The University of Chicago Medical Center
Office of Medical Center Compliance

Summary of
The HIPAA Privacy & Security Rules

Training Document

HIPAA PRIVACY RULE OVERVIEW

The Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 became effective on April 14, 2003. The federal government said that every employee working in healthcare in any job must be taught about the Privacy Rule. The Privacy Rule tells us how we are to use and share health information about patients. A major goal of the Rule is to assure patients that their health information will be protected.

The Privacy Rule applies to all members of the workforce of The University of Chicago Medical Center (UCMC) and includes all physicians, residents, medical students and permanent as well as temporary staff. This summary is being given to you to help you understand the Rule and how important it is to the patients and the Medical Center.

PROTECTED HEALTH INFORMATION

Protected Health information ("PHI") is anything that might reveal something about the medical or emotional condition of a patient. It is also information that might tell us who the patient is. Many different pieces of information can identify a patient or tell us something about their medical condition. Examples of things that might identify a patient or tell us something about their condition include a social security number, driver's license, state ID, fingerprints, name, address, and photographs, medical record number, labels, ID bands, and any reports or x-rays.

USE AND DISCLOSURE

An organization like the UCMC can use and disclose or share patient information without a patient's specific authorization if it is for treatment, payment, and healthcare operations.

Treatment is anything we may do to care for the patient for example talking about or to the patient, asking another doctor's opinion, and sending the patient for tests or to therapy.

Payment is sharing information in order to be paid for the services we have given to the patient.

Health Care Operations covers any activity that might be done for or with the patient to help them get better such as setting up home care, arranging transportation, obtaining a wheelchair. It also includes quality control, credentialing, and educating medical students, nurses, and other allied health professionals.

Sometimes we are required by law to disclose a patient's health information to a government agency. Child abuse, communicable disease, and medical examiner reporting are a few examples of disclosures to government agencies. It is important that we keep track of the places where we disclose or send information about the patient. If the patient wants to know where we have sent

information about them, we have to be able to provide a list. If the unit that you will be working in makes these kinds of disclosures, your supervisor will train you on how to keep track of them.

One way that we try to safeguard the privacy of our patients is by making sure that the person asking for any information about a patient has a right to get that information. So we must always make certain we identify the caller or visitor as someone the patient wants us to speak to. At the UCMC we have a password system in place to protect our patients and their information.

INCIDENTAL USE AND DISCLOSURE

It is very important that we try to limit the patient information that other people (like visitors) might hear while we are doing are jobs. We should speak in quieter voices when in public places and never discuss a patient or their condition in the elevators or cafeteria. We should always pull curtains in patient rooms, and ask visitors to step out while we finish our work or speak with the patient. We should make sure our workspace is clean and does not have patient information lying around for others to see.

All written information about patients that is no longer needed and is not part of the medical record, like report sheets, notes, labels, and post-its, should be placed in the shredding boxes and not thrown in the garbage.

AUTHORIZATIONS

For anything outside of treatment, payment, or healthcare operations, we need to get the patient's consent to share their health information or we are risking the patient's privacy. The law also tells us to share only the information that is absolutely needed. Only the patient can ask for and get a copy of his own medical information.

ENFORCEMENT AND PENALTIES FOR NON-COMPLIANCE

The Office for Civil Rights enforces the Privacy Rule.

Civil penalties for not obeying the Privacy Rule are tiered based on increasing levels of culpability:

Violation	**Each violation**	**Multiple violations in same year**
Violations occurred without the knowledge of covered entity and by exercising reasonable diligence would not have known it violated the HIPAA Privacy Rule	$100-$50,000	$1,500,00
Violations due to reasonable cause	$1,000 to $50,000	$1,500,000
Violations due to willful neglect but are corrected within 30 days	$10,000 to $50,000	$1,500,000
Violations due to willful neglect and are not corrected	$50,000	$1,500,000

Criminal penalties for a person who knowingly violates HIPAA are as follows:

- $50,000 and a one year prison term
- $100,000 and up to 5 years in prison for wrongful conduct involving false pretenses
- $250,000 and up to 10 years in prison for wrongful conduct with intent to sell, transfer, or use individually identified health information personal gain or malicious harm.

HIPAA SECURITY RULE OVERVIEW

The HIPAA Security Rule became effective on April 20, 2005. The Security Rule standards define how we are to ensure the integrity, confidentiality, and availability of our patients' electronic protected health information (ePHI). The Security Rule requires that we have administrative, physical, and technical safeguards for protecting ePHI. Some examples of each are:

Administrative Safeguards: administrative functions that should be implemented to meet the security requirements.

1. Assigning or delegating security responsibility to an individual – Chief Security Officer.
2. Training workforce members on security principles and organizational policies/procedures.
3. Terminating workforce members' access to information systems.
4. Reporting and responding to security incidents.

Physical Safeguards: mechanisms to protect electronic systems, equipment, and the data they hold, from threats, environmental hazards and unauthorized intrusion.

1. Limiting physical access to information systems containing ePHI (i.e. server rooms).
2. Preventing inappropriate viewing of ePHI on computers.
3. Properly removing ePHI from computers before disposing or reusing them.
4. Backing up and storing ePHI .

Technical Safeguards: automated processes used to protect data and control access to data.

1. Providing users with unique identifiers for accessing ePHI.
2. Accessing ePHI during an emergency.
3. Encrypting ePHI during transmission.
4. Automatically logging off users after a determined time period.

PRIVACY/SECURITY AND TECHNOLOGY

As we use technology to improve patient care, we are faced with additional challenges to protect patient information from unauthorized use and disclosure. It is important to understand the form of technology being used and the precautions we must take to safeguard patient information. The following are things to remember:

PASSWORD MANAGEMENT

Never share your password.

Your account is assigned to you. You will be held responsible for the activities of the account. We do see cases where people will use someone else's e-mail account to send harassing e-mail messages. Don't let this happen to you. There is never a real need to share your password. The IT systems have been designed to allow delegation of resources to multiple people without sharing passwords. Do you need to access someone's calendar? We can delegate those privileges; all we need is permission from the user. The same applies to file sharing, applications, websites etc. Don't share your password.

Never write down a password.

Passwords that are written down can be easily stolen. While receiving a new password you may wish to write down your password until you have a chance to memorize it. If you do this, you should take *extreme* care not to lose the paper you have written it on. You should destroy the paper (e.g. tear it to shreds) once you have learned the password.

If you MUST write down your password – never store it near your resource (computer).
Don't write your password down and stick it on your monitor! Some users have upwards of ten different passwords. That's a lot to memorize. Write them down and store them in your wallet. Never store them in your office, with your laptop or under your keyboard. You wouldn't store your ATM PIN with your debit card – would you?

Change your password with some frequency.
The longer you have used your password, the more likely it is that someone else will manage to figure it out. Just how frequently you should change your password depends on how frequently you use it and what you are protecting with it. For example, you may wish to change a password used to give access to patients' financial information more frequently than one to give access to read the news on a web page.

Never store your password in a program.
Many e-mail clients, web browsers, and web services will offer to store your password for you so that you don't need to type it in each time you want to use it. This is a bad idea -- it is generally easy for people to recover your password from inside one of these programs if they have access to your computer (and sometimes even if they don't). It is also possible for some computer viruses to recover your password from your computer and e-mail them to random people or post them publicly on the Internet. Such viruses may even distribute the password before anti-virus software is able to locate and remove the virus.

Create complex but easy to remember passwords.
The more complex a password the more difficult it is to crack. A password based on a dictionary word can be cracked in less than five minutes by a determined hacker with the proper tools. By contrast a complex password (i.e. longer than eight characters with upper & lower case letters, numbers and symbols), increases the time needed to crack a password to months. An easy way to create a password is to think of a sentence and use the first letter of each word in the sentence, leaving in the punctuation. For example, "I have three kids named John, Michael and Sarah!" becomes "Ih3knJ,MaS!".

LOCK/LOG-OFF COMPUTER WHEN FINISHED WITH SESSION

Help secure UCMC sensitive information and protect our patients' privacy. Would you leave your house without locking the front door? An unlocked computer is like leaving your doors unlocked. Remember, you are responsible for actions taken under your login!

Avoid pitfalls and consequences by playing smart… **LOCK** or **LOGOFF!**

Before leaving your computer, do one of the following (Windows workstations):

- Press Ctrl+Alt+Delete on your keyboard and then select "Lock Computer"
- Press Ctrl+Alt+Delete on your keyboard and then select "Log Off"

Protect our Patients . . . Protect Yourself . . . Remember to Log-Off

ACCESSING PHI

You may only access protected health information (e.g. electronic) for purposes necessary to perform your own job duties.

You may not access and/or copy their own medical information through the institution's current information systems, including test results, clinic notes, and operative reports.

You may not access through the institution's current information systems the medical information of family members, friends, or other individuals for personal or other non-work related purposes, even if written or oral patient authorization has been obtained.

In those very rare circumstances where your job requires you to access and/or copy the medical information of family members, a co-worker, or other personally known individuals, then you may do so only to the extent necessary to perform your job. However, you should report the situation to your supervisor who will determine whether to assign a different employee to complete the task involving the specific patient. You should continue your responsibilities to the extent patient privacy is not compromised.

CONCLUSION

Our patients entrust us with their health information; therefore we must protect it against deliberate or inadvertent misuse or disclosure. The consequences of not complying with HIPAA are too great.

We do not want to see the University of Chicago Medical Center's name in the newspaper associated with a systems attack or theft of patient information. So, it is imperative that we all follow our privacy and information security policies, and do the right thing . . . protect our patients' privacy and confidentiality of their health information.

The following page is a list of HIPAA tips on protecting our patients' privacy, and information and security of their health information. In addition, please feel free to go to the HIPAA Program Office website at http://HIPAA.bsd.uchicago.edu for additional information and resources.

THE UNIVERSITY OF CHICAGO
HIPAA Program Office

GUIDANCE January 2007

A to Z: HIPAA TIPS for PROTECTING PRIVACY AND SECURITY

A. Contact Security Services if you see suspicious individuals in patient care or restricted areas.

B. Wear your ID badge at all times.

C. Discard documents containing patient information only in a shredding container.

D. Discard floppy disks or CD-ROMs containing patient information only in shredding containers

E. Use private areas to discuss PHI. Do not discuss patient information in cafeterias, elevators, or other public places.

F. Lower voices when having conversations concerning patients in non-private areas.

G. Report any suspicious activity appearing on your computer to the IS Help Desk.

H. Do not leave messages concerning a patient's condition or test results on answering machines. Do not leave messages containing highly confidential patient information (i.e. mental health, substance abuse, HIV/AIDS, genetic testing, etc.) on answering machines.

I. Do not open unknown email attachments or unrecognizable emails.

J. Do not access protected health information unless it is necessary to perform your job duties, including that of your friends, family members, and colleagues.

K. Use private areas to discuss patient information with patient, family, or visitors.

L. Access only electronic information that you “need to know” to perform your job.

M. Log-off your computer when away from your workstation.

N. Turn computer monitors so they cannot be viewed by unauthorized persons.

O. Verify caller’s identity or applicable code before releasing patient information by phone.

P. Lock laptop computers and other portable devices in secure location when not in use.

Q. Store passwords in secure areas - not accessible by others.

R. Remove patient information from copy machines, fax machines, printers, or conference rooms.

S. Obtain patient verbal permission before discussing information in front of family and friends.

T. Do not share your computer user ID or password with anyone.

U. Do not access your PHI or PHI of family members, friends, or other individuals for personal or other non-work related purposes even if written or verbal authorization has been obtained.

V. Medical records should not be taken away from the UCMC campus or off-site property.

W. Clinic schedules, surgery schedules, and procedure schedules that contain PHI should not be left out in view of others. When no longer needed, schedules should be placed in shredding bins, not regular trash cans.

X. If you do not need PHI to do your job, do not seek it out.

Y. If you overhear a conversation concerning a patient, keep it to yourself.

Z. Report suspected privacy violations to the HIPAA Program Office by calling (773) 834-9716.

THE UNIVERSITY OF CHICAGO MEDICAL CENTER
OFFICE OF MEDICAL CENTER COMPLIANCE

CONFIDENTIALITY AGREEMENT

I understand that I will have access to protected health information (PHI) PHI is anything that identifies or could lead to the identification of a patient or reveals something about the patient's health status.

I understand that any information that I learn about a patient, including the fact that a person is a patient, is confidential under the laws of Illinois and the United States and that information about a patient cannot be disclosed to anyone. I understand that Illinois and federal law provides for possible civil and criminal penalties for disclosure of confidential patient information.

I agree that I will hold PHI in the strictest confidence and will **NOT**:

- Reveal to anyone the name or identity of a patient.
- Repeat to anyone any statements or communications made by or about the patient.
- Reveal to anyone any information that I learn about the patient as a result of reviewing medical records or from discussions with others providing care to the patient.
- Make any copies of, release, sell, loan, review, alter, or destroy any medical records or other medical and/or Confidential Information.
- Give access to medical information to anyone not authorized by UCMC to have access.

I have read this statement. I understand my obligation to maintain patient confidentiality and I agree to follow that obligation. I understand that if I breach my obligation to maintain confidentiality, my access to UCMC information systems will be immediately revoked and I may be subject to disciplinary action.

_____

Print Name

_____ _____

Signature **Date**

_____

Organization Name

_____

Supervisor's Name

This page should be maintained by the UCMC department.

.

ATTESTATION FOR HIPAA TRAINING
COMPLETION OF HIPAA OVERVIEW

I _____have read the material about HIPAA that was given to me. I understand the information about the Privacy and Security Rules and how important it is to patients at the University of Chicago Medical Center. I understand a copy of this signed document will be kept on file as proof that I have completed my HIPAA training.

NAME (PRINT) _____

SIGNATURE _____ DATE _____

ORGANIZATION _____

UCMC CONTACT _____

This page should be maintained by the UCMC department.