THE UNIVERSITY OF CHICAGO MEDICINE & BIOLOGICAL SCIENCES

GUIDANCE | **HIPAA TIPS- Staff Guide to HIPAA Privacy and Security** | **June 2017**

TRAINING REQUIREMENTS

Faculty, staff, volunteers, and students of the University of Chicago Medical Center (UCMC) and Biological Sciences Division (BSD) are required to take HIPAA Privacy and Security training within 45 days of being hired and on an annual basis.

KEY TERMS

❖ ***Protected Health Information*** (PHI) is individually identifiable health information that is transmitted or maintained in any form (paper, electronic, oral) by UCMC or its Business Associates which relates to the patient's physical or mental health, or provision of or payment for health care.

Examples of PHI include medical records, x-rays, test results, and billing records.

❖ ***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.

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

❖ 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.

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 applies to the records of your spouse, domestic partner, siblings, children, grandchildren, co-workers, friends, neighbors, public 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 the UCMC medical record systems.

However, you may not edit or make changes to your information.

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, providing an AVS or discharge summary to the wrong patient, or the theft of an unencrypted laptop that contains PHI. If you are involved in, or suspect, a breach, notify your supervisor and the HIPAA Privacy Program immediately. Be prepared to provide

- a detailed report of how the incident occurred (how, when, 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

THE UNIVERSITY OF CHICAGO MEDICINE & BIOLOGICAL SCIENCES

HIPAA ESSENTIALS

❖ *For Verbal Information*

- Avoid discussing patient information in public areas such as hallways, the cafeteria, or elevators.
- 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.
- 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.

❖ *For Electronic Information*

- Do not download and store patient information on your personal electronic devices. This includes PHI maintained on all computers, flash drives, smart phones, ipads, pagers or any other electronic device. Store PHI on UCMC secure servers and use encryption methodologies.
- Never share your password or store it on your laptop, phone or in any other unsecure location.
- Log-off your computer when away from your workstation and lock laptop computers and other portable devices in a secure location when not in use.

❖ *For Social Media*

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

❖ *For Hard Copy Information*

- Do not take PHI off the premises. If you do, you are responsible for securing the records from unauthorized access (i.e., do not leave it unattended in your car, bag, home, public transportation, etc.). Keep it secured and on 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 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.

❖ *For E-mail*

- Only use your UCHospitals or BSD e-mail address for work-related business.
- NEVER use your Hotmail, Yahoo, Gmail or other personal e-mail accounts.
- 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.
- Do not access e-mail from unencrypted portable devices.

❖ *For PHI Disposal*

- Shred containers, call EVS (773) 795-5537, Option 1
- UCMC Computers, call CBIS (773) 702-3456

HIPAA PRIVACY PROGRAM RESOURCES

The HIPAA Privacy Program website contains links to a variety of resources such as HIPAA Authorization Forms, medical records request forms, guidance documents, and links to the HIPAA Privacy and Security Policies.

To ask questions or report concerns, you may contact us using any of the following methods:

- Compliance Hotline: 1-877-440-5480 (use this line if you wish to remain anonymous)
- HIPAA Privacy Line: 773-834-9716
- E-mail: hpo@bsd.uchicago.edu
- Program Website: http://hipaa.bsd.uchicago.edu/