

HIPAA Trainer

Health Insurance Portability and Accountability Act

The HIPAA Privacy Rule

An Overview of the Basics

(This information is subject to frequent updates and modifications)

HIPAA

Health

Insurance

Portability and

Accountability

Act

Federal legislation enacted in 1996 to improve the efficiency and effectiveness of electronic information transfers used in the provision, management, and financing of health care in the U.S.

This legislation impacts **anyone and everyone** involved in clinical activities by virtue of new, strict rules for handling health information.

What is in the Law?

- Privacy rules
- Security rules
- Civil and criminal penalties

What is the goal of HIPAA legislation?

- To protect health information
- Ensure confidentiality and accuracy
- Establish use and disclosure procedures
- Ensure proper handling of data
- Implement audit controls

Privacy and HIPAA

PRIVACY refers to **WHAT** is protected *health information* about an individual and the determination of who is permitted to use, disclose, or access the information. (This presentation addresses the privacy provisions of the regulations.)

SECURITY refers to **HOW** information is safeguarded --- ensuring privacy by controlling access to information and protecting it from inappropriate disclosure and accidental or intentional destruction or loss. Security is also regulated under HIPAA.

A future presentation will address the security provisions of the regulations.

***Health Information* is defined in section 1171 of the Act**

It includes:

- **ANY INFORMATION**, whether oral or recorded in any form or medium, that
- is **CREATED OR RECEIVED** by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and
- relates to the past, present, or future **PHYSICAL or MENTAL HEALTH** or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and
- **IDENTIFIES THE INDIVIDUAL**

Examples of Health Information

- Paper records and reports
- Electronic records
- Spoken communications
- Patient radiographs
- Patient photographs

HIPAA regulates how health care providers must deal with **PROTECTED HEALTH INFORMATION (PHI)**

What is PHI?

PHI is health information (defined as **any** information gathered by a health care provider, including non-health related data) **that contains data that may be used to directly or indirectly identify the patient.**

What data elements make health information Protected Health Information?

- Name
- Names of relatives
- Address

- Names of employers
- E-mail address
- Fax number
- Telephone number
- Birth date
- Finger or voice prints
- Photographic images/X-rays
- Social security number
- Internet address
- Vehicle/device serial number
- Medical record number
- Health plan number
- Account number
- Certificate/license number
- Web URL

HIPAA applies to any PHI , regardless of the data format

Examples...

- a patient's chart and medical record
- database or computer stored files
- email
- images or x-rays
- conversations
- word documents
- PDA stored information
- student logs
- academic curriculum
- laptop files
- personal databases of clinical material
- personal clinical experience logs

Bottom Line? Virtually all of the information routinely used in the clinical setting is PHI and must be properly handled and protected.

What does the Privacy Rule MEAN?

1. It limits the Use and Disclosure of PHI

Use. Defined as the employment, application, utilization, examination, or analysis of information WITHIN an entity that holds the information

Disclosure. Defined as the release of PHI that is not related to treatment, payment, or health operations

2. It establishes Individual (Patient) rights to control access and use of PHI, including the:

- right to inspect or copy PHI
- right to amend incorrect information
- right to receive an accounting of all disclosures made for reasons other than payment, treatment, or health care operations

3. It balances health information protection and individual rights against public health and safety needs.

4. It defines specific administrative requirements:

- a privacy officer
- patient notice of the privacy policy
- training for ALL employees
- sanctions for policy violations
- documented Policies and Procedures for handling and protecting PHI

Privacy Regulation Requirements

Effective 4/14/03, **YOU MUST...**

1. Clearly communicate information practices and honor privacy promises (e.g., the PRIVACY NOTICE)
2. Get detailed patient authorization for each non-routine (research) use and disclosure
3. Limit information use and disclosure to the MINIMUM NECESSARY
4. Require business partners (by contract the BUSINESS ASSOCIATE AGREEMENT) to protect health information
5. And hold them accountable Be able to provide an accounting of non-routine disclosures
6. Adopt comprehensive privacy policies and procedures and train every employee
7. Appoint a privacy officer
8. Use effective controls (physical and technical) to avoid privacy breaches
9. Impose discipline for breaches of privacy and mitigate any resulting harm
10. Document what was done to protect patient privacy

Privacy Notice

This document must:

- inform the patient of his/her rights
- disclose the organization's privacy practices
- explain the organization's responsibilities under the law
- inform the patient about all the uses and disclosures of PHI required and allowed by law
- outline the process for the patient to gain access to their medical record and to request amendments to this information
- list the contact person within the practice who will receive complaints and/or be available for questions

Minimum Necessary

The **minimum necessary** refers to the concept that PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. As an example, the receptionist does not require access to the patient's entire medical record; perhaps only the name, current address, and insurance information.

This concept does **not** apply (and does not limit) disclosures by a health care provider for treatment purposes, disclosures to the patient, and disclosures may pursuant to the patient's authorization.

Access to see or hear patient information

Not everyone needs to see or hear PHI. Before you look at or listen to health information, ask yourself, Do I need to know this to do my job or provide high quality care? If the answer is no, don't look or listen. If the answer is yes, look or listen only to the information you need and protect the confidentiality of that information.

Patients must be given a copy of the PRIVACY NOTICE and it must be documented that it was received

You must undergo specific HIPAA training and this training must be documented

Access to clinical records for research will become more cumbersome

Everyone must be much more attuned to the inadvertent disclosure of PHI.. do **not** talk about patients in the hallways, elevators, and cafeteria; only access PHI when necessary and then only to the extent necessary to do your job (the *minimum necessary* concept)

Dispose of PHI properly

- place patient information in secure containers

- shred the documents
- erase/destroy diskettes
- avoid improper disclosure

Avoid improper disclosures

- verify FAX numbers and email addresses
- do not leave detailed phone messages
- turn computer screens away from passersby
- use a screen saver

Guard against improper access

- log off when finished
- change your password often
- do not share your password
- password protect access to your PDA

The Privacy Rule DOES NOT mean that you...

- cannot discuss patient care with colleagues
- cannot talk to patients in public areas
- cannot use sign-in sheets in the clinic
- cannot use patient-based material for teaching, presentations, and projects
- cannot do clinical research

Frequently Asked Questions

Can Health Care Providers (HCPs) use sign-in sheets or call out the names of patients in the waiting room? **YES**

Can HCPs place medical charts at the bedside or outside exam rooms? **YES**

Does a HCP need a patient's written authorization to send a copy of the medical record to a specialist or other HCP who will provide treatment? **NO**

Can a physician's office FAX patient medical info to another MD's office? **YES**
(but the recipient fax should be in a secure location)

Does the Privacy Rule and minimum necessary concept prohibit trainees from accessing PHI in the course of their training? **NO**

Can a researcher abstract data from 30 charts for a review article? **ONLY AFTER** approval from the IRB and Individual Authorizations by the patients or a waiver from the institutional privacy board. Individual Authorizations, signed by the patients, are required for the use and disclosure of PHI for any purpose other than treatment, payment, or health care operations or as otherwise excepted by law.

Access to PHI for research purposes will require individual authorization by the patient or a Waiver, granted by the institutional privacy board.

Situations in which PHI may be released without Individual Authorization or Waiver

- Reporting a communicable disease
- FDA required reporting of information about medical devices that break or malfunction
- Child abuse and neglect reporting laws
- Criminal investigations
- Court order
- Suspicious deaths or injuries (e.g. gunshot wound)
- Cause of death to a coroner or funeral director

Consequences of Noncompliance that may be levied by the Office of Civil Rights

Criminal Penalties

Fines up to \$250,000
Prison time up to 10 years

Civil Penalties

\$100 for each violation
Maximum of \$25,000 per year per incidence

Penalties may apply to the individual violator and/or to the organization or its officers.

Consequences of Noncompliance that may be levied by the Institution or Practice

- Verbal warning
- Written warning
- Suspension
- Termination of employment

If you have questions about HIPAA, contact the Privacy Officer of your department or send an email to hipaa@med.wayne.edu.

If you suspect your institution is not complying with HIPAA, a complaint can be filed with the Office for Civil Rights. A complaint must be filed within 180 days of the date the complainant knew about the possible violation of the law.

Useful Links

- <http://www.med.wayne.edu/hipaa>
- <http://www.hipaadvisory.com/regs/hipaaprimer1.htm>
- <http://aspe.hhs.gov/admsimp/bannerps.htm>
- <http://www.amc-hipaa.org>
- <http://www.nchica.org>

The HIPAA Privacy Rule and Research

A General Overview

The Privacy Rule has important implications for human research.

New administrative requirements are mandated by HIPAA that must be met before you can access, study, and disclose Protected Health Information (PHI).

HIPAA defines RESEARCH as "any systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

The HIPAA Privacy Rule **does not** override the Common Rule or FDA's human subjects regulations.

Researchers must now address regulatory requirements by **BOTH** the IRB and HIPAA.

The HIPAA regulations do not differentiate between treatment and non-treatment related human research studies.

HIPAA applies to **all** human research, regardless of the funding source.

HIPAA Privacy Rule Stipulates

The Use or Disclosure of Protected Health Information (PHI) for research purposes requires either:

- A written **Authorization** from the subject

or

- A **Waiver** approved by the Privacy Board / IRB /HIC

or

- **Verification** that the research involves:
 - De-Identified Information
 - Limited Data Sets
 - Reviews Preparatory to Research
 - Decedents' Information

Patient Authorization for the Use and Disclosure of PHI may be the most advantageous route to research

- No Representations (Assurances) required
- No Privacy Board review required (but the project **must** be reviewed and approved by the IRB)
- No Accounting of Disclosures required
- No "Minimum Necessary" limitations

Note:

Patient Authorization (HIPAA - privacy issues)

is **NOT** the same as

Patient Consent (IRB - risk versus benefits)

HIPAA compliant forms for Patient Authorization for the Use and Disclosure of PHI can be obtained from the WSU HIC website (www.hic.wayne.edu)

There Are 5 Pathways to Obtain Protected Health Information for Research Without Individual Patient Authorization

- Waiver of Authorization Requirement
- Use of De-identified Information
- Use of Limited Data Sets
- Research using Decedents' Information
- Reviews Preparatory to Research

Detailed information can be obtained from the WSU HIC website at www.hic.wayne.edu.

Psychotherapy Notes

Psychotherapy Notes are notes that:

- Are recorded in any medium by a health care provider who is a mental health professional

and

- Document or analyze the contents of conversation during a private counseling session or a group, joint, or family counseling session

and

- Are separated from the rest of the medical record

Psychotherapy Notes

Psychotherapy Notes do **NOT** include:

Medication prescription and monitoring

Session start and stop times

Modalities and frequencies of treatment furnished

Results of clinical tests

Any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, or progress

Psychotherapy Notes Authorization and Research Consent

An Authorization for the Use and Disclosure of Psychotherapy Notes

May **NOT** be combined with Informed Consent for Research

May **ONLY** be combined with another Authorization for use or disclosure of Psychotherapy Notes

What about research that was approved before April 14, 2003, but continues to enroll new subjects after April 14, 2003?

Subjects enrolled after April 14, 2003 must sign an Authorization for Use and Disclosure of Protected Health Information in Research.

HIPAA and Education

HIPAA impacts everyone who participates in clinical activities by virtue of new, strict rules for handling health information. These rules also govern the use and disclosure of health information during teaching and educational activities.

You are personally responsible for the proper use and protection of health information in the clinical setting... whether on the ward, in the classroom, or in a conference.

You are personally liable for YOUR violations of the WSU School of Medicine policies concerning the HIPAA guidelines

What is HEALTH INFORMATION that must be protected under the HIPAA guidelines?

Defined in section 1171 of the Act, this includes:

- **ANY INFORMATION**, whether oral or recorded in any form or medium, that
- is **CREATED OR RECEIVED** by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and
- relates to the past, present, or future **PHYSICAL or MENTAL HEALTH** or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and
- **IDENTIFIES the INDIVIDUAL**

Examples of Health Information

- Paper records and reports
- Electronic records
- Spoken communication
- Patient radiographs
- Full face photographs

What is PROTECTED HEALTH INFORMATION (PHI) ?

PHI includes one or more of the following:

- First name
- Last name
- Medical record number
- Social security number
- Address or other geographical info
- Email address
- Phone number, fax number, cell phone number
- Date of birth
- Age
- Admission date

- Discharge date
- Procedure date
- Date of death
- License plate number
- Medical device number or serial number
- Account numbers
- Biometric identifiers
- Any other unique identifying number, characteristic, or code

HIPAA provides specific protections for Protected Health Information. To protect privacy and avoid inappropriate disclosures:

- Access and use PHI only to the extent necessary to perform a task or complete an assignment (the Minimum Necessary)
- Protect the confidentiality of patient data at all times
- Always de-identify PHI to the extent possible
- Safely and securely discard PHI when it is no longer needed
- Avoid talking about patients in public areas
- Carefully safeguard all electronic devices that contain Individually identifiable health information

Electronic devices, including laptops and PDAs, are commonly utilized in the clinical setting. Typical uses include but are not limited to:

- Patient lists for rounding information
- Call-back numbers
- Patient test results
- Surgery schedules
- Procedure lists

HIPAA does not prohibit these uses but it does require that you make reasonable efforts to protect and safeguard any patient data that may reside on these devices.

PHI in your electronic device must be properly secured at all times. This may be accomplished in several ways:

- Password protect the log-on to your system
- Password protect access to data sets
- Change your password frequently
- Do not share your password
- Encrypt data
- Safeguard your PDA and guard against theft

Be sure to safeguard any patient data that may be on your home computer. This information should not be accessible to family members or others.

Educational activities are also subject to HIPAA Privacy Guidelines.

Clinical education occurs in many settings and forums. It is your responsibility to safeguard the confidentiality of patient information (PHI) in the educational setting as well as the treatment setting. PHI should only be used to the extent necessary (the Minimum Necessary).

To understand what you must do to comply with HIPAA in the educational setting, it is helpful to consider whether or not PHI is to be presented and who will participate in the activity.

Remember.....

Protected Health Information (PHI) includes **ONE** or more of the following:

- First name
- Last name
- Medical record number
- Social security number
- Address or other geographical info
- Email address
- Phone number, fax number, cell phone number
- Date of birth
- Age
- Admission date
- Discharge date
- Procedure date
- Date of death
- License plate number
- Medical device number or serial no.
- Account numbers
- Biometric identifiers
- Any other unique identifying number, characteristic, or code

If the educational activity does NOT involve the presentation of PHI, further consideration with regard to HIPAA is NOT required.

If PHI will be presented AND?

The audience is limited to the Health Care Team, PHI may be used without HIPAA compliant authorization by the patient.

Health Care Team includes those individuals with a TREATMENT or OPERATIONS relationship to the patient as defined by HIPAA. As a practical matter, this includes attending physicians, fellows, residents, students, and other trainees, as well as support staff who are involved in some aspect of the care of the patient.

The audience includes the Health Care Team AND a visiting participant (such as a visiting professor, community MD, etc) who has NO relationship to the patient but *contributes to the discussion regarding treatment and/or education.*

PHI may be used without patient authorization or a HIPAA compliant Confidentiality Agreement.

The audience includes the Health Care Team AND a visiting participant who has NO relationship to the patient and *does **NOT** contribute to the discussion regarding treatment and/or education.* An example would be a pharmaceutical representative who sponsors the conference.

The visitor must sign a HIPAA compliant Confidentiality Agreement **OR** leave the room prior to the presentation of PHI.

The audience includes attendees with no relationship to the patient and they make no contribution to the presentation. An example would be Grand Rounds, which is open to the public, and the attendees do not actively participate.

The PHI must be de-identified **OR** the patient must sign a HIPAA compliant authorization prior to disclosure of the PHI.

Observers in the clinical setting

On occasion, observers may be present in the clinic, operating room, or other patient care areas. These individuals must first sign a HIPAA compliant Confidentiality Agreement.

Disposal of Protected Health Information (PHI)

PHI includes any information gathered by a health care provider, including non-health related data, that contains information that may be used to directly or indirectly identify the patient. Examples include paper records and reports, clinic lists, handwritten notes about a case, electronic records, email, radiographs, photographs, student activity logs, and resident experience logs.

It is expected that PHI will be properly disposed of as soon as it has fulfilled its purpose. By example, when a course has been completed, a clerkship rotation has ended, or an assigned presentation has been made, any PHI in your possession should be destroyed.

Ways to securely dispose of PHI

- Erase electronic media
- Destroy electronic media
- Shred paper documents
- Place paper documents in a proper receptacle at work so that it can be properly destroyed

Questions concerning HIPAA compliance may be directed to hipaa@med.wayne.edu.

Check the WSU School of Medicine HIPAA website for frequent updates and responses to Frequently Asked Questions (FAQs).

Wayne State University School of Medicine HIPAA Security Training

This training material is designed to introduce faculty, staff, and students to the HIPAA Security Rule, the proper use and disclosure of protected health information (PHI), the proper safeguards for confidential information including electronic protected health information (ePHI), and highlights from the University Physician Group HIPAA Policies and Procedures. It is not intended to replace University Physician Group Policies. Please refer to the actual policy and departmental procedures and workflows for additional details.

The HIPAA Security Rule compliance date is April 20, 2005. It requires additional protections for electronic Protected Health Information (ePHI).

The primary focus of the HIPAA Security Rule is to ensure the ***confidentiality, integrity and accessibility*** of ePHI:

- Protect ePHI against unauthorized access, and improper alteration or destruction
- Protect against threats or hazards to the security and integrity of ePHI
- Protect against unauthorized uses or disclosures of ePHI
- Make ePHI readily available to authorized personnel when needed
- To do this, security measures must be in place, and it is your job to abide by the University Physician Group policies to meet the HIPAA Security requirements

Who is Responsible for Information Systems Security?

- **YOU are!**
 - The greatest risk to the confidentiality, integrity and accessibility of ePHI is through human error
 - **Your** commitment to protect information is critical
 - Don't share passwords
 - Don't try to get around security rules
 - Protect portable computer equipment (laptops, PDAs)
 - Be computer safety-savvy

What is PHI?

Protected Health Information is any information that may identify the patient and that relates to:

- Past, present, or future physical or mental health condition or
- Health care services provided or
- Payment for health care

- ***Includes***

- Diagnosis and Treatment Information
- Identifying Information
- Insurance and other payment information

What is PHI?

Information about the identity of patients is protected (18 identifiers apply to patients, relatives, employers, or household members of patients)

- Name
- Dates directly related to patient
- Fax number
- Social security number
- Health plan beneficiary number
- Certificate/license number
- Web address/URL
- Finger or voice prints
- Photographic image
- Age (if 89 or greater)
- Any unique identifying number, characteristic, or code, address (street, city, county, zip to 3 digits), telephone number, email address, medical record number, account number, any vehicle or device serial number, internet protocol (IP) address

What is ePHI?

- ePHI is any information specifically identifying a person that is:
 - Stored electronically
 - Sent or shared electronically

Examples of ePHI include, but are not limited to:

- laboratory results that are emailed to a patient
- demographic information about a patient contained in UPG information systems such as IDX and NextGen

- a note regarding a patient stored in your Palm Pilot
- billing information that is saved to a CD or Floppy
- a digital photograph of a patient stored on your hard drive
- Patient names, procedures, and OR times on your electronic calendar or other procedure/surgery scheduling

The HIPAA Security Rule breaks security safeguards into three main categories:

- Technical Safeguards
- Administrative Safeguards
- Physical Safeguards

The Security Rule lists a wide range of activities for which we must provide protection:

- Computer hardware and software
- Buildings that house computer hardware and software
- Storage and disposal of data and the backup of data
- Who has access to data
- Visitor access to any facilities

Technical Safeguards

Technical safeguards include the use of computer technology to protect ePHI and track activity in information systems.

ePHI Transmission - Encryption

- When PHI is electronically sent from one point to another, it must be secured to avoid theft, damage, or destruction of the information.
 - All transmissions of ePHI from WSU-UPG to an outside network must utilize an encrypted mechanism between the sending and receiving entities
 - Encryption makes the information "unreadable" by anyone who doesn't have the "key"

Emailing ePHI

- If you email PHI outside of the UPG Exchange system, you must abide by the UPG Email Policy
- IS is implementing a technical solution to ensure encryption of internet bound email containing PHI

- You MAY NOT use commercial ISP (Yahoo, AOL) to send email with PHI

Domain Log-on & Email

- Every employee of the School of Medicine or an affiliated practice plan is required to have an UPG domain log-on ID and email account.

Malicious Software - Malicious software, such as "worms" and "viruses" take over or damage computer networks/resources. IS protects against malicious software:

- Anti-virus software is installed and kept current on all required information systems
- Email attachments are scanned for viruses prior to delivery
- **How can you help:**
 - Never bypass or disable anti-virus software
 - Do not install personal software or download Internet software such as Kazaa, Weatherbug, anti-virus software, and/or pop-up blockers

Security Reminders - IS will start providing security updates to users with information, reminders, and updates to reinforce security training and to provide additional information.

- ***Mobile and remote devices require special care.***
- PCs, mobile devices such as PDA's, Blackberry's, laptops, digital cameras, CDs, and diskettes, or any other portable device containing confidential information or ePHI should be appropriately secured with password protection
- All computers, remote and on-site, including home computers that contain ePHI must be protected with a secure log-on
- ePHI must be destroyed before hardware or media containing ePHI is disposed of or made available for reuse. Deleting ePHI is not enough.
- In order to safely destroy electronic media, please contact the Help Desk at (313) 577-1527 for assistance.

You may need help with technical safeguards. The IS Technical Support Center is ready to help.

The Help Desk is available 24 hours a day, 7 days a week to assist you with computer/software related questions and problems. You can reach the Help Desk by:

- Calling (313) 577-1527
- Emailing them at helpdesk@med.wayne.edu
- Go to their website at <http://www.med.wayne.edu/msis>

Administrative Safeguards

Administrative safeguards exist to ensure that all members of the workforce have appropriate access to ePHI in order to perform their jobs.

As a workforce member, your role is to be familiar with and follow these policies and procedures to protect ePHI. You must also take steps to make certain ePHI is not inappropriately seen or altered.

Password Management - choosing a good password and keeping it secure - are two of the most important steps you can take to protect electronic information

Password Reminders

- Keep your passwords confidential - do not share them with others!
- Avoid maintaining a paper record of passwords
- Do not use the same password for business and personal accounts
- Always maintain and use passwords in a secure and confidential manner

Selecting a Strong Password - passwords should be:

- a minimum of eight characters
- Based on something besides personal information
- Composed of a mix of numeric and alphabetic characters
- Refer to the UPG Password policy for additional password requirements

Disciplinary Action - you are personally responsible for the access of any information using your password and will be held responsible for any violations of WSU-UPG policies involving your ID.

Report Unauthorized Access/Use - if you believe someone else is using your ID or password, immediately notify the IS Help Desk at (313) 577-1527.

Computer Access - access to confidential information is granted on a need to know basis. Computers should be used only for authorized purposes. Do not engage in any activity that is illegal under local, state, federal, or international law or that violates WSU-UPG policies.

Log-on and Access Monitoring - IS monitors login attempts to UPG electronic information systems. If you suspect inappropriate login

attempts, you must report it to the IS Help Desk at (313) 577-1527. All UPG computers systems are subject to audit and your access may be monitored.

System Access for Transferring and Terminating Members of the Workforce - Department supervisors are responsible for reviewing transferring employees' computer access levels and notifying the IS Help Desk so appropriate adjustments can be made. Upon separation from WSU - UPG or affiliated practice plan, all access is terminated and the IS Help Desk must be notified.

Locking the Computer - When leaving your computer unattended, lock the computer using "control/alt/delete" or log-off the computer.

Physical Safeguards

We have established specific measures to protect our information systems, buildings and equipment from natural, environmental hazards and unauthorized intrusion. If you have access to secure areas, keep these measures in mind:

- Only authorized personnel should be in areas of our building where protected health information is stored
- ePHI should never be left unattended or unsecured
- Security devices such as keys, key cards, and badges should be stored in secure locations
- Data should always be backed up before it is moved to a new location

- Confidential information, including ePHI, must not be removed from the UPG without prior approval.

- You are responsible for maintaining the privacy and security of all confidential information that you may be transporting, storing, or accessing off-site.

Secure Work Environments

- Secure environments and workstations are necessary for the security of ePHI. Good security practices need to be incorporated into your daily routine so your work area is secure. Simple habits relating to the use of your computer can significantly increase the safety of your workstation.

Security Of The ePHI You Handle

- Employee access to ePHI may change due to the Security Rule. Information may have been more available within our organization before the new security requirements. Now, under the Security Rule, you should only have access to the information you need to do your job. Access includes reviewing, moving, sharing or disclosing information. It is very important if you are granted access to secure areas, you do not allow unauthorized users access to these areas.
- ***Identifying and reporting security incidents is an important part of security maintenance. If you suspect a security incident, you should immediately report the activity to the IS Help Desk.***

- ***The following examples are activities that should be reported:***
 - Viruses
 - Sharing of passwords
 - Public disclosure of passwords (e.g. password reminders taped onto computers)
 - Loading of games and unnecessary software
 - Suspicious emails
 - Unexpected changes in documents

"Phishing"

- Phishing is a way of stealing information by pretending to be someone authorized to obtain that information.
- Immediately report any attempts to gain access to your passwords, or enticing you to violate policies.
- IS will never ask you for your passwords or ask you to violate a policy.
- When in doubt, ask a manager before sharing sensitive information.

Computer Audits

- The Security Rule requires organizations to regularly review computer system activity. Audit logs and access reports will be used to regularly monitor activity on our computer systems to ensure access is appropriate.
- We are very serious about protecting our computer systems from malicious software that could disable or damage our computer system. If you notice an unusual email or computer function notify the IS Help Desk. Malicious software uses viruses, spyware and other activities to disrupt computer systems.

HIPAA Penalties for Noncompliance

- **Employee Sanctions:** Violations by workforce may result in disciplinary action, up to and including termination from employment.
- **Severe civil and criminal penalties:** In addition to employee sanctions, you can be subject to civil and criminal penalties imposed by the federal government up to \$250,000 and 10 years in prison.

Conclusion

- We must all remember to protect the privacy and security of patient information at all times.
- We are all patients ourselves from time to time. Think about how you would feel if your own health information were used or disclosed in a way that was harmful to you or your family.
- If you have a question about HIPAA, ask your supervisor or manager, contact your Privacy or Security Officer, or call the IS Help Desk at (313) 577-1527.
- For more detail, please refer to the WSU UPG HIPAA website at <http://www.med.wayne.edu/hipaa>