



University of Connecticut
Health Center

Form C
2011-2012

Dear Student,

As many of you know, all health care organizations were required to be compliant with HIPAA Privacy Regulations in 2003 and later HIPAA Security Regulations that became effective in 2005. New legislation referred to as HITECH in 2009 addresses additional requirements. One of the requirements under these laws is mandatory training for all students who, as part of their educational experience, will have access to patient's protected health information. This training includes a review of the organization's policies and procedures relating to protecting patient information.

We have developed the attached training packet for your review and completion. It is a summary of your responsibilities as a student working at The University of Connecticut Health Center (UCHC). Completion of these materials will satisfy your HIPAA training requirements for any UCHC site. At the end of the text is a self-scoring quiz of the materials.

Please sign the last page of the packet indicating that you have completed the training packet and return it to your instructor, host, and preceptor or the individual that is responsible for your student rotation here at UCHC. Continued participation in your Program is contingent upon proof of completion of this material. We are available to you to answer any questions or to address any concerns about the privacy and security of patient information during your work at UCHC.

Thank you in advance for your cooperation,

Iris Mauriello, RN, CHC
Corporate Compliance Integrity Officer and HIPAA Privacy Officer

Jonathan Carroll
AVP, Enterprise IT Operations and Information Security Officer

University of Connecticut Health Center (UCHC) Student HIPAA Privacy/Security Training and Summary of Relevant HIPAA and HITECH Policies Academic Year 2011-2012

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 and in April 2005, the HIPAA Security Regulations became effective. Most recently Congress passed The Economic Stimulus Act officially titled the American Recovery and Reinvestment Act of 2009. This Act includes significant expansion of HIPAA Privacy and Security requirements. Within this massive legislation, a section titled the Health Information Technology for Economic and Clinical Health (HITECH) Act requires changes to HIPAA Privacy and Security. As of the date this training is written, the U.S. is awaiting further detailed guidance on the HITECH Act from several government agencies. Additional guidance is expected by the end of 2011.

All health care entities subject to these regulations must abide by these rules. These regulations **do not** supersede Connecticut State law where State requirements are more stringent. The Office for Civil Rights has been given the authority to enforce these regulations. Both civil and criminal penalties are associated with violations.

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

These 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 and disclosing patient information through the Department of Health Information Management.
- Protocols for disclosing PHI to family members and friends of patients.
- Protocols for confidential waste destruction.
- Speaking quietly while discussing a patient's condition with family members in public areas.
- Avoiding using patient identifiable information in publicly accessed areas.
- Never leaving PHI unattended.
- Protecting personally assigned passwords for access to systems with PHI and never sharing your assigned password with others.
- Never storing or sending PHI over the internet unless it is encrypted.
- Reporting breaches immediately to the proper persons in the institution.

All students, 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. Information learned within the course of your work as a student should not be disclosed outside the institution at any time unless properly authorized.

The regulations also impose 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 and Security Policies and Procedures can be located via the UCHC Policies Home Page at www.policies.uchc.edu. Due to ongoing changes in the Federal HIPAA regulations, please check this website periodically for UCHC policy changes and updates.

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

- University of Connecticut Health Center
- John Dempsey Hospital
- University Medical Group (all locations)

Protected Health Information (PHI) and Electronic Protected Health Information (ePHI)

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.*

ePHI is defined as individually identifiable health information that is transmitted by electronic media or maintained in electronic media. Examples of ePHI include any medium used to store, transmit, or receive PHI electronically.

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

UCHC Training of Workforce: HIPAA Privacy and Security

As mentioned in the introduction to this packet, UCHC workforce must be trained on Federal HIPAA regulations and UCHC organizational policies related to security and privacy of protected health information.

Refer to UCHC policy # 2003-07 “*UCHC Training of Workforce: HIPAA Privacy and Security*”

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 before disclosing any PHI. 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 Health Information Management.

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 PHI 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 interest 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 is allowable to facilitate treatment, payment and health care operations provided the guidelines outlined in **POLICY NUMBER 2003-22 “E-MAIL: USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION”** are adhered to. Information transmitted must be limited to the minimum necessary to meet the requester’s needs.

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

Please note: A new UCHC policy referencing use and disclosure of confidential electronic information is under development. When completed, this policy will govern the use of email encryption when transmitting PHI outside of the UCHC network. Please check the UCHC policy website periodically for updates.

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.

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 will be sent.

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.

Telephone/Voicemail/Answering Machine Disclosure of PHI

Patient PHI shall not be left on voicemail/answering machines. Information left on answering machines/voicemail shall be generic in nature and not indicate services being performed or provider of such services. If the patient is calling to obtain information about him/herself staff shall verify identity of person(s) on the phone using information available in the Registration system: e.g. last four digits of the social security number and date of birth. The verification requirements are met if UCHC relies on the exercise of professional judgment or acts on a good faith belief in making a disclosure.

Refer to UCHC policy # 2003-24 “*Telephone/Voicemail/Answering machine Disclosure of PHI*” 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 PHI. All restriction agreements must be documented. Under the new HITECH Act patients may request to pay for specific services out of pocket and not through their health care insurance. UCHC must accommodate all such requests and not bill the patient’s insurance or release PHI regarding that service to the insurance company. Government guidance on this specific rule is expected by the end of 2011. As a student you should never release any PHI directly to anyone without first checking with a UCHC staff member.

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 PHI. 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.

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 the Identity of Persons Regarding Requests Related to PHI

UCHC will verify the identity of any person requesting access to or disclosure of PHI, 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 Mobile Computing Devices (MCD)

UCHC confidential or restricted data is not authorized to be stored on a UCHC or non-UCHC mobile computing device unless several criteria are met. These criteria are as follows:

- The device is encrypted using methods authorized by the UCHC IT Department
- Data is protected from any and all forms of unauthorized access and disclosure.
- The device stores only the minimum necessary to perform the function necessitating storage on the device

- Information is stored only for the time period needed to perform the function

Electronic resources are computing and telecommunications devices that can execute programs or store data; examples of which may include, but are not limited to: computers, mobile computing devices, smartphones, and storage devices (USB or otherwise connected).

Refer to UCHC policy # 2008-03 “*Mobile Computing Device (MCD) Security*” for more information and 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 PHI in preparation for case presentations or other academic requirements, you are obligated to destroy this material in a confidential manner.

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. Never leave computers/laptops or other devices unattended when planning disposal; always contact Materials Management staff to dispose of 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 View, Copy, or Amend their PHI

Patients have the right to request to view, 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. This policy is currently undergoing revision and will be split into three separate policies addressing each specific type of request. The new policy titles will separately identify viewing, copying and amending and will be noted as policies 2003-17 A, B, and C respectively.

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. This policy is expected to be revised once further guidance is issued on HITECH.

Patient Complaint Regarding Use and Disclosure of PHI

Patients have the right to make a complaint regarding the privacy/security practices of UCHC. The organization has identified the Office of Patient Relations, 860-679-3176, for receiving patient complaints related to the privacy and security of PHI. Often the Patient Relations Department will work with the Privacy and/or Security Officer to resolve complaints. Patients also have the right to make complaints directly to the Office for Civil Rights of the Department of Health and Human Services.

Refer to UCHC policy # 2003-19 “*Patient Complaint Regarding Use and Disclosure of PHI*” for further information.

Data Authentication and Physical Safeguards

UCHC is committed to maintaining formal policies and procedures to protect ePHI from improper alteration or destruction. This includes mechanisms to ensure that electronic protected health information has not been altered or destroyed in an unauthorized manner. To this end, authentication to systems or devices containing ePHI shall minimally include a unique logon or password and be encrypted where feasible. In addition, IT resources (IT Resources are tools that allow access to electronic technological devices, or are the electronic technological devices themselves) – including but not limited to PCs, laptops, cell phones, email, software, applications, etc) shall be secured using physical safeguards for protection from unauthorized access.

Refer to UCHC policy # 2005-01 “*UCHC HIPAA IT Security: Data Authentication, Physical Safeguards*” for further information.

Please note: The new UCHC policy # 2011-01 “*UCHC Information Security: Data Authentication and Physical Safeguards*” will soon replace UCHC policy #2005-01 and will encompass the security of all types of personal information. Please check the UCHC policy website periodically for updates.

Acceptable Use

UCHC workforce members are responsible for the appropriate use and security of ePHI when using any IT resource. This includes the prohibition of introducing any unauthorized IT resources into the environment. Furthermore, the introduction of any IT resource that could disrupt any operations or compromise security is prohibited.

Refer to UCHC policy # 2005-02 “*UCHC HIPAA Security Acceptable Use*” for further information.

Please note: The new UCHC policy # 2011- 02 “*UCHC Information Security: Acceptable Use*” will soon replace UCHC policy # 2005-02 and will encompass the security of all types of personal information. Please check the UCHC policy website periodically for updates.

Facility Access Control

UCHC maintains formal procedures to limit physical access to all forms of protected health information and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. Always keep all file cabinets and rooms that contain PHI locked. As a member of the community, you should always wear your Health Center identification provided to you from the Department of Public Safety.

Refer to UCHC policy # 2005-04 “*UCHC HIPAA Security Facility Access Control*” for further information.

Systems Access Control

The use and access of UCHC’s information systems is restricted to appropriately identified, validated and authorized individuals. Unauthorized access is a violation of UCHC’s policies. You are reminded to not share your account information (username/password) and password creation and password changes will be in accordance with UCHC policy. Please memorize your password and log off your computer, or use a screen saver if your computer is going to be left unattended.

Refer to UCHC policy # 2005-04 “*UCHC HIPAA Security Information Systems Access Control*” for further information.

Please note: The new UCHC policy # 2011-03 “*UCHC Information Security: Systems Access Control*” will soon replace UCHC policy # 2005-04 and will encompass the security of all types of personal information. Please check the UCHC policy website periodically for updates.

Virus Protection

All computer equipment connected to the UCHC network shall have UCHC approved anti-virus protection software installed with current virus definitions. All computer equipment connected to the UCHC network shall be up to date with the manufacturer’s operating system’s security software patches.

Refer to UCHC policy # 2005-10 “*UCHC HIPAA Security Virus Protection Policy*” for further information.

Breaches of Patient Privacy or Security

Anyone who is aware of or suspects a violation of privacy/security policy or a breach of patient information is required to report it immediately to:

- The Privacy Officer, Iris Mauriello at 860-679-3501; E-mail: mauriello@nso1.uchc.edu
- or
- The Information Security Officer (ISO), Jon Carroll at 860-679-3528; E-mail jcarroll@uchc.edu
- or
- The confidential REPORTLINE at 1-888-685-2637

Once the initial report is made, notify your immediate supervisor or major advisor.

Refer to UCHC policy # 2003-09 “*Breaches of Privacy and Security of PHI: Reporting Requirements, Sanctions and Mitigation*” for further information.

Self Quiz

1. 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.
2. 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.)
3. True or False: A patient has no choice but to be included in the facility directory.
4. True or False: A patient may request an amendment to his/her protected health information.
5. True or False: It’s OK to discuss patients in the public elevator with colleagues regardless of who’s in the elevator.
6. True or False: It is fine to conduct research without IRB approval.
7. True or False: I should report any known breaches of the HIPAA requirements at UCHC to the HIPAA Privacy Officer, or the HIPAA Security Officer or UCHC REPORTLINE.
8. True or False: You will be writing a report at home over the weekend and need to access notes on a patient that includes protected patient information. It is OK to copy these notes to your unencrypted laptop or unencrypted USB memory stick.

9. True or False: You walk into a conference room and find a stack of computer printouts from a meeting dated seven days ago. It looks like the printouts contain patient lab results. You should simply throw the papers away and not notify your supervisor or UCHC Privacy officer.
10. True or False: On your way to the Emergency Department a gentleman not wearing his UCHC identification badge approaches you. He states he is late for a meeting being held in a restricted area of the hospital. You should use your badge to swipe the card reader and let him in.
11. True or False: You are doing your rotation in the hospital and you observe a woman, who is not displaying any form of UCHC identification attempting to gain access to a closet where IT hardware is secured. You should call Public Safety and report this suspicious behavior.
12. True or False: You see what appears to be a fellow student struggling to sign into one of the clinical systems in use at the Health Center. Feeling sorry for them, you decide to share your user name and password with them because you know yours works. This is OK for you to do.
13. True or False: A friend calls you to let you know that a mutual friend has apparently been admitted to the hospital. Your friend asks you to access this person's clinical data and find out why your mutual friend was admitted. Even though you have the ability to access the data, you tell your friend that it is inappropriate for you to view this information, especially since you are not treating this patient. You've done the right thing.
14. True or False: It is permissible for you to email Protected Health Information (PHI) to a mailbox external to UCHC.
15. True or False: You use your laptop computer to connect to the UCHC network. The virus protection software is annoying, so you disable it. This is OK to do.

Answers:

1. True
2. True
3. False
4. True
5. False
6. False
7. True
8. False
9. False
10. False
11. True
12. False
13. True
14. False
15. False



UConn
Health
Center

Please read and then print and sign your name below. Send the signed form to:

[PLEASE ENTER PERSON NAME HERE WHO CAN TRACK RETURNS FOR YOUR DEPT.](#)

Certification of HIPAA Privacy/Security/HITECH
Training Packet Completion
Academic Year 2011-2012

I have read and understand the University of Connecticut Health Center HIPAA Privacy/Security/HITECH training materials. Further, I understand that the location of additional information about UCHC's policies and procedures related to patient privacy have been detailed in the training documents.

Printed Name

Signature

Date