THE UNIVERSITY OF CHICAGO
HIPAA Program Office

HIPAA QUICK REFERENCE GUIDE FOR EMPLOYEES

Did you ever find yourself in a situation and wonder, hmm, does HIPAA allow me to do that? We thought so. That's why we've created this quick reference guide. Here you will find the most frequently asked questions and their answers. It is important to note, that for most of these, more detailed information is available on the HIPAA website.

But, speaking of the website – did you know we have a HIPAA website? Yes we do and you can find it here: http://hipaa.bsd.uchicago.edu/

If you have questions or suggestions for how we can improve this reference, please give us a call at the HIPAA Program Office at 4-9716 or stop by in L147 located on the first floor of the Wyler building.

This Guide is intended for the use of the employees of the University of Chicago Medical Center (UCMC) and the University of Chicago Biological Sciences Division (BSD). These organizations are referred to as "we" or "us" or "our" throughout the questions. The locations are referred to as "the Medical Center". If you are not sure if this document applies to you, please contact the HIPAA Program Office.

The University of Chicago Organized Health Care Arrangement or "OHCA," includes physicians, nurses, residents, and other staff at the University of Chicago Medical Center.

Table of Contents

HIPAA QUICK REFERENCE GUIDE FOR EMPLOYEES

Resources for questions and training	**There are some HIPAA questions regularly coming up in my work area. I know we have all had the required new employee HIPAA training, but a refresher class might be really helpful.** It is always good to talk about a potential HIPAA problem early before it becomes an actual problem. The HIPAA Program Office staff will be happy to discuss and plan an education session to fit your specific needs. If you would like to schedule a Refresher Training, just call the HIPAA Program Office at 773-834-9716. Sometimes a problem can result in an employee or patient concern being reported to the HIPAA Program Office. In this case, we would recommend a Refresher Training be scheduled so everyone is aware of the problem and the solution. **Who can I call if I have questions about HIPAA?** The HIPAA Program Office is available if you have questions about patient privacy and confidentiality. This includes questions on existing processes or functions you perform as well as new processes, programs, or initiatives you are considering that involve patients and protected health information (PHI). Contact the HIPAA Program Office early in your planning process so we can provide guidance and help you ***do the right thing***. **What should I do if I want to file a patient privacy complaint?** You can file a complaint by contacting: 1. The HIPAA Program Office directly at (773) 834-9716, if you don't want to be anonymous. 2. The toll-free Compliance Resource Line at 1-877-440-5480, if you wish to be anonymous. The Compliance Resource Line is available 24 hours a day. The HIPAA Program Office will investigate all complaints, work with the appropriate UCMC and BSD Departments on resolving them, and apply disciplinary action when appropriate.
HIPAA Hero	**Who is a HIPAA Hero?** A HIPAA Hero is someone who observes, or has information regarding an incident, administrative procedure, or practice that may violate our patients' privacy or confidentiality of their health information. This person would contact the HIPAA Program Office (HPO) at (773) 834-9716 or stop by L147 to discuss the issue. Sharing this information may prevent a HIPAA violation or a patient privacy breach from occurring now and in the future.

Terms

What is "PHI"?

Protected Health Information is health information about a patient held by health care providers and health plans. This includes things like:

- Patient's medical record number
- Patient's demographic information (e.g. address, telephone number)
- Information doctors, nurses and other health care providers put in a patient's medical record
- Images of the patient
- Conversations a doctor has about a patient's care or treatment with nurses and others
- Information about a patient in a doctor's computer system or a health insurer's computer system
- Billing information about a patient at a clinic

Thinking about it another way, Protected Health Information (PHI) is any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual.

What is meant by "use"?

Use means, with respect to individually identifiable health information, any sharing, application, utilization, examination, or analysis of such information within the physician practice, hospital or clinic that maintains such information.

What is "disclosure"?

Disclosure is the release, transfer, provision or access to or divulging health information in any manner information outside the Medical Center.

What does HIPAA mean by "treatment"?

Treatment is when a health care professional provides, coordinates or manages the health care services of one or more providers. This includes coordinating or managing the care with someone outside the Medical Center, consulting with other providers or referring the patient for health care to another provider.

What does HIPAA mean by "payment"?

Under HIPAA, payment means the activities we perform to get reimbursed for the health care services we have provided. For instance, determining eligibility of coverage, billing, claims management, collection activities, review of health care services with respect to medical necessity, utilization review activities and disclosure to consumer reporting agencies in an effort to collect reimbursement.

What does HIPAA mean by "health care operations"?

Under HIPAA, health care operations include activities that ensure our effective business operations. These include, but are not limited to conducting quality assessment and improvement activities, reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs, accreditation, certification, licensing, or credentialing activities, conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs, business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment.

What is "authorization"?

An Authorization is an individual's signed permission to allow healthcare professionals to Use or Disclose their protected health information (PHI) for reasons generally not related to treatment, payment or health care operations. The Authorization must include: a detailed description of the PHI elements to be disclosed, the person who will make the disclosure, the person or entity to which the disclosure will be made, an expiration date, and the purpose for which their PHI will be used.

What is "OCR"?

OCR is the acronym for the U.S. Office for Civil Rights. The OCR is responsible for enforcement of the HIPAA Privacy regulations.

Highly Confidential Information

I've heard the term highly confidential information, what's the difference between highly confidential information and protected health information?

Illinois state law has provided strict protection of certain health information, which we refer to as "highly confidential". We are required to treat this information with special care.

How do I know if the patient information I work with each day is considered *Highly Confidential*?

Highly Confidential Information includes:

- Psychotherapy Notes (which are not part of the official medical record)
- Information about a Mental Illness or Developmental Disability
- Information about HIV/AIDS Testing or Treatment (including the fact that an HIV test was ordered, performed or reported, regardless of whether the results of such tests were positive or negative)
- Information about Communicable Diseases
- Information about Venereal Disease(s)
- Information about Substance (i.e., alcohol or drug) Abuse
- Information about Genetic Testing
- Information about Child Abuse and Neglect
- Information about Abuse of an Adult with a Disability
- Domestic Abuse/Violence
- Information about Sexual Assault
- Information about Artificial Insemination

Would I do anything differently when handling highly confidential information vs. PHI?

Extra precautions should be taken with Highly Confidential Information such as:

- Even though a patient may have agreed to have a family member present when you are discussing the patient's general health, you should always check with the patient before discussing highly confidential information in the presence of family and/or friends.
- While a patient may have given you permission to leave messages on an answering machine, you should never leave a message asking the patient to return a call concerning their HIV test results.

Additional guidelines are available in the *Minimum Necessary Policy* on the HIPAA Website at: http://hipaa.bsd.uchicago.edu/policies.html - click on A05-31/PC 77 Minimum Necessary Requirements

I have a signed form authorizing the use and disclosure of information to a patient's assistant. Can I release *Highly Confidential* Information?

First, you must determine if you need a consent to release medical information form or an authorization to release medical information form. Then, the form that you need must specifically identify the particular Highly Confidential Information that you may release. For example, if you have a signed consent to release medical information to a patient's payer, the consent must also include language specifically permitting you to release the patient's HIV/AIDS testing and treatment information. For another example, if you have a signed authorization releasing the patient's mental health records from January 1, 2005 through the present to his lawyer, then you may release the mental health information for the specified time.

For questions, please contact Legal Affairs at (773) 702-1057.

Faxing Patient Information	**Can I fax protected health information (PHI) to someone within the Medical Center?** Yes, if they have a legitimate need to know. Please read this section for more detailed instructions for faxing. **Can I fax protected health information (PHI) outside the Medical Center when the information is needed quickly for a legitimate need to know such as:** ▪ **for an emergent patient care encounter,** ▪ **for arranging services with another provider (i.e. continuity of care),** ▪ **for a referring physician,** ▪ **for mandated reporting requirements, or** ▪ **for approval of services or to facilitate payment?** Yes, but limit the amount of information being faxed to the minimum amount necessary. Please read this section for more detailed instructions for faxing. **Do I have to do anything special when faxing patient information?** Each fax should be accompanied by a fax cover sheet – available on the HIPAA website at http://hipaa.bsd.uchicago.edu/fax_cover_sheet.doc Faxing of highly confidential information is not recommended. Faxing of highly confidential information is only permitted if the sender first calls the recipient and confirms that the recipient or his/her designee can be waiting at the fax machine, and then, the recipient or his/her designee waits at the fax machine to receive the fax and then calls the sender to confirm receipt of the document. Both the sender and the recipient must be attentive to the sensitive nature of highly confidential information. [NOTE: Highly confidential information (as described in more detail in the highly confidential information section of this Guide) is information related to the treatment of any of the following: Mental Illness or Developmental Disability, HIV/AIDS Testing or Treatment, Communicable Diseases, Venereal Disease(s), Substance (i.e. alcohol, drugs) Abuse, Abuse of an Adult with a Disability, Sexual Assault, Child Abuse and Neglect, Genetic Testing, Artificial Insemination, and Domestic Violence.] **What if I fax something to the wrong place?** If the fax was transmitted to the wrong recipient, in all cases follow these steps: ▪ Fax a request to the incorrect fax number explaining that the information has been misdirected, and ask that the materials be returned or destroyed. ▪ Document the incident by logging the inappropriate disclosure in the "DisclosureTrac" system and notify the HIPAA Privacy Office at 4-9716. ▪ Verify the fax number with the recipient before attempting to fax the information again. More details and the fax cover sheet are available in the HIPAA Faxing Guidance on the HIPAA Webpage http://hipaa.bsd.uchicago.edu/faxing.html
FAX Machine Setup	**Is there anything I have to be aware of when setting up my fax machine?** Yes. A few notes on fax machines: ▪ Fax machines used for sending and receiving patient information must be placed in a secure location. ▪ Incoming faxes should be removed timely from the output tray and distributed to the recipient to reduce the chance of an inappropriate use or disclosure. ▪ Pre-programmed numbers should be validated periodically and regular fax recipients should be reminded to provide notification in the event their incoming fax number changes. ▪ If the fax machine supports the feature to print the fax number on outgoing faxes, set the feature.

Responding to questions about a patient	**What can I tell an inpatient's family members or friends when they call and ask about a patient?** If the person inquiring can provide the patient's 4-digit code and the patient has not requested that information be withheld, we can release information relevant to the patient's current medical care (e.g. the patient's condition after surgery). If the inquirer can not provide the patient's 4-digit code, only directory information can be released, which includes the patient's name, location (e.g. room number), and the patient's general condition, such as fair, stable, or good. **Is the patient's authorization needed to release directory information?** No. If the patient has not exercised his/her right to "opt out" of the directory at the time of admission, the patient's authorization is not needed to release directory information. [Directory information consists of confirming that the patient is in-house when given a name and providing the room number and phone number.] **What if a patient doesn't want anyone to know he/she is admitted?** A patient has the right to request that information regarding his/her stay not be given to anyone outside the treatment team by notifying the Admission department staff that he/she wants to "opt out" or not be listed in the patient directory.
Looking up information about family and friends	**Can I access my family member's, friend's, or co-worker's PHI (e.g. electronic, written)?** Employees may not access either through our information systems (e.g. OACIS, EPIC, or Lastword) or the patient's medical record the medical and/or demographic 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 given. **What if my child or parent is a patient here?** Employees designated as "Personal Representatives" (e.g. parent for a minor, adult son/daughter for an elderly parent) should contact the physician, clinic, or submit a formal request to the Health Information Management (HIM) Department (Medical Records) for the information. Employees must not use their employee status to obtain medical and/or demographic information for anyone else. **What if I am involved in the treatment, billing or other activity of a person who I know?** In the very rare circumstance when an employee's job (e.g. billing, providing treatment) requires him/her to access and/or copy the medical information of a family member, a co-worker, or other personally known individual, then he/she should immediately report the situation to his/her supervisor who will determine whether to assign a different employee to complete the task involving the specific patient. Additional guidelines are available in the Guidance section on the HIPAA Webpage: http://hipaa.bsd.uchicago.edu/access_phi.html.
Looking up your own information	**As an employee may I access my own PHI (e.g. electronic, written)?** Your access to your own PHI must be based on the same procedures available to other patients not based on your job-related access to our information systems (e.g. OACIS, EPIC, Lastword). For example, if you are waiting for a lab result or want to view a clinic note or operative report, you must either contact your physician for the information or make a written request to the Health Information Management (HIM) Department. More specific guidelines are available in the Guidance section on the HIPAA Webpage: http://hipaa.bsd.uchicago.edu/access_phi.html.

Patient wants all or part of the medical record	**What do I do when a patient requests a copy of his/her medical record?** A patient can request a copy of his/her medical record by completing a *Request and Authorization to Copy Health Information* form and submitting it to the UC organization that maintains the information being requested. Employees can access the form online at http://www.uchospitals.edu/pdf/uch_003278.pdf. To get a form in person, patients can be directed to the hospital website at http://www.uchospitals.edu/medicalrecords/ or they can stop by or call Health Information Management (HIM) [Medical Records] or the HIPAA Program Office to request a copy at: Health Information Management (WB20) 5841 S. Maryland Avenue Chicago, IL 60637 (773) 834-0444 HIPAA Program Office (L147) 5841 S. Maryland Avenue Chicago, IL 60637 (773) 834-9716 **What do I do when patients are checking out after a clinic visit, and request a copy of their clinic notes or labs?** It's okay to provide a patient with a copy of a clinic note or labs that are maintained in your clinic files. It is recommended that you follow the Best Practice of stamping or writing "Patient Copy" on each page. **What if patients need help completing the form or have questions about where to send it?** You can either provide them with a copy of the detailed guidelines on completing and submitting the form (which includes the cost) or direct patients to the hospital website at http://www.uchospitals.edu/medicalrecords/ . If the patient is on the premises he/she can be directed to HIM to ask questions and/or submit the form.
Changing a medical record	**Sometimes patients want things changed or removed from their medical record. Can we do that?** Under HIPAA, patients have the right to request that their medical record information be amended. However, information can't be removed once it is written in the medical record. Statements can be added by following the amendment process, but not removed. Individuals may request an amendment by completing a form and submitting it to the HIPAA Program Office. Patients must include a reason to support the amendment request. Upon review of the request with all appropriate clinical and administrative personnel, the patient will be notified if the request has been accepted or denied. More details are available in the Amendment of Health Information Policy located on the HIPAA website at http://hipaa.bsd.uchicago.edu/policies.html click on A05-32/PC 78 Amendment of Protected Health Information
Patient Authorization	**When do I need a patient's authorization?** In general, anytime you release patient information for a reason unrelated to treatment, payment (e.g. billing), or healthcare operations, an authorization is required. For example: ▪ If a patient's Life Insurance Company requests a copy of information from the patient's medical record in order to process an application for life insurance, you would need a signed authorization from the patient before you could release that information. ▪ If a patient's employer contacted you and requested a confirmation that the patient was seen in the clinic on a certain date, you must have the patient's signed authorization before sharing that information. **There is an inventory of Authorization Forms for a number of specific purposes as well as a brief description of each on the HIPAA website at http://hipaa.bsd.uchicago.edu/authInventory.pdf.** IMPORTANT NOTE: There are times when we may disclose information without an authorization. These disclosures must be accounted for so that we are able to report on those to the patient if requested. These situations are outlined in detail in the section on Accounting for Disclosures.

Trusted Requestor Process	**How do I request PHI from departments in the Medical Center, including Information Services, Patient Accounts, Medical Records, Radiology, Pathology, or TSI?** Individuals wishing to request PHI for uses other than treatment and payment must complete a trusted requestor form and submit it to the HIPAA Program Office for approval. If the data request is for research purposes then a copy of the University of Chicago Institutional Review Board (IRB) research protocol approval letter and submission forms must be included. More information about the trusted requestor process and a copy of the form are available in the Forms section on the HIPAA Webpage: http://hipaa.bsd.uchicago.edu/forms/TrustedRequestorProcessInstructions.doc http://hipaa.bsd.uchicago.edu/forms/TrustedRequestForm.doc

White Boards	**What information can I put on a white board?**
	It is ok to put the room number and either the patient name or the physician name.
	
	Specifically,
	▪ If putting patient name – may not put physician name
	▪ If putting physician name – may not put patient name
	▪ Always ok to put room number
	▪ Never put:
	  ▪ Patient diagnosis
	  ▪ Medications
	  ▪ Status (e.g. ICU, step-down)
	  ▪ Complaint
	  ▪ Activity (dialysis, PT)
	  ▪ Transfer Location (e.g. unit/floor)
	  ▪ Mental health information
	  ▪ Alcohol and drug abuse information
	  ▪ HIV/AIDS information
	  ▪ Venereal disease information
	  ▪ Genetic testing information
	  ▪ Child abuse and neglect information
	  ▪ Domestic abuse information
	  ▪ Sexual assault information
	
	More details are available in the HIPAA White Board Guidance on the HIPAA Webpage:
	http://hipaa.bsd.uchicago.edu/white_boards.html

Posting Allergy Information	**Can we post allergy information on the patient's hospital room door?** Yes and No. In general, good patient privacy practices require us to eliminate posting patient care information outside of the patient's room. However, sometimes patient safety issues must supercede the need to maintain privacy. Since the hallway is a semi-public area, only information that has serious patient safety benefits should be posted. So . . . It IS OK to post environmental allergy information for items such as latex, cleaning chemicals, or even food exposure that could cause a reaction because the item in the presence of the patient alone can cause a risk for the patient. Thus, in this situation, patient safety principles outweigh our need to protect patient privacy. However, the posting should be generic (e.g. a picture or colored tab that is identifiable by only UCMC healthcare providers). It IS NOT OK to post any other allergy information outside the door. Respect for patient privacy supercedes our convenience. For example, rarely would it be necessary to post information next to the door regarding a patient's allergies to medication.

Vendors	**Can a pharmaceutical or medical device vendor representative observe patient care or have access to PHI?** No. It is not appropriate for a supply or equipment vendor representative (such as a pharmaceutical or medical device vendor) to be present during a patient's appointment, treatment or surgery. Additionally, a vendor may not have access to patient charts or lists of patient names. There are limited exceptions when a vendor representative's presence may be necessary and therefore allowed: ☑ To educate or guide faculty or other staff in the use or insertion of a device, piece of equipment, or a drug, or ☑ To service a device or piece of equipment for which the vendor is responsible. The guidelines for these exceptions are available in the Guidance section on the HIPAA Website at http://hipaa.bsd.uchicago.edu/advisory2.html and http://hipaa.bsd.uchicago.edu/advisory3.html. If you suspect a vendor's presence is not authorized or his/her behavior is inappropriate, you should ask the vendor representative to leave or contact security at 2-6262 to have the vendor removed from the premises.
House Phones	**What precautions should I take when I am discussing a patient on a house phone?** Reasonable safeguards to protect patient privacy and to minimize the likelihood of incidental use or disclosure of PHI should be used. For example: ▪ Do not discuss PHI on a house phone if you are likely to be overheard. ▪ Lower your voice when having conversation concerning patients. ▪ Do not say the patient's name. ▪ Keep PHI use or disclosure to a minimum. **Go to a more private area when discussing highly confidential PHI (see section on highly confidential information for categories.)**

Students **Shadowing and Tours**	**We have been contacted by a high school/college student that wants to observe a physician to better understand what it's like to be a doctor. Can we host them?** Yes, under certain conditions. The HIPAA Program Office reviews and approves these kinds of requests with respect to compliance with patient privacy and confidentiality policies. The requests may be made verbally to the HIPAA Program Office, but needs to meet the following guidelines: ▪ Pre-professionals must be enrolled in an educational institution that has a formal observation/shadowing program; ▪ The pre-professional must have a Medical Center sponsoring provider; ▪ The sponsor must submit to the HIPAA Program Office materials about the originating institution's program. If the request is approved, then the pre-professional (observer) and the sponsor must complete the steps listed in the "Pre-professionals Observation and Patient Confidentiality" guidance. The guidelines are available in the Guidance section on the HIPAA Webpage: http://hipaa.bsd.uchicago.edu/prepro_obs.html **My neighbor's son is a high school student and he is interested in a career in healthcare. Can I arrange to have him come to the office with me so I can take him on a tour of our facilities?** Generally speaking, such activities are limited to high school students enrolled in a school that is a participant in the University of Chicago's The Best of The Best program which was created to educate, encourage, and empower students by introducing them to various career opportunities in healthcare. Students wanting more information about The Best of the Best program can visit the hospital website at http://www.uchospitals.edu/programs/community/programs/best.html or they can have their school representative contact: University of Chicago Office of Community Affairs Phone: (773) 702-5600 Fax: (773) 702-3193 If the student's school does not qualify to participate in The Best of the Best program, the student: ▪ Must be in an educational institution that has a formal observation/shadowing program; ▪ Must have a Medical Center sponsoring provider; ▪ The sponsor must submit to the HIPAA Program Office materials about the originating institution's program. If the request is approved, then the student and the sponsor must complete the steps listed in the "Pre-professionals Observation and Patient Confidentiality" guidance. The guidelines are available in the Guidance section on the HIPAA Webpage: http://hipaa.bsd.uchicago.edu/prepro_obs.html

Notice of Privacy Practices – Acknowledgment Form

What is the Notice of Privacy Practices (Notice)?

This Notice is required by law to inform patients how their health information will be protected, how the University of Chicago OHCA may use or disclose their health information, and about the patients' rights regarding their health information.

Why are patients required to sign an Acknowledgment Form?

Patients are asked to sign an acknowledgment of receipt of the Notice of Privacy Practices because we are required to demonstrate that we have given our Notice of Privacy Practices to each patient at the first point of service. We ask patients to sign the form that simply says they received the Notice.

How do I know when to issue a Notice of Privacy Practices booklet to a patient?

We are required to give our Notice of Privacy Practices to each patient at the first point of service. Before issuing a Notice (booklet), you should check the EPIC and/or Lastword systems to see if it has already been issued. If the system indicates a Notice has not been given, the Notice and acknowledgment form should be issued to the patient. If the system indicates a Notice has been issued, do not provide it again. At a patient's first point of service, a Notice of Privacy Practices booklet should be issued and a signed acknowledgment form obtained. We are only required to issue the Notice once provided there have been no significant changes made to the content of the Notice.

Where can I get a copy of the Notice of Privacy Practices?

You can access our Notice of Privacy Practices as well as the Acknowledgment form on the HIPAA website at http://hipaa.bsd.uchicago.edu/forms.html and click on the Acknowledgement or the Notice of Privacy Practices that you would like.

Is the Notice of Privacy Practices available in languages other than English?

Yes, it is available in Spanish and Arabic on the HIPAA website at http://hipaa.bsd.uchicago.edu/forms.html and click on the Acknowledgement or the Notice of Privacy Practices that you would like.

Where can I get more 'Notice of Privacy Practices' booklets and Acknowledgment Forms?

To re-order booklets and forms:

- UCMC Intranet site
- Employee Tools Tab
- Under Purchasing heading, click on North American Corporation.
- All Clinic Managers should already have a user ID and password to enter
- NPP is called HIPAA Booklet - it is packaged in single quantities, not bundled.
- Acknowledgment is form #10.26 and is packaged in bundles of 100

Where should I send the signed Acknowledgment Forms?

Once the patient has signed the Acknowledgment Form, your department should have a process in place in which these forms are collected and forwarded to the HIPAA Program Office located in L-147. Please ask your manager for specific instructions on your location's process.

Disclosure Tracking

My job requires me to notify various agencies, like the Department of Public Health, of information about our patients. Is there anything special that I need to do with respect to HIPAA?

Yes, you may be required to notify these agencies in accordance with Medical Center policies. While a patient authorization form is not needed, we are required to account for these in order to produce a list (called an accounting of disclosures) for the patient upon request. Patients are informed of this right to an 'accounting of disclosures' in our Notice of Privacy Practices.
The following types of disclosures must be tracked:

- Reports of child abuse, neglect, or domestic violence
- Any disclosure required by law (state encounter data, infectious disease reporting, etc.)
- Disclosures to funeral directors, coroners, and medical examiners
- Disclosures in accordance with a judicial subpoena
- Public health activities (births, deaths, public health investigations, adverse events, work related injuries, FDA required reporting, etc.)
- Health oversight activities (audits and investigations by Government benefit or regulatory programs)
- Specialized government functions (law enforcement custodial situations) Disclosure for certain law enforcement purposes (identification of a suspect or missing person, identification of a crime victim, suspected crime, etc.)
- Disclosures to organ procurement and banking organizations
- Disclosures to a third party when the safety of an individual is at risk (threat of violent
- Disclosure for research with a waiver of informed consent from the IRB
- Workers' compensation disclosures
- Disclosures made in error (e.g. faxed to a wrong number or message left on the wrong answering machine).

For more detail on these disclosures and a list of the types of disclosures we must account for, please see the Purpose of Disclosure Definition Table found on the UCMC intranet. Under Employee Tools, click on Disclosure Tracking (under Compliance), and click on the Purpose of Disclosure Definition Table (PDF) - http://home.uchospitals.edu/pdf/uch_003046.pdf.

,

How do I keep track of these disclosures?

To facilitate the accounting of disclosures, we have a centralized electronic system to log the disclosures. Any disclosure meeting the criteria outlined in the Purpose of Disclosure Definition Table should be entered into the system. The information captured in the system is linked to the patient's medical record number (MRN), and will allow us to respond completely and accurately to patient requests for an accounting of disclosures.

How do I get access to the disclosure tracking system?

For access to the Disclosure tracking system, complete and submit a system access request form (SARF). This form can be found on the UCMC intranet. Under Employee Tools, click on Disclosure Tracking (under Compliance), and click on the. Disclosure Tracking System Access Request Form (SARF) - http://home.uchospitals.edu/assets/uch_010829.doc. For training, log in id and password assistance, contact medical records at 4-0444.

Computer Passwords

What can I do to help prevent other people from getting information that they should not?

1. **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.

2. **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?

3. **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.

4. **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.

5. **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!".

For information on choosing a good password and keeping track of the passwords you have, please see http://security.uchicago.edu/docs/userpassword.shtml.

Consequences	**What can happen to me if I violate our HIPAA privacy and security policies?** All workforce members (e.g. staff, physicians, nurses, residents, medical students, volunteers) must comply with all applicable HIPAA patient privacy and information security policies. If after an investigation you are found to have violated the organization's HIPAA privacy and information security policies then you are subject to disciplinary action. Disciplinary action will be consistent with the organization's corrective action policies, and can include but is not limited to: ▪ Verbal counseling ▪ Written reprimand ▪ Required retraining ▪ Suspension ▪ Termination/Discharge The organization's disciplinary/corrective action policies can be found at: http://hr.uchicago.edu/policy/p703.html http://frontline.mcis.uchicago.edu/admin/hsp_pp.nsf/0fae4f0f5b607eb40625687a0057d0db/d5cb0d50711c1cdd86256ac600665e80?OpenDocument

This Guide brought to you by the HIPAA Program Office. The HIPAA Program Office ***provides information and tools to support employees, faculty, and students in their efforts to ensure the privacy and security of our patients' health information. The HIPAA Program Office utilizes a variety of methods and initiatives to keep the workforce informed about privacy and security obligations and best practices.***