A GENERAL INTRODUCTION TO HIPAA AND THE PRIVACY REGULATIONS FOR UMB PERSONNEL

This is a brief summary about new federal rules governing the privacy of health information. It defines basic terms and lists basic principles that all UMB Personnel must follow.

Objectives
You will learn:
- What HIPAA is
- The basics of the Privacy rule
- How HIPAA Privacy affects each of us
- The consequences of non-compliance with HIPAA Privacy rules
- Where to go with questions

WHAT IS HIPAA?
- Health Insurance Portability & Accountability Act of 1996
- HIPAA is a Federal law
- HIPAA establishes uniform rules for protecting Health Information and privacy
- Maryland law that is stricter than HIPAA and is more protective of health information privacy than HIPAA still applies

Basics of the HIPAA Privacy Rule
- UMB personnel cannot see or use Protected Health Information unless it is required for the job.
- UMB personnel can only see or use the minimum amount of Protected Health Information that is necessary for a task
- UMB personnel who see or use Protected Health Information in violation of HIPAA have violated federal law. Penalties include, fines, jail, and UMB disciplinary action, which may include termination or expulsion.

HIPAA Penalties
- $100 fine per day for each standard violation. (Up to $25,000 per person, per year, per standard.)
- $50,000 fine + up to one year in prison for improperly obtaining or disclosing health information.
- $100,000 fine + up to five years in prison for obtaining or disclosing health information under false pretenses.
- $250,000 fine + up to ten years in prison for obtaining health information with the intent to sell, transfer or use for commercial advantage, personal gain or harm.
- Penalties under University policy, which can include termination or expulsion.

Who Must Comply with the Privacy Rules?
- All UMB personnel including faculty, staff, students, residents, fellows, and volunteers who see or use Protected Health Information, including information from:
  - University of Maryland School of Medicine
  - University of Maryland Dental School
  - University of Maryland Medical Center
  - University Physicians, Inc.
  - Affiliated University of Maryland Faculty Practice Associations

What is "Protected Health Information"?
- Comes from a health care provider or a health plan
- Identifies an individual or
- Could be used to identify an individual
- Describes the health care, condition, or payments of an individual
- or the demographics of an individual.

Examples of Demographics:
- Name
- Address, phone number, fax number, e-mail address
- Birth date
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- License or certificate numbers
- Vehicle license number
- Web (URL) address
- IP address
- Biometric identifier (finger print, iris scan, etc.)
- Full-face photographic images (new baby photos on bulletin boards)
- Any other unique identifying characteristic

"Protected Health Information" Describes Health Condition
- Information from a health care provider or health plan about an Individual's Physical or Mental condition, including:
- Past history of a condition
- Present condition
- Plans or predictions about the future of a condition

"Protected Health Information" Describes Health Care

- Information from a health care provider or health plan about an Individual's Health Care, including:
    - Who provided care
    - What type of care was given
    - Where care was given
    - When care was given
    - Why care was given

"Protected Health Information" Describes Health Care Payments

- Information from a health care provider or health plan about an Individual's Health Care Payments, including:
    - Who was paid
    - What services were covered by the payment
    - Where payment was made
    - When payment was made
    - How payment was made

"Protected Health Information" must be secured in all forms

- Written information (reports, charts, x-rays, letters, messages, etc.)
- Oral communication (phone calls, meetings, informal conversations, etc.)
- E-mail, computerized and electronic information (computer records, faxes, voicemail, PDA entries, etc.)

When Can UMB Personnel Use Protected Health Information?

- When authorized by the School of Medicine, the Dental School, University Physicians, Inc., the Affiliated University Professional Associations, or the University of Maryland Medical Center
- When the individual has signed a valid authorization form
- As specifically permitted or required by law
- In all cases, use reasonable security measures to safeguard Protected Health Information

Reasonable Security Measures for Protected Health Information

- Use and do not share computer passwords
- Lock doors, lock file cabinets, and limit access to workspace where health information is used or stored
- Limit access to printers and faxes where health information is printed
- Limit access to health information to only those who need it for a specific task
- Redact or use de-identified health information whenever possible
- Shred or otherwise properly dispose of health information trash
- Use and keep only the minimum health information necessary for a specific task
- Follow privacy policies and procedures

Privacy - In Summary

- Keep Protected Health Information private and secure at all times
- Make sure only UMB Personnel who need to use Protected Health Information see it or use it
- Use only the minimum amount of Protected Health Information necessary to accomplish the task
- Read and understand UMB Privacy policies and procedures
- Know your Privacy Official
- Consult your Privacy Official with any questions you have about privacy or Protected Health Information

Privacy Rules -Next Steps
Additional HIPAA information and a PowerPoint presentation of this "General Introduction to HIPAA" is available on-line at www.umaryland.edu/cits/

- Some UMB Personnel will receive additional training about privacy that is designed to address a specific job or activity.
- Questions can be addressed to the Privacy Official in your school or administrative division or to the
    UMB Privacy Official:
    Dr. Peter Murray
    pmurray@umaryland.edu