Uhicago Medicine & Biological Sciences
HIPAA Privacy Program

Summary of HIPAA Privacy & Security Rules

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 Department of Health and Human Services published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005. HIPAA governs the use and disclosure of protected health information and the protections that must surround it. The fundamental question always centers around what is the purpose of the use and disclosure

UChicago Medicine, a HIPAA covered entity, is part of an Organized Health Care Arrangement (OHCA) which includes the UChicago Medicine and its subsidiaries, the University of Chicago Biological Sciences Division along with other portions of the University of Chicago that support health care activities, the UChicago Medicine Community Physicians. The HIPAA regulations apply to all members of our workforce; our workforce means faculty, staff, volunteers, students, and all others whose conduct, in the performance of work for the UChicago Medicine, is under its direct control, whether or not they are paid by an entity within the Medical Center. This includes the Biological Sciences division. This summary is being given to you to help you understand the Rule and how important it is to our patients.

KEY TERMS TO KNOW

- ***Individually Identifiable Health Information*** (IIHI) is a subset of health information that is created or received by a health care provider, health plan, employer or health care clearinghouse which relates to the past, present or future physical or mental health condition of an individual; provision of health care to an individual or payment for that health care that identifies the individual or can reasonably be used to identify the individual.

- ***Protected Health Information*** **(PHI) means IIHI that is transmitted by or maintained in any form or medium by a covered entity.** Many different pieces of information can identify a patient or tell us something about their health care or their medical conditions.

Examples of things that might identify a patient or tell us something about their condition include social security number, driver's license number, fingerprints, name, address, photographs, medical record number, labels, ID bands, and medical record documentation, reports and diagnostic imaging or laboratory results.

- ***Highly Confidential Information*** (HCI) is a subset of PHI and includes information related to abuse or neglect of a child, elderly person, or adult with a disability, domestic abuse, alcohol and drug abuse prevention and treatment, genetic testing, HIV/AIDS testing, diagnosis, and treatment, in vitro Fertilization, infertility, artificial insemination, mental health and developmental disabilities, psychotherapy notes, communicable diseases, sexually transmitted diseases, and sexual assault. Extra care should be taken to keep highly confidential information protected. For example, obtain the patient's verbal permission before discussing highly confidential information in front of family and friends.

HIPAA BASICS

- You may access, use, or disclose PHI for purposes related to ***Treatment, Payment or Operations (TPO)*** without patient authorization.

  Treatment is anything we do to care for the patient (providing, coordinating and managing a patient's health care); for example inter-disciplinary care planning, talking to the patient or family, asking another doctor's opinion, performing diagnostic testing and ordering or referring services.

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

  Health Care Operations are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. It includes quality control and improvement, credentialing, reviewing competence or qualifications of our health care professionals and educating medical students, nurses, and other allied health professionals.

  If your access, use, or disclosure is not for TPO and not otherwise covered by the UChicago Medicine Notice of Privacy Practices (NPP), an authorization from the patient must be obtained prior to proceeding.

- If you De-Identity a patient's health information through an expert determination or safe harbor (removal of all 18 PHI identifiers) you may use or disclose it without restriction. Contact the Privacy Program for more information about de-identification or refer to Policy A05-22 Use and Disclosure of Limited Data Set and De-identified Health Information.

- The ***Minimum Necessary Standard*** requires that you limit your access, use, disclosure or request for PHI to the smallest amount required to accomplish your purpose, and that you share PHI only with parties who have a need to know This includes when you are looking in medical records, discussing patient information, or collecting, displaying, or releasing PHI.

- ***Snooping*** is when a workforce member accesses the record of a patient for a non-job related reason. If you are caught snooping, you are subject to disciplinary action, up to and including termination. This zero tolerance includes access to the records of your spouse, domestic partner, siblings, children, grandchildren, relatives, co-workers, friends, neighbors, and persons of media interest including but not limited to political, public, sport figures and celebrities.

- ***Accessing your own record:*** You may access, view, and print your own electronic medical record if you already have work-related access to UChicago Medicine medical record systems. However, you *may not* edit or make changes to your information and schedule appointments or tests.

HIPAA ESSENTIALS

- **Verbal Information**
  - Implement steps to minimize incidental uses or disclosures of PHI by lowering your voice, moving conversations to more private areas, or asking patients to step back if they are in line.
  - Avoid discussing patient information in public areas such as hallways, the cafeteria, or elevators.
  - Obtain the patient's verbal permission before discussing any information in front of family and friends, particularly highly confidential information.
  - Do not leave messages concerning confidential patient information on answering machines.

- **Electronic Information**
  - Do not download and store patient information on your unencrypted personal electronic devices. This includes PHI maintained on all computers, flash drives, smart phones, iPads, pagers or any other unencrypted electronic device. Store PHI on UCM/BSD secure servers.
  - Encrypt all of your devices (workstations, laptops, mobile devices, USB thumb drives).
  - Do not use Dropbox, Google Docs, SkyDrive or other "cloud file storage utilities" without authorization.

❖ **Social Media**

- Social Media (i.e., Facebook, Twitter, YouTube, Instagram, etc.) is not the place for UCM information, images or comments. Only those individuals who have been approved may post to UCM social media sites.

❖ **Hard Copy Information**

- Do not take PHI off the premises. If you do, you are responsible for securing the information from unauthorized access (i.e., do not leave it unattended in your car, bag, home, public transportation, etc.). Keep it secured and with you at all times.
- When faxing, verify the fax number and recipient is correct before sending the documents.
- Before mailing documents with PHI, verify that you are sending the correct documents to the right recipient.
- If you give a patient his/her appointment information (i.e. After Visit Summary), double-check that you do not accidentally hand them another patient's paperwork.
- Discard documents with PHI in a HIPAA shredding container. Do not place it in the recycle or trash bins.

❖ **E-mail**

- Only use your UCHospitals or BSD e-mail address for work-related business.
- NEVER use your UChicago, Yahoo, Gmail or other personal e-mail accounts to correspond about patients.
- DO NOT put PHI in the subject line of emails and limit the PHI in the body of the e-mail to the minimum necessary. Avoid sending HCI via email.
- Do not access e-mail from unencrypted portable devices.
- Do not send your personal information over email.
- Check and double-check to ensure you are sending the email to the correct person. Watch out for autocorrect, similar names, autocomplete and mass distribution lists.

❖ **E-mail Encryption**

- Email sent from a UCHospitals or BSD email account to an external third party (i.e., Hotmail, Gmail, etc.) can be encrypted using Secure Email Service.
- When it is appropriate to email PHI to an external third-party, using #encrypt is required.
    - To encrypt the email, simply type #encrypt next to the subject title in the Subject Line. Click "Send" which will trigger the email system to send the email with encryption over the internet.
    - The recipient will receive a message with a link to instructions for registering to the secure email portal. Registration involves providing a name and creating a password. Once the recipient has registered, he will be able to access the encrypted email using his new password.

- Recipients can reply to the sender and others in the email, but are not permitted to forward the email to any contact other than those included in the original email.
- Detailed instructions can be found at http://home.uchospitals.edu/pdf/uch_042980.pdf

❖ **Pagers**

- Be mindful about any information being sent through a text page and remember to send the minimum necessary to convey your message. Report lost or stolen pagers as soon as possible so it can be immediately disabled.

❖ **Faxed Information**

- Double check manually-entered fax numbers before pressing send and check pre-programmed fax numbers regularly to ensure they remain correct.
- Remove PHI and other sensitive information from the fax machine in a timely manner; contact the recipient to verify that he/she is waiting at the machine prior to faxing "highly confidential information" (e.g. HIV/AIDS, Mental Health, Genetic Testing).

❖ **Password Habits**

Security breaches can and do occur due to bad password habits. <u>You should understand that it is a violation of UCMC Policy to share your passwords with anyone.</u> Follow the guidance below:

- Never share your password or store it on your laptop, phone or in any other unsecure location (such as under your keyboard or taped to a monitor).
- IT will never ask you to turn over your password. Report any attempts to do so the Information Security Office (702-3456).
- Create unique passwords with complexity (i.e., letters-upper/lower case, numbers, special characters).
- Lock/log-off your computer when away from your workstation. An "open" session exposes you to the possibility of an unauthorized individual accessing, altering or deleting PHI or other confidential information under your username/ID.

PHI Disposal

- All paper documents (encounter forms, EKG strips, clinical notes, call logs, etc.) containing PHI must be disposed of in the shredding containers located throughout the Medical Center campus.
- PHI must not be discarded or temporarily held in wastebaskets, recycling bins or other accessible locations.
- Do not over stuff locked shredding containers with PHI so that the items are sticking out of the open drop slot.
- If HIPAA Shred containers are broken or full, call EVS (773) 795-5537, select Option 1

- Do not throw away computers, USB drives, CD/DVDs or other electronic media without destroying or sanitizing them.
- For assistance with UCM Computers, call CBIS (773) 702-3456.

SOCIAL ENGINEERING ATTACKS

Social Engineering is the practice of malicious people attempting to trick YOU into sharing sensitive information about the organization, our patients, or yourself.

Rather than "hacking," - using a computer to gain unauthorized access to sensitive information - social engineers will attempt to get this information from you directly. This process is much easier than sophisticated attacks. They might try a number of avenues, such as:

- Sending a phishing email asking you to divulge information, click on a link, or open an attachment. The email may appear to be from your bank, the government, or a co-worker asking you to provide information.

- Calling you on the phone and posing as someone authorized to have access to information. They might ask for your sensitive information, ask to divulge financial information, or ask you to provide them with access.

- Asking you to open a door, or follow you through open doors to get access to physical facilities. The perpetrator can steal physical documents or even computers once inside a building.

For everybody's protection, follow these guidelines:

Email

- Do not open unsuspecting attachments
- Do not operate your computer as an "administrator"
- If you need administrative access use a separate account for those needs
- Do not click on suspicious links in emails, especially those that ask you to input your username and password
- Be cautious of any site that asks for your login credentials
- Do not access email from unencrypted portable devices

Phone

- Maintain a high level of awareness on conversations
- Be suspicious of any person who calls you unsolicited and asks for sensitive information, or institutional information
- Never share your password over the phone

Physical

- Challenge any visitor without a badge following you into a facility
- Do not hold doors into secure facilities for others
- Do not leave PHI on your desk

EMAIL CACHING

When you connect your desktop, laptop, or mobile device to the UCM or BSD email system, the device stores your emails on the local hard drive. *A loss of an unencrypted device that stores email will require a forensic analysis to determine if a breach has occurred.* Any PHI discovered in such an analysis, that is unencrypted, could result in a breach. *Contact the CBIS Service Desk for assistance or to report suspicious activity.*

BREACH INCIDENTS

A breach is the impermissible access, use or disclosure of PHI. Examples of breaches include sending a letter for patient John Smith to patient Joan Smith, or the theft of an unencrypted laptop that contains PHI.

If you are involved in, or suspect, a breach, notify the HIPAA Privacy Program immediately and your supervisor. Be prepared to provide

- a detailed report of how the incident occurred (how, when, who was involved and where),
- how you tried to mitigate any harm from the incident (i.e., asking the recipient to delete an e-mail, immediately retrieving the PHI, calling CBIS or security), and
- the nature and extent of PHI involved

BREACH OBLIGATIONS

After the incident has been reported, the HIPAA Privacy Program will conduct an investigation. All incidents are assumed to be a Breach unless a risk assessment indicates there is a low probability the PHI has been compromised.

UChicago Medicine has the following obligations when it is aware of a Breach:

- Notify all affected patients no later than 60 days after becoming aware of the breach
- Report the breach to HHS in its annual report

For breaches involving 500 or more individuals, UChicago Medicine is also required to contact the media, place a notice on its website, and report the breach to the Department of Health and Human Services (HHS) immediately (rather than annually).

Disciplinary Action: Workforce members who violate our HIPAA Privacy and Security policies will be subject to appropriate disciplinary action as outlined in our policies.

ENFORCEMENT AND PENALTIES FOR NON-COMPLIANCE

The Office for Civil Rights within HHS 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.

Analytics Core

Requests for PHI that will be used for operational purposes must meet the Privacy Rule definition of the health care operations. Data requests may be submitted through the Analytics Core request system (ACReS). The Analytics Core is a collaboration of leaders from several analytic teams to help you obtain useful information from the various systems at the University of Chicago. The role of the Analytics Core is to: simplify the data/analytics request process, ensure routing to the correct data/analytics provider, reduce duplicative data/analytics work, and promote QI initiatives and research projects. More information about the Analytics Core can be found here: http://data.bsd.uchicago.edu/analyticscore/.

Privacy and Security Policies:

All UChicago Medicine HIPAA Privacy and Security Policies can be found on the intranet website at http://home.uchospitals.edu/.

Privacy and Security Contacts and Resources

Erik Decker is The UChicago Medicine Chief Security and Privacy Officer.

Erik Decker, Chief Security and Privacy Officer
773-834-5471; erik.decker@uchospitals.edu

Karen Habercoss, Deputy Privacy Officer
773-834-2563; khabercoss@bsd.uchicago.edu

Paul Yates, Assistant Director, Information Security
773-702-3207; paul.yates@uchospitals.edu

The HIPAA Privacy Program website http://hipaa.bsd.uchicago.edu contains links to a variety of resources such as guidance documents, Authorization Forms and medical record request forms. The Information Security Office resources along with the HIPAA Privacy and Security policies are accessible on the Intranet.

- CBIS Service Desk: help@bsd.uchicago.edu or 702-3456
- HIPAA Privacy Program: hpo@bsd.uchicago.edu or 834-9716
- Anonymous Resource Line: 1-877-440-5480, select option 2.
- UCM Information Security Office: security@uchospitals.edu
- BSD Information Security Office: security@bsd.uchicago.edu
- ITS Security: Security@uchicago.edu
- Campus Security: 773-702-8181
- Public Safety: 773-702-6262

ATTESTATION FOR 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 UChicago Medicine and Biological Sciences. 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 _____

UCM CONTACT _____