



Compliance Training Module

Volume 3, Number 1

Contents

HIPAA Privacy Training March 2003 Rev. 10/06; 5/09

Behavioral Objectives

After completing the programmed study guide and/or watching the videotape, the participant will be able to:

1. Define what HIPAA is.
2. Name the six patient rights regarding protected health information guaranteed by the HIPAA Privacy rule.
3. Understand UMC staff member responsibilities regarding ensuring the privacy and confidentiality of patients' protected health information (PHI).
4. Name four safeguards for protecting the privacy and confidentiality of PHI.
5. Know who the UMC Privacy Officer is and how to address a privacy complaint.
6. Identify where to find the UMC policies on HIPAA.

α α α

Accompanying Activities

Consult the indicated references for a more in-depth review of University Medical Center's privacy compliance commitment.



What is HIPAA?

- ◆ HIPAA is the acronym for the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996.
- ◆ This act provides for fraud enforcement (accountability), insurance portability (continuity of coverage between health plans; no denial of coverage for pre-existing conditions); and Administrative simplification--Standardized Electronic Data Interchange (EDI)-- Transactions and Code Sets, to cut healthcare costs and to streamline operations, and Privacy and Security of patients' medical information.
- ◆ Implementation Dates: Privacy, April 14, 2003 EDI/Transactions, October 16, 2003 Security, April 21, 2005
- ◆ The Office of Civil Rights (OCR) is charged with enforcement of the HIPAA Privacy Rule.
- ◆ Health Care organizations that fail to comply with the HIPAA Privacy rule may receive criminal and civil penalties including fines and/or jail time. Criminal penalties up to \$250,000 and 10 years in jail may be issued for improperly disclosing patients' protected health information.
- ◆ All members of the UMC workforce must receive HIPAA Privacy training in order to ensure: 1) workforce members will do things right; 2) compliance with the law; and 3) minimization of UMC's exposure to sanction for non-compliance.

Culture of Health Care Privacy

- ◆ Patients and consumers are concerned about the use and release of their private information without their knowledge, including the transmission of their medical information over the Internet. Healthcare workers need to maintain patients' trust.
- ◆ When patients do not trust us they may fail to obtain needed treatment, give incomplete or inaccurate information, pay out-of-pocket to prevent an insurance claim, move from one physician to another for treatment and request that the doctor not document the patient's condition, care and/or treatment.
- ◆ We know that humans are curious by nature and healthcare workers have a tendency to become desensitized to patient privacy because they work with patients' medical information daily.
- ◆ Our goal is to change the personal behavior of UMC's workforce by enhancing our awareness of the need to maintain privacy and ensure the confidentiality of patients' protected health information.
- ◆ UMC's expectation is to develop a culture based on values, that ensures staff members' compliance with the UMC Code of Conduct that addresses confidentiality as its third principle.
- ◆ Protecting patient confidentiality and privacy results in quality healthcare.

What is Protected Health Information (PHI)?

- ◆ PHI is individually identifiable health information (IIHI) that is protected under the HIPAA Privacy rule if it contains any of the following identifiers: *Name; Street address (including city, county, precinct or zip code); dates including birth date, admission date, discharge date, date of death and age (except over 89); telephone numbers; FAX numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certification or license numbers; vehicle identifiers such as serial numbers and license plate numbers; device identifiers and serial numbers; URLs and internet addresses; biometric identifiers such as fingerprints, full face photographs and any comparable images; and any other identifying numbers, characteristics etc.*
- ◆ Protected PHI includes any paper records, oral communications and electronic information, and any media including photographs.
- ◆ When patients give us their protected health information they expect that only people in health care will see it.
- ◆ Confidentiality of patients' PHI is maintained by not sharing it with anyone, including co-workers, other patients, patients, visitors and in some cases family, or anyone else who may ask you about it who does not need to know.
- ◆ Your use of patients' PHI is limited to what you need to know to do your job — the "minimum necessary".
- ◆ The HIPAA Privacy rule covers all PHI in written or spoken format and the security provisions of HIPAA covers PHI in electronic format.

Patient Rights under HIPAA

Patients are guaranteed the following rights under HIPAA regarding their medical information:

1. Right to receive notice of UMC's privacy practices
2. Right to inspect and copy his/her own information
3. Right to request amendment of erroneous or incomplete information
4. Right to obtain an accounting of disclosures made for purposes other than treatment, payment or operations (TPO)
5. Right to request restrictions of use and disclosure for TPO
6. Right to request confidential communications.

What has UMC Done to Ensure Compliance with the HIPAA Privacy Rule?

- ◆ UMC identified a Privacy Officer, Valerie Evans, Corporate Compliance Officer, 694-5049.
- ◆ There is a process for reporting privacy concerns or violations--talk with your supervisor, talk with the Privacy Officer or call the UMC Alertline 800-726-0713.

- ◆ HIPAA Privacy policies and procedures have been developed and can be found on the UMC Intranet.
- ◆ UMC, UPH, AHSC and the UMC Medical Staff have formed an organized healthcare arrangement [OCHA]. The purpose of the OCHA is to provide for the sharing of patients' protected health information without having to obtain patient authorization each time this is done.
- ◆ UMC has a notice of privacy practices and distributes it to all patients. A condensed version will also be posted throughout the organization wherever patients are registered as in-patients or for outpatient services.
- ◆ UMC reviews all contracts and including a HIPAA Business Associate Agreement where applicable.
- ◆ UMC privacy compliance is provided for under the UMC Compliance Plan and the UMC Code of Conduct.
- ◆ UMC will take disciplinary action up to and including termination for breaches of privacy and confidentiality.

UMC promotes the use of safeguards to ensure the protection of patient privacy and confidentiality, including the following information security measures:

1. Do not to share computer passwords;
2. Change passwords frequently;
3. Do not leave patient data on screens;
4. Do not leave charts open on desks or counters;
5. Shred printed documents containing patient data;
6. Watch what you say in public areas; Minimize conversations about patients in hallways and talk in low tones.
7. Access only the patient data that you need to know to do your job;
8. Avoid gossip situations;
9. Report known or suspected privacy breaches;
10. Do not leave voicemails containing sensitive information;
11. Do not leave phone messages with sensitive information that other persons may hear;
12. Do not leave PHI in or around copy machines;
13. Avoid inadvertent disclosures among professionals;
14. Be careful with patient lists.
15. Follow the UMC E-mail and FAX policies for guidelines on transmitting protected health information.
16. Never photograph a patient using a personal cell phone camera or regular camera—even for teaching purposes. Always use business equipment.
17. Always obtain a patient's written consent if communicating via E-mail. Ensure consent is documented in the patient's medical record.

Your Responsibilities

- ◆ Be sensitive.
- ◆ Respect patients' privacy rights.
- ◆ Know where to find the UMC Privacy policies.
- ◆ Participate in training.
- ◆ Follow the UMC Code of Conduct.
- ◆ Report Privacy concerns or violations to your supervisor, the UMC Alertline or to the Privacy Officer.
- ◆ Talk with your supervisor if you have questions about patient privacy policies and procedures.



Glossary of Terms

HIPAA--Health Insurance Portability and Accountability Act

OCHA--Organized Health Care Arrangement

TPO--Treatment, Payment and Operations

PHI--Protected Health Information

IIHI--Individually Identifiable Health Information

References

1. The UMC Code of Conduct
2. The UMC Privacy Policies and Procedures (See the UMC Intranet at [HTTP://intranet.umcaz.edu](http://intranet.umcaz.edu))