sticks, and computers in a secure place, and be careful to **NOT** leave them in open areas outside your workplace, such as a library, cafeteria, or airport.

• **DO NOT** place PHI or PII on a mobile device without required approval. **DO** encrypt mobile devices that contain PHI or PII.

• **DO** hold discussions of PHI in private areas and for job-related reasons only. Also, be aware of places where others might overhear conversations, such as in reception areas.

• **DO** make certain when mailing documents that no sensitive information is shown on postcards or through envelope windows, and that envelopes are closed securely.

• **DO NOT** use unsealed Department mail envelopes when sending sensitive information to another employee.

• **DO** follow procedures for the proper disposal of sensitive information, such as shredding documents or using locked recycling drop boxes.

• When sending an e-mail, **DO NOT** include PHI or other sensitive information such as Social Security numbers, unless you have the proper written approval to store the information, follow proper procedures, and you encrypt e-mail sent outside louisvilleky.gov.
HIPAA Web Resources

U.S. Dept. of Health & Human Services HIPAA Page:
http://www.hhs.gov/ocr/hipaa/
HIPAA, Privacy & Security Training Module

Please take the quiz now.

After you take the quiz, print the certificate, retain a copy for your records, and give the original to the Training Office, 400 E. Gray Street.

To go back to your HIPAA training course page, click the back button on your browser.