

# HIPAA PRIVACY and SECURITY AWARENESS TRAINING

## Training Objectives



After completing this program you will:

- Have a general understanding of the HIPAA Regulations.
- Have an understanding of UMC's Privacy and Security policies.
- Know how to obtain more information regarding HIPAA.

Jan 8, 2007



---

---

---

---

---

---

---

---

## HIPAA



- Mandated by the 1996 Health Insurance Portability and Accountability Act, known as HIPAA, contained two main provisions.
  - Health Insurance reform to protect workers and their families from losing coverage when they change or lose their job.
  - Administrative Simplification which adopted national standards for electronic transactions, privacy and security of protected health information.

Jan 8, 2007



---

---

---

---

---

---

---

---

## Potential Costs of Non-Compliance



- The Office of Civil Right and Centers for Medicare and Medicaid Services investigate reports of non-compliance
  - Fines of up to \$100 per occurrence to \$25,000 per calendar year for failure to comply with standards
  - Fine of up to \$50,000 for wrongful disclosure of individually identifiable health information and up to 1 year in prison
  - Fine of up to \$100,000 and prison up to 5 years for committing the offense under false pretenses
  - Fine of up to \$250,000 and prison up to 10 years when committing the offense with intent to sell, transfer, or use for personal gain, commercial advantage, or malicious harm

Jan 8, 2007



---

---

---

---

---

---

---

---

## Why HIPAA?



People are concerned about the use or disclosure of personal health information without their knowledge. When patients do not feel their information will be kept confidential, they may do any of the following to protect their privacy:

- Refuse treatment
- Give incomplete or inaccurate information
- Pay out of pocket to avoid insurance claims
- "Doctor-hop" to keep one from having a complete medical history
- Ask the doctor not to document their actual condition

Jan 8, 2007



---

---

---

---

---

---

---

---

## What Information is Protected by HIPAA?

- HIPAA defines "protected health information" (PHI) as any information that identifies an individual and describes the individual's past, present or future physical or mental health condition.
- PHI can be any verbal, paper or electronic information maintained by a covered entity.
- Such information may be found in:
  - Medical and Billing Records
  - Computer Systems/Electronic Records
  - Photographs, Videos, Audiotapes



Jan 8, 2007



---

---

---

---

---

---

---

---

## What Information is Not Protected by HIPAA?

- ✗ Health information that is in personnel records.
- ✗ Student health information of federally funded schools and colleges.
- ✗ Health information disclosed to a non-covered entity.

Jan 8, 2007



---

---

---

---

---

---

---

---

## Who Must Comply with HIPAA?



- Most doctors, nurses, pharmacies, hospitals, clinics, nursing homes, and many other health care providers
- Health insurance companies, HMO's, and most employer group plans
- Certain government programs that pay for health care, such as Medicare and Medicaid

Jan 8, 2007



---

---

---

---

---

---

---

---

## HIPAA & Clark County



- Clark County has determined these departments are healthcare components within the County. These departments either provide medical services or are considered a health plan:
  - University Medical Center
  - Social Services
  - Juvenile Justice Services
  - Employee Assistance
  - Self-Funded Group Medical & Dental Benefit Plan
  - Risk Management

Jan 8, 2007



---

---

---

---

---

---

---

---

## HIPAA & Clark County

- The following departments support the covered departments on the previous page and may have access to protected health information from those departments during the course of normal operations. They are therefore also included in the County's Hybrid Entity:
  - Comptroller / Treasurer
  - Board of County Commissioners
  - County Manager Office
  - Information Technology
  - Audit
  - Civil District Attorney



Jan 8, 2007



---

---

---

---

---

---

---

---

## HIPAA Compliance Activities at UMC

- HIPAA compliance is an ongoing effort. As we change systems and procedures we may also need to change our privacy and security practices.
- We provide training and education about HIPAA to our employees, students, volunteers, contractors and members of the Medical and Dental Staff.
- We balance protecting patient information with ensuring caregivers have the information they need to properly care for patients.
- We investigate complaints.
- We monitor regulations and guidance to ensure current our practices are compliant.
- We put mechanisms in place to ensure compliance and identify instances of non-compliance.

Jan 8, 2007



---

---

---

---


---

---

---

---

## What is My Role?

- 
- Understand the Privacy and Security rules as outlined in this presentation.
  - Continually assess risks to the availability, integrity, and confidentiality of protected health information and implement or suggest measures to reduce those risks.
  - Protect health information.
  - Follow UMC's policies and procedures that minimize risks to protected health information.
  - Know your department's specific procedures.

Jan 8, 2007



---

---

---

---


---

---

---

---

## Highlights of Privacy Rule

- 
- Requires UMC to keep PHI safe and secure.
  - Requires UMC to verify the identity of a requestor before any disclosures are made.  
(There is a reference tool that gives examples of ways to verify identity available on the intranet.)
  - Provides new individual rights such as the right to request restrictions on sharing PHI, to request confidential communications, to access PHI, or to have corrections made to their records.

Jan 8, 2007



---

---

---

---

---

---

---

---

## Highlights of Privacy Rule

- Disclose only the minimum information necessary to meet the need.
- State laws that provide more privacy protection than HIPAA take precedence.
- Each department must maintain policies, procedures and documentation related to their compliance with the law.
- Records of compliance must be maintained for 6 years.
- Patients may file a complaint with UMC or the Office for Civil Rights if they believe their rights are violated.

Jan 8, 2007



---

---

---

---

---

---

---

---

## Notice of Privacy Practices

- The law requires health care providers to give patients a notice detailing their privacy rights, including how their health information will be used and disclosed, and when their authorization is needed before a disclosure is made.
- The Notice must also explain who will have access to their medical records—from researchers and students to public health officials.



Jan 8, 2007



---

---

---

---

---

---

---

---

## Notice of Privacy Practices

- The Notice must be given to patients the first time they are seen in any UMC location.
  - Included in the patient handbook issued to all new inpatients
  - Separate handout given to all new outpatients
- The Notice must be posted and available upon request.
  - On the UMC internet and intranet
  - Available in Spanish
  - Posted in UMC's Patient Access Services department



Jan 8, 2007



---

---

---

---

---

---

---

---

## Highlights of Privacy



- HIPAA is not intended to interfere with patient care
- Insurance and health care providers are permitted to share PHI without an authorization only if the purpose is for Treatment, Payment, or Operations purposes, such as:
  - Treatment – a doctor calling for the results of the tests he ordered on one of his patients
  - Payment – a durable medical equipment company requesting a copy of the doctor's order so they can bill for their services
  - Operations – internal performance improvement studies

Jan 8, 2007



---

---

---

---

---

---

---

---

## Sharing Information as Required by Law



UMC is permitted to share limited PHI without a patient's authorization in the following instances:

- Public Health Requirements: Mandatory reporting of communicable diseases, birth and death certifications, animal injuries
- Health Oversight Activities: Authorized agencies surveys, inspections, audits.
- Judicial & Administrative Proceedings: Court orders, investigations in response to complaints.

Jan 8, 2007



---

---

---

---

---

---

---

---

## Sharing Information as Required by Law



UMC is permitted to share limited PHI without a patient's authorization in the following instances:

- Organ Donation
- Public Safety
- Workers Compensation

HIPAA does require us to record these "permitted" disclosures. UMC uses an application known as HIPAASafe. Be sure you know what your department's specific procedures are for required disclosure tracking.

Jan 8, 2007



---

---

---

---

---

---

---

---

## Sharing Information with Family Members and Friends

Healthcare professionals must seek direction from the patient. When this is not possible, healthcare providers may use professional judgment to determine what information to share.

Some patients may request restrictions, such as "NFP" (Not for Publication) or the use of a password to limit calls and visitors. Be sure you know how to identify when a patient has exercised his privacy rights.



Jan 8, 2007

---

---

---

---

---

---

---

---

## HIPAA Security



HIPAA requires covered entities to ensure the **CONFIDENTIALITY** of information, **INTEGRITY** (information is not improperly altered or destroyed), and the **AVAILABILITY** (information is available to authorized people) of all electronic protected health information created, received, maintained and transmitted.



Jan 8, 2007

---

---

---

---

---

---

---

---

## Why is Security Important?



- Technology has allowed UMC to collect, maintain and automate large amounts of sensitive or personal information.
- We rely on this information to make decisions every day.
- Our patients may suffer from improper disclosures that can impact employment decisions, cause embarrassment, and have negative impacts in personal relationships and social interactions.



Jan 8, 2007

---

---

---

---

---

---

---

---

## Security Compliance at UMC

### UMC must:

- Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.
- Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required under the privacy rules.



Jan 8, 2007

---

---

---

---

---

---

---

---

## Examples of Threats to Information



- Theft (of equipment or information)
- Vandalism (to equipment or information)
- Snooping (for information someone has no authority to access)
- Environmental (power outages, fires, floods)



Jan 8, 2007

---

---

---

---

---

---

---

---

## The Basics of a Secure Information System

- Information is entered and processed correctly
- Authorized individuals have access to the minimum information to do their jobs
- Physical access to information systems resources is restricted. This also applies to removable media such as disks, CDs, DVDs, cameras, and hard drives.



Jan 8, 2007

---

---

---

---

---

---

---

---

## The Basics of a Secure Information System

- Changes are tested and approved before implementation.
- Data is regularly backed up and procedures are in place to operate during an emergency and to recover information if necessary.
  - Each department has "downtime" procedures to be used when the computers are not available. Be sure you know what they are.
  - The IS Department regularly backs up the network, you need to back up removable media only.

Jan 8, 2007



---

---

---

---

---

---

---

---

## What Can I Do?



- Comply with UMC's Information Security Agreement conditions for access.
- Use caution when entering information
- Be careful when overriding system defaults
- Verify you entered the information correctly

Jan 8, 2007



---

---

---

---

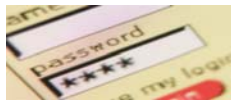
---

---

---

---

## Your Password



- Follow UMC IS guidelines on password selection.
- Keep your password safe, do not share it with anyone.
- UMC provides user IDs based on minimum necessary to complete job duties for your protection.
- Following UMC policy on passwords will protect you from being held responsible for actions done under your user name.

Jan 8, 2007



---

---

---

---

---

---

---

---

## What About E-Mail?



- Do not send unencrypted PHI outside UMC's network (only users with an address ending in umcsn.com are inside the network).
- Verify the email address before hitting send - there are sometimes two people with the same name in the Outlook address book.

The IS Department is working on an encryption solution so that e-mail can be safely used for communications with external agencies and clients in the future.

Jan 8, 2007



---

---

---

---

---

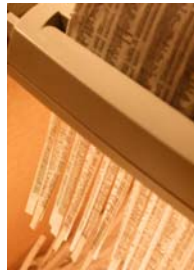
---

---

---

## What Safeguards Should I Use To Protect Information?

- Shred or recycle all documents containing individually identifiable information. Use the recycle bins to discard paperwork that has PHI on it.
- Keep printers, fax machines and copiers in secured areas.
- Do not discuss protected information in public areas, such as halls or elevators.



Jan 8, 2007



---

---

---

---

---

---

---

---

## What Safeguards Should I Use To Protect Information?



- Do not look at anyone's protected health information unless it is required for your job.
- Know the difference between gossip and a legitimate "need to know".
- Do not print or save PHI when accessing UMC webmail from outside network.
- Do not use cell phone cameras. UMC has digital cameras available for treatment purposes.

Jan 8, 2007



---

---

---

---

---

---

---

---

## What Other Safeguards Do I Use to Minimize the Risks?



### Protect Physical Access

- Control locations – know who is authorized to be in the area or to use the terminal.
- Lock equipment – cables can be used to secure terminals to desks.
- Use screen filters – only the user may see the screen.
- Label laptops – and use passwords to open them.
- Lock or shut down the computer when away from the desk.



Jan 8, 2007

---

---

---

---

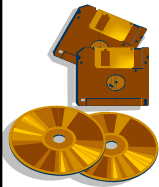
---

---

---

---

## Deleting Files



- All removable media such as disks, cds, cameras, or hard drives containing ePHI must be wiped using DOD approved software or physically destroyed before re-use or disposal.
- Information on media **CAN BE RECOVERED** even if files are deleted or the disk is formatted.
- Before destroying any ePHI, make absolutely certain the information is contained elsewhere or is no longer needed.
- Call the IS Help Desk if you have questions about safe disposal of equipment.



Jan 8, 2007

---

---

---

---

---

---

---

---

## Viruses



Viruses are a significant threat to UMC, and may result in lost productivity or reduced access to files and resources.

- Always check disks for viruses before using them.
- Do not open suspicious e-mails or open unknown attachments.
- Do not access web-based e-mail accounts from your work computer. (This is one of the most common ways to introduce a virus or worm into UMC's system because they do not get processed by our security tools, such as the anti-virus program.)
- Contact the IS Help Desk if you believe you have a virus.



Jan 8, 2007

---

---

---

---

---

---

---

---

## Incident Response



- UMC has an IS incident response plan.
- If you believe that your password has been compromised, contact the IS Help Desk immediately.
- If you suspect unauthorized access to or disclosure of confidential information, contact the IS Security Officer at 383-7397 immediately.

Jan 8, 2007



---

---

---

---

---

---

---

---

## Contacts



### HIPAA Program Management Office:

- Angela Darragh, Manager 383-6211
- Hope Hammond, Privacy Officer 383-3854
- Mac Mintz, UMC I.S.Security Officer 383-7397
- Michael Smith, Clark Co.Security Officer 455-0029
- HIPAA Privacy Hotline 383-7373
- HIPAA Security Hotline 671-1001

Jan 8, 2007



---

---

---

---

---

---

---

---

## Resources



- UMC Privacy and Security Policies, Procedures, Forms  
<http://umcintranet/hipaa/index.asp>  
UMC Administrative Policy manual
- Clark County Privacy and Security Policies
- Office for Civil Rights  
<http://www.hhs.gov/ocr/hipaa/>
- Centers for Medicare and Medicaid Services:  
<http://www.cms.gov/hipaa/>

Jan 8, 2007



---

---

---

---

---

---

---

---