



Student HIPAA Privacy Training and Summary of Relevant HIPAA Privacy Policies for Academic Year 2009-2010

The Health Insurance Portability and Accountability Act (HIPAA) was originally passed by Congress in 1996. In April of 2003 a key portion of this act, HIPAA Privacy Regulations, came into effect. All health care entities subject to these regulations must abide by these rules. HIPAA's privacy regulations **do not** supersede Connecticut State law where State requirements are more stringent. The Office of Civil Rights has been given the authority to enforce the privacy regulations. Both civil and criminal penalties are associated with violations of these regulations.

One of the administrative requirements of HIPAA Privacy regulations is training on the regulations as well as internal policies and procedures related to patient privacy. As a student at the University of Connecticut Health Center (UCHC), you are required to complete this self-learning packet and review the associated HIPAA privacy policies.

HIPAA privacy regulations require hospitals/clinics to have in place appropriate processes to safeguard Protected Health Information (PHI). These safeguards include:

- Access level security for information systems.
- Protocols for requesting patient information through the Department of Health Information Management.
- Protocols for confidential waste destruction.
- Speaking quietly while discussing a patient's condition with family members in public areas.
- Avoiding using the patient's name in publicly accessed areas.
- Not leaving protected health information unattended.
- Protecting personally assigned passwords and not sharing with others.
- Not sending protected health information over the Internet unless you confirm that it is encrypted.

In addition, all employees and medical staff members are reminded not to conduct conversations about patients in public areas such as public elevators, corridors, lobbies and the cafeteria. Although the regulations acknowledge that there will occasionally be an incidental disclosure, such occurrences should be unavoidable and limited in nature.

HIPAA also imposes changes to the approval process for research. All research conducted at UCHC must be reviewed and approved/waived by the Institutional Review Board (IRB).

All HIPAA Privacy Policies and Procedures can be located via the UCHC Home Page at www.uchc.edu. Click on "*Faculty and Staff*", look for the section entitled "*Reference*", click on "*UConn Health Center Policies*", and click on "*HIPAA Privacy Policies*."

Completion of this training material will satisfy your training requirement for:

- University of Connecticut Health Center
- John Dempsey Hospital
- University Medical Group
- University of Connecticut Health Partners



Student HIPAA Privacy Training and Summary of Relevant HIPAA Privacy Policies for Academic Year 2009-2010

Protected Health Information (PHI)

PHI is defined as any individually identifiable health information that is maintained or transmitted in any form. There are many “identifiers” that can link an individual to health information (i.e. name, address, SS#, insurance plan numbers, email address etc.). *All health information that can be linked to an individual must be protected.*

Refer to UCHC policy # 2003-03 “*Privacy Definitions*” for more detailed explanations of PHI and other HIPAA related terms.

Notice of Privacy Practices

Under the HIPAA regulations patients are entitled to receive a “Notice of Privacy Practices” which informs patients about how their PHI is used and disclosed as well as their rights and how to exercise those rights. This notice is completed and acknowledged by the patient at the time of first service delivery as part of the “Permission to Treat” form (HCH 901). Returning outpatients will be asked to sign the form every six months thereafter and inpatients will be asked to sign the form at the time of each admission.

The UCHC “*Notice of Privacy Practices*” may be found at <http://health.uchc.edu/privacy/index.htm>.

Refer to UCHC policy # 2003-13 “*Permission to Treat/Assignment of Benefits/Authorization to Release Medical/Dental Records/Acknowledgement of Receipt of Notice of Privacy Practices*” and the associated form for more information.

Sharing PHI without Authorization

Healthcare providers may share PHI *without* patient authorization for:

- Treatment within and between UCHC providers (i.e. JDH, UMG, UCHP).
- Payment for treatment.
- Health care operations (i.e. quality improvement, training, compliance reviews, evaluating caregiver performance).

There are other specific circumstances where authorization is not required before disclosing PHI.

Refer to UCHC policy #2003-27 “*Use and Disclosure of PHI Where Authorization or Opportunity for Patient to Agree or Object is **NOT** Required*” and “*Certification Regarding Subpoena*” for more information.

When is authorization required for disclosure of PHI?

In general, if access, use, or disclosure of PHI does not fall within the treatment, payment, or operations categories outlined above you must have the patient’s signed authorization. A valid authorization includes specific requirements. Always use UCHC HIPAA compliant authorization forms. A patient may withdraw authorization at any time except to the extent that UCHC has already used or released information while the authorization was still valid. Written revocation must be made to the Director of Medical Records.



Refer to UCHC policy # 2003-16 “*Authorization for Release of Information*” and associated authorization form for more information.

Disclosure of PHI to Friends and Family Members Involved in a Patient’s Care

When the patient is present and has the capacity to make health care decisions, UCHC will provide the patient an opportunity to agree or object to the disclosure of protected health information to friends or family members involved in his/her care before the disclosure occurs.

When the patient is not present, or the opportunity to agree or object to the disclosure cannot practicably be provided because of the patient’s incapacity or an emergency circumstance, UCHC may determine whether the disclosure is in the best interests of the patient.

Refer to UCHC policy #2003-25 “*Use and Disclosure Involving Family and Friends*” for more detailed information.

Disclosure of Patient Information to the Public and Community Clergy Members

Unless a patient objects, UCHC may disclose that patient’s location (room number and telephone number) to persons who inquire about that patient **by name**. Members of the clergy will also be provided a patient’s religious affiliation unless the patient objects.

Inquiries made by the media/press must be directed to the UCHC Office of Communications. The telephone operator will assist.

Refer to UCHC policy #2003-26 “*Directory Information: Disclosure of a Patient’s Information*” for more detailed information.

Disclosure of PHI via E-mail

PHI should be hand delivered or mailed whenever possible. However, e-mailing of patient information internally to authorized personnel **within the UCHC system** is allowable to facilitate treatment, payment and health care operations. These e-mails can **only** be sent from and to secure e-mail addresses within the UCHC network. UCHC defines a secure e-mail address as one that ends either with ***uchc.edu*** or ***uchp.org***.

E-mails of PHI cannot be sent unless the recipient address can be verified as being secure.

Refer to UCHC policy #2003-22 “*E-Mail: Use and Disclosure of Protected Health Information*” and “*HIPAA Email Policy Attachment*” for more detailed information.

Disclosure of PHI via Facsimile

Faxing of patient information outside of the facility is allowable in situations when health information is needed **immediately** for patient care purposes, continuing care placement, payment or when mail or courier delivery will not meet a necessary timeframe.



Student HIPAA Privacy Training and Summary of Relevant HIPAA Privacy Policies for Academic Year 2009-2010

Employees authorized to FAX patient health information must confirm the accuracy of the FAX numbers and security of recipient machines by calling the intended recipients to verify the numbers and notify them that the FAX is on the way.

When expecting the arrival of a FAX containing PHI schedule with the sender whenever possible to ensure that the faxed documents can be promptly removed from the FAX machine.

Facsimile machines that receive and/or transmit health information must be located in a secure and controlled area so information being displayed or printed is not accessible to unauthorized users.

Refer to UCHC policy # 2003-23 "*Faxing of Protected Health Information*" and fax cover sheet for more detailed information.

Disclosure of Protected Health Information by Whistleblowers

PHI may be used or disclosed by whistleblowers or workforce member or student crime victims under certain circumstances. If the workforce member believes in good faith that UCHC has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, the workforce member may disclose PHI to the UCHC Corporate Compliance Office and/or a government agency. A member of the UCHC workforce or student who is the victim of a crime may disclose PHI to a law enforcement official, provided that the PHI disclosed is about the suspected perpetrator of the crime and the PHI disclosed is limited to certain data items.

Refer to UCHC policy # 2003-08 "*Use and Disclosure of Protected Health Information by Whistleblowers and Workforce Member Crime Victims*" for more detailed information.

Restrictions on the Use and Disclosure of PHI

Patient care units and departments must review and honor approved patient requests for restrictions before using or disclosing protected health information. All restriction agreements must be documented.

Refer to UCHC policy #2003-14 "*Patient Right to Request Restrictions on Use and Disclosure of Protected Health Information*" for more detailed information.

Patient Request for Confidential Communication

Patient care units and departments must review and, if operationally feasible, honor all patient requests for confidential communications before using or disclosing protected health information.

UCHC will approve requests for one alternative mailing address and/or telephone number at the time of the request.

Refer to UCHC policy #2003-15 "*Patient Right to Request Confidential Communications*" for more detailed information.



Student HIPAA Privacy Training and Summary of Relevant HIPAA Privacy Policies for Academic Year 2009-2010

Minimum Necessary Data

Minimum necessary data means limiting the request for use or disclosure of PHI to the minimum necessary to accomplish the intended purpose. The concept of minimum necessary does not apply to treatment situations with patients and a few other uses and disclosures required by law.

UCHC will make reasonable efforts to limit the request for use or disclosure of PHI to the minimum necessary to fulfill assigned duties. Health care providers are reminded to consider the concept of minimum necessary data in all activities where use, disclosure and requests for PHI are made.

Refer to UCHC policy # 2003-21 "*Minimum Necessary Data*" for more information.

Verification of Requests Related to PHI

UCHC will verify the identity of any person requesting access to or disclosure of protected health information, if the staff member responding to the request does *not* know such person. Once any requester's identity is verified, staff may use whatever means are available to them in their department to determine the person's authority to have the information requested. Staff may only disclose minimum necessary information unless the request is solely for the patient's treatment.

In the event that the identity and/or legal authority of an individual or entity cannot be verified, UCHC staff will *not* make the requested disclosure of PHI, and will report the request for PHI to their immediate supervisor.

Refer to UCHC policy # 2003-20 "*Verification of Individuals or Entities Requesting Disclosure of Protected Health Information*" for more information and specific procedures for verifying requester.

Use of Portable Computing Devices (PCD)

Whenever PHI is kept on a PCD, it must be in encrypted format and have secure password protection approved by UCHC. The information should only be maintained on these devices as long as it is absolutely necessary, then it should be deleted. At the end of your association with the hospital/clinic you *must* delete all patient information from your personal devices.

Refer to UCHC policy # 2003-32 "*Portable Computing Device (PCD) Security Policy*" for specific procedures.

Disposal of Confidential Information

Any printed material (e.g., faxes, printed emails, informal notes about patients) containing PHI must *not* be discarded in trash bins, unsecured recycle bins or other publicly accessible locations. Instead this information must be personally shredded or placed in secured shredder bins. If you have in your possession copies of protected health information in preparation for case presentations or other academic requirements, you are obligated to destroy this material in a confidential manner.



Student HIPAA Privacy Training and Summary of Relevant HIPAA Privacy Policies for Academic Year 2009-2010

Secure methods will be used to dispose of electronic data and output. The Materials Management Department is responsible for the removal of all UCHC information, including PHI, residing on any electronic storage media/device prior to removal or sale of such devices.

See UCHC policy # 2008-01 “*Disposal of Documents/Materials Containing PHI and Receipt, Tracking, and Disposal of Equipment and Electronic Media Containing Electronic Protected Health Information*” for specific procedures.

Patient Requests to Review, Copy, or Amend their PHI

Patients have the right to request to review, copy, or amend the health information contained in their medical/dental records or billing records. All requests must be made in writing and will be reviewed with the patient’s attending of record. UCHC and the physician will determine if the request will be honored and will provide a written response to the patient for any denial of the request. The original medical/dental/billing record is the property of UCHC and may *not* be removed from the facility except by court order.

Refer to UCHC policy #2003-17 “*Patient Right to Inspect, Copy, and Amend their Medical Record*” and associated forms for more information.

Patient Requests for Accounting of PHI Disclosures

With the exception of disclosures for treatment, payment or health care operations patients have the right to request in writing an accounting of all disclosures of their PHI of which they would not otherwise be aware (i.e. regulatory agencies, in response to subpoenas). All such disclosures are recorded on an accounting log. For disclosures that may be made many times for the same purpose to the same person or entity, some of the accounting may be summarized.

Refer to UCHC policy # 2003-18 “*Accounting of Disclosures of Protected Health Information to Patients Upon Their Request*” and associated forms for more detailed information.

Remember:

If you suspect any breaches of privacy or non-compliance with HIPAA Privacy regulations you may report your concerns to:

- your immediate supervisor or major advisor.
- the UCHC Corporate Compliance Integrity and Privacy Officer, Iris Mauriello. Phone number 860-679-3501 E-mail: mauriello@nso1.uchc.edu
- the confidential REPORTLINE for the University of Connecticut Health Center: Phone number 1-888-685-2637.
- the Office of Civil Rights.



Self Quiz

True or False: A Notice of Privacy Practices will be given to patients when they are first seen in a clinic or admitted to the Hospital explaining how the hospital will use and disclose their protected health information.

True or False: A patient authorization is required to release protected health information to an attorney. (Note: assume a subpoena has not been issued for the information.)

True or False: A patient has no choice but to be included in the facility directory.

True or False: A patient may request an amendment to his/her protected health information.

True or False: It's OK to discuss patients in the public elevator with colleagues regardless of who's in the elevator.

True or False: It is fine to conduct research without IRB approval.

True or False: I should report any known breaches of the HIPAA Privacy requirements at UCHC to my immediate supervisor, the UCHC HIPAA Privacy Officer, or UCHC REPORTLINE.

Answers: T, T, F, T, F, F, T