UCONN HEALTH

HIPAA Privacy and Security/HITECH Training
2016-17

Greetings,

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 unpaid paid individuals offering their services to UConn Health who, as part of their 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 an unpaid individual offering your service to UConn Health. Completion of these materials will satisfy your HIPAA training requirements for any UConn Health 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 UConn Health. 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 UConn Health.

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

UCONN HEALTH

Certification of HIPAA Privacy/Security/HITECH Training Packet Completion 2016-2017

I have read and understand the UConn Health 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

UConn Health
Privacy and Security

Student Training
Academic Year 2016-2017

Introduction

Welcome to Privacy and Security training.

All members of the UConn Health workforce and students are obligated to ensure the privacy and security of confidential information with which they may come in contact. This training will assist you to be aware of important privacy and security principles as well as UConn Health policies and procedures.

Refer to the policy links throughout the training for more detailed information.

Continued participation in your educational program is contingent upon proof of completion.

Thank you for your participation.

UConn Health Confidentiality Policy

- UConn Health has a responsibility to protect all types of confidential information related to:
  - Patients
  - Research participants
  - Students
  - Employees
  - Social Security numbers, credit card numbers, and other financial data
  - Systems IDs and passwords
  - Institutional data and processes

Unless you have a "need to know" specific confidential information to carry out your UConn Health responsibilities, do not access it, look at it, use it or share it.

Please ***review*** the *Confidentiality* policy.

HIPAA Privacy and Security

I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know.

Excerpt from the Hippocratic Oath

HIPAA at a glance…

- *HIPAA stands for: Health Insurance Portability and Accountability Act*
- The *Privacy* Rule:
  - established national standards for the protection of *all forms of health information* created by "covered entities", including health care providers.
  - set limits on the uses and disclosures of such information.
  - gave patients rights over their health records.
- The *Security* Rule:
  - established national standards for the security of *electronic health information* (ePHI) to protect individual ePHI created, received, used or maintained by covered entities.
  - outlined administrative, technical and physical procedures to ensure the confidentiality, integrity and availability of ePHI.

And then came HITECH…

- *HITECH stands for:*
- *Health Information Technology for Economic and Clinical Health Act*
  - HITECH resulted in significant changes to HIPAA Privacy and Security.
  - Widened the scope of privacy and security protections under HIPAA.
  - Includes health care information technology incentives such as:
    - creating a national health care infrastructure.
    - adopting an electronic health record (EHR) system.
- Electronic data transmission is a double edged sword. Advances in technology lead to increased vulnerability of personal information.
- *Confidential information is only as safe as our weakest link.*

"Protected Health Information"(PHI)

PHI is defined as any type of health information that is maintained or transmitted in any media (verbal, paper, photographed, electronic, others) and can be linked to a specific individual by a *unique* "identifier" such as:

- Name
- Address
- Zip Code
- Telephone or fax numbers
- Dates such as date of birth/death and dates of service
- Email or internet addresses
- Numbers including social security, medical record, patient account, insurance plan, license or medical equipment
- Vehicle information
- Photos and fingerprints

Electronic PHI (ePHI) is patient information stored on computers, storage devices, or in any UConn Health electronic system.

When is information not identifiable (de-identified)?

- Information is considered de-identified when ***all*** identifiers are removed such that the information cannot be linked to any individual or be re-identified.
- De-identified information is ***not*** considered PHI and, therefore, is not protected under the HIPAA Privacy rule.

Refer to policy: *Creation, Use and Disclosure of De-identified PHI*

Genetic Information and HIPAA

- Genetic information, including family history, is considered PHI.
- Includes:
  - genetic tests, requests for genetic services, or participation in clinical research that includes genetic services by an individual or his/her family member.
  - any manifestation of a disease in the individual's family member.
- Genetic information may not be used for underwriting purposes.

Let's remember what HIPAA is really all about: *Patients' Rights*

With respect to their PHI, patients under our care are entitled to:

- information about their rights under HIPAA and how their PHI will be used or disclosed.
- protection of the privacy and security of their health information.
- access to their health information.
- request corrections of information in their records.
- restrict certain disclosures of their information.
- notification if the privacy or security of their information is compromised.

HIPAA privacy begins with the consent to treatment…

- The *Notice of Privacy Practices* (NOPP) explaining patients' rights under HIPAA is provided to all patients *except* Correctional Managed Health Care (CMHC) inmate/patients as part of the treatment consent process.
- A patient's signature on the *consent form* also acknowledges receipt of the NOPP.
- As part of consent, a patient may give "permission to communicate" health information with others and request to restrict disclosure of PHI to health insurers or to be excluded from appointment reminders.
- If another individual signs the consent on behalf of the patient, that person's identity and his or her relationship to the patient (i.e. parent, guardian, authorized representative) must be verified.

Refer to policy: *Consent to Treatment*

Patient Requests to View Records

- Original medical records are the property of UConn Health and ***may not*** be removed from the facility under any circumstances except by court order.
- Patients or their authorized representatives have the right to view their own records upon written request using approved forms.
  - Requests to view are first reviewed with the patient's attending physician or appropriate UConn Health representative.
  - A written response is provided to the patient for any request denial.

Refer to policy:
Patient Right to View His/Her Medical/Dental/Research and/or Billing Record

Patient Requests for Record Copies

- Most requests for patient records should be referred to the Health Information Management (HIM) Release of Information department.
- If information is needed immediately and the treating provider approves, clinical areas may provide ***to the patient*** copies of documents such as labs, diagnostic results and clinical notes related only to the care in that department.
- Information that ***may not*** be released:
  - Psychotherapy notes (separate from the clinical record).
  - Patient information from research labs that are exempt from Clinical Laboratory Improvement Amendment (CLIA) requirements.
  - Information for use in pending litigation.

Refer to policy:
Patient Right to Request Copies of His/Her Medical/Dental/Research and/or Billing Record

Do patients have the right to request changes to information in their records?

Yes, amendments may be requested at any time during or after treatment.

- Whether granted or denied, all amendment requests must be acted upon promptly but no later than **60 days** after the request is made.

Refer to policy:
Patient Right to Amend His/Her Medical/Dental/Research and/or Billing Record

Confidential Communications and Restriction of Certain Disclosures

- UConn Health *must* honor all patient requests:
  - to receive communications of PHI from UConn Health by alternative means or at alternative locations.
  - to restrict certain disclosures of PHI to *health plans* if specific criteria are met.
- Patients may also choose to be excluded from automated, verbal or written appointment reminders.

Refer to policies:
Patient Right to Request Confidential Communications ***and***
Patient Right to Request Restrictions on Use And Disclosure of Protected Health Information

Patients are entitled to a list of certain disclosures of their PHI

- "Disclosure Tracking Logs" must be completed when PHI is released *outside of UConn Health* for reasons unrelated to treatment, payment or operations and of which the patient is unaware (e.g. to regulatory agencies, for judicial proceedings, to medical examiners, for research purposes or to report abuse, neglect and domestic violence).
- *Unauthorized disclosures that result in a privacy incident must also be documented on the tracking log.*

Refer to policy:
Accounting of Disclosures of Protected Health Information to Patients

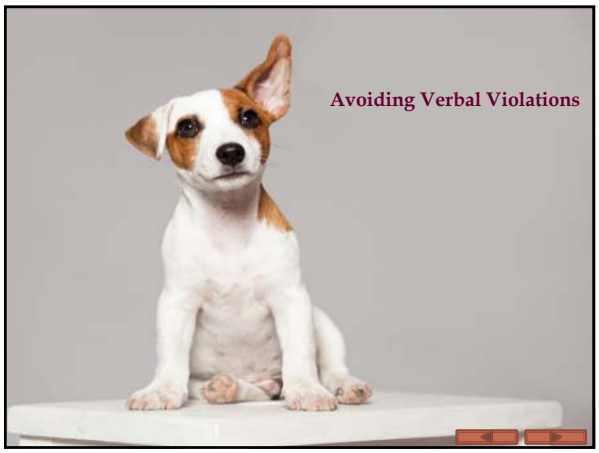
When it come to PHI, always consider the need for patient permission…

- Patient authorization to access, use or share their PHI is needed ***unless:***
  - the purpose is related to treatment, payment for treatment, or "healthcare operations" such as quality improvement, training, performance evaluations, audits ***or***
  - as required by law
- A valid authorization must include specific information to ensure the patient or representative understands what PHI is involved, who is requesting PHI, the purpose of the requested use or disclosure, and the right to revoke an authorization.
- *Regardless of the need for patient authorization, PHI accessed, used or shared for any purpose other than treatment, should be limited to the "minimum necessary" information required to accomplish the task at hand.*

Refer to policy: *Authorization for Release of Information*

Other confidentiality laws

- In addition to HIPAA, there are specific federal and state laws that govern the confidentiality of mental health, substance abuse, and HIV information as well as information related to minors.
- The stricter law *always* applies.
- Remember to consider additional regulations that may apply to a particular scenario and seek guidance as needed.



Be discreet….

- Discuss PHI only with those that "need to know" for their assigned job or student functions.
- Don't talk about identifiable patient information in any area where you might be overheard, *even if you think no one is nearby.*
- Never assume it is OK to share a patient's information with or in front of family, friends or others in the area. Ask for patient permission or check the "Permission to Communicate" form as appropriate.
- If obtaining patient permission is impossible, only that information believed to be in the patient's best interest should be discussed.
- Under certain circumstances, care providers may disclose PHI to a family member or person involved in the care of a deceased patient.
  - HIPAA will no longer apply to those deceased more than 50 years.

Refer to policy: *Use and Disclosure Involving Family and Friends*

Remember privacy over the phone…

- Confirm that you are speaking with the patient or someone that has permission to communicate about the patient.
- For appointment reminders, include only date, time and location on answering machines *--no PHI or other details.*
- For phone messages to patients, only provide your name, that you are calling from UConn Health, who the message is intended for, and ask that the individual return your call.

Refer to policy: *Telephone/Voicemail/Answering Machine Disclosure of PHI*

When someone calls asking for a patient…

- Unless a patient has specifically "opted out", individuals may disclose:
  - a patient's location (hospital room and telephone number) to persons that inquire about that patient ***by name*** (*except* for patients on the Psychiatric and Department of Correction units).
  - a patient's religious affiliation to members of the clergy.
- All inquiries about John Dempsey Hospital patients *must* be forwarded to the UConn Health Information Desk or telephone operators.
- All media requests for patient information must be forwarded to the Office of Communications.

Refer to policies:
Directory Information: Disclosure of a Patient's Information

Media Relations

Verify Requests for PHI

- Before sharing any PHI, verify:
  - the identity of the individual requesting the information.
  - that this individual has the right to obtain the information requested.
- The identity of a patient who calls for information about *himself/herself* must also be verified.
- If an individual's identity and/or legal authority cannot be verified, *do not* disclose any PHI and report the request to your supervisor.

Refer to policy:
Verification of Individuals or Entities Requesting Disclosure of Protected Health Information

Speaking with law enforcement

- Particular caution must be used when PHI is requested for law enforcement reasons.
- *Do not assume that a subpoena or court order requires immediate release of PHI. Check before disclosing.*
- Refer all law enforcement PHI requests (including those by UConn Health Police Department) to your supervisor.

Preventing Paper Problems

General Reminders

- Keep documents with any confidential information in locked areas or cabinets.
- Do not leave papers lying around or unattended in offices or any desks/counters, printers, or fax machines.
- If you must carry documents that may include PHI, keep track of all pages and *shred* them as soon as they are no longer needed.
- Avoid taking notes or documents with confidential information into bathrooms, cafeterias, lounges or other public places but, if you do, *make sure you have everything before you exit.*
- *Do not remove documents with PHI from the facility or personally transport PHI from one UConn Health location to another.*
- Dispose of PHI in locked, secure shredder bins and *not* in wastebaskets or recycling receptacles.

Handling Paper with PHI

- It only takes a few extra seconds to ensure the right documents are provided to the right patient.
- Rushing or skipping important steps takes much more time and creates many more headaches in the end.
- Do your part to prevent paper errors that can lead to patient harm and UConn Health embarrassment.

Refer to policy: *Handling Paper Communications About Patients Including PHI*

Checklist for mailing PHI

- I have made sure that this mailing is for the correct patient.
- I have confirmed the patient's/recipient's mailing address and that the recipient is authorized to receive this document.
- *I have checked and initialed each page to be sure I am sending the correct papers for this patient and that I haven't included other patients' information.*
- The delivery name and address on the envelope matches that of the correct recipient.
- There is no PHI visible through the address window.
- I have tested the system and run a sample before starting a mass mailing.

Checklist for handing documents with PHI to a patient or other

- I have checked two forms of patient identity to ensure the document is intended for this patient.
- *I have checked and initialed each page to be sure I am handing the correct papers and that I haven't included other patients' information by mistake.*
- If handing a document to someone other than the patient, I have confirmed the individual's identity and association with the patient and that he or she is authorized to receive the paper(s).
- I have checked two forms of identity before actually handing the document to the recipient.

Checklist for faxing

- I have confirmed the recipient's correct fax number.
- I have entered the right fax number or chosen the correct pre-programmed number.
- I am using an approved cover sheet *whether faxing internally or externally.*
- I have dialed "9" before faxing to a number outside of UConn Health.
- I have collected my papers from the machine after faxing.

Refer to policy: *Faxing of Protected Health Information*

- Notify your supervisor of any outdated or incorrect fax numbers that may require revision in electronic systems.
- If you send a fax to the wrong recipient/location or learn that a fax sent from UConn Health was misdirected, notify your supervisor or contact the Privacy Office immediately.
- If you receive a misdirected fax from another entity, notify the sender.

Protecting Patient Photographs and Recordings

- Protecting and securely storing patient "nontextual" data (i.e. photos, recordings, physiologic tracings, images or slides) is also important.
  - Personally owned devices may be used for this data *only if deemed secure by UConn Health and if IT policies are followed.*
- Patient consent *is required* to obtain data related to:
  - research
  - sexual assault
  - neonatal death
  - newborn pictures
  - marketing or publicity
  - education if data is identifiable or can be recognized by the patient.
- Patient consent is *not required* for clinical purposes or for photos documenting abuse, neglect, or domestic violence.

Refer to policy:
Visual, Audio, or Other Recording of Patient Data Obtained Through Any Other Medium

Using and Sharing PHI in Research

- PHI in any form may be used or disclosed for purposes of research provided there is a valid participant authorization.
- An authorization is not required only if certain criteria are met and approved by the UConn Health research Institutional Review Board (IRB).
- Research authorizations must be written in plain language and include specific elements.

Refer to policy:
Use and Disclosure of Protected Health Information for Research Purposes

Limited Data Sets

- A Limited Data Set is information from which all *direct* identifiers associated with that PHI is removed.
- Specific steps must be followed when creating, using or disclosing a Limited Data Set for research or other purposes.

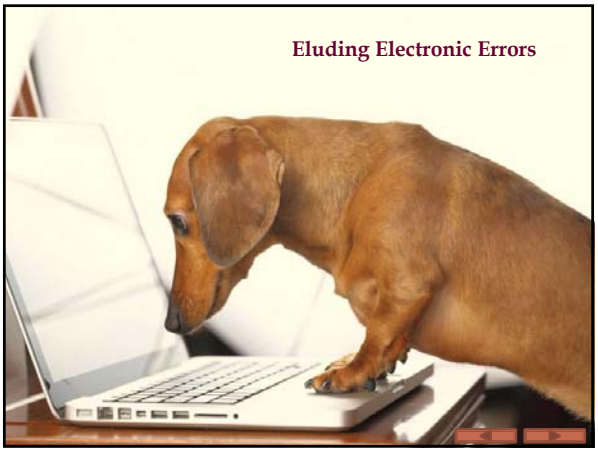
Refer to policy: *Limited Date Set-Creation, Use and Disclosure*

Disposal of Paper Containing Confidential Information

- All documents with PHI or other confidential information must be destroyed in a secure manner.
- Dispose of all copies with confidential information (faxes, printed emails, informal notes or copies of patient notes) either by tearing them up *to render them unreadable* or by placing in *locked* shredder bins.
- Never dispose of confidential documents in a trash or recycle receptacle or in a publicly accessible area.

Refer to UConn Health policy:
Disposal of Documents/Materials Containing PHI and Receipt, Tracking and Disposal of Equipment and Electronic Media Containing Electronic Protected Health Information.

Eluding Electronic Errors



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Bruce Schneier

Using Electronic Systems Responsibly: Important Do's and Don'ts

- Electronic resources are *university/state agency property.*
- *There is no expectation of privacy. All data* stored on UConn Health systems is discoverable under certain circumstances.
- *Never* use UConn Health electronic systems for non-business purposes.
- *Never* collect transmit, or store credit card numbers on UConn Health's computing devices and networks.
- When you leave UConn Health, all information must be properly destroyed or returned to your supervisor.
  - *You may not remove any data from UConn Health without Privacy and Security Office approval.*

Please review policies:
Information Technology Computer/Electronic Resource Use Policy
UCHC Information Security: Acceptable Use
UCHC HIPAA Security Virus Protection Policy

Accessing Electronic Systems

- If you use UConn Health electronic systems, you must have and protect your unique login information.
- *UConn Health Information Technology will never ask for your password in email.*
  - *An email asking you to reply with your user credentials is a hoax and should be deleted without response.*
- *Do not allow anyone to access systems using your username and password.*
- *Always log off when you step away from a computer on which you have been working.*
  - ***You will be held accountable for improper accesses by another individual using or completing work under your login information.***

Refer to UConn Health policy: *UCHC Information Security: Systems Access Control*

Just because you can, doesn't mean you should

- *Unless it is related to your assigned student responsibility do not access, use or disclose PHI related to family, friends, employees, supervisors, other students or any individuals even if they ask you to do so including:*
  - *Do not* view or print clinical data.
  - *Do not* check billing or other financial information.
  - *Do not* "surf" the hospital census to see who has been admitted.
  - *Do not* look at, use or share any confidential information out of curiosity or just because it's there.

Would you want someone to look at your personal information if they have no legitimate reason to do so?

It's really pretty simple to decide what is appropriate…

Before you click on, open, use or disclose any information, especially PHI, ask yourself:
"Do I need this information to complete an assigned task?"
- If the answer is "yes", it is likely OK to access, use or share the information.
- If the answer is "no", *don't do it.*

If using PHI for education within UConn Health, generally no patient authorization is needed ***but*** use only the minimum necessary PHI to meet the goal.

For meetings, lectures, conferences outside of UConn Health:
- information must be de-identified ***or***
- patients must give authorization.

- Always check with your supervisor before accessing, using or sharing any type of confidential information.

Refer to policy: *Use of Protected Health Information in Education*

Mobile Computing Devices (MCDs)

- Confidential data may be stored on UConn or non-UConn Health MCDs only ***if:***
  - the device is encrypted by UConn Health IT.
  - data is protected from unauthorized access and disclosure.
  - the minimum necessary information for a specific function is stored and only for as long as needed to perform that function.
- If certain requirements are met, users may work with IT to access UConn Health's electronic information via their personally owned MCDs.
- Personally-owned MCDs must be registered and secured at the *BYOD website*.
- Upon leaving UConn Health, institutional data, UConn Health email and WiFi settings must be completely deleted from the MCD.

Refer to policy: *Mobile Computing Device (MCD) Security*

Emailing Confidential Information or PHI

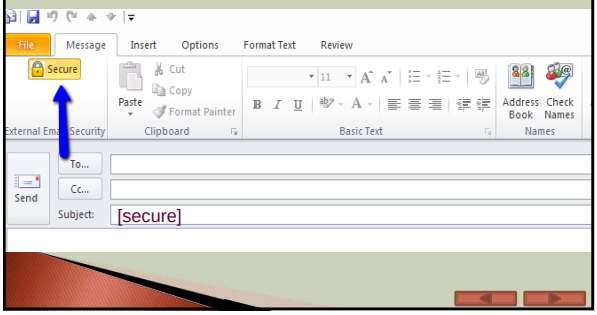
- Treat any email containing PHI with the same degree of privacy as a patient's medical record.
- Communicate only with individuals that have a need to know and are properly authorized to receive the information.
- *Double check* all email recipients to be sure you are including the correct individual(s).
- *Use extra care when choosing names from the address book, persons with similar names or when recipient names auto-populate in the "To" or "cc" lines.*
- Emails containing any confidential information or PHI that are sent outside of the UConn Health network *must be sent securely.*

To send a secure email:

Click the secure icon in the upper left hand corner of the email message screen

or

Type [secure] (brackets and the word) in the email subject line or body.



Texting and Social Media

- *Do not* text confidential information unless a UConn Health approved secure text application has been *installed and activated.*
- Immediately report to the IT Security Office any text that is sent without appropriate software.
- Information related to your UConn Health work should *never ever* be shared on social media sites.

Electronic Information Disposal

- Contact the *Office of Logistics Management* (OLM) to scrub all UConn Health information from electronic devices, especially PHI, before removing any electronic storage media/devices.
- *Store computers/laptops or other devices in a locked, secure area when planning disposal. Do not leave them in hallways or other unlocked areas.*

Refer to policy:

Disposal of Documents/Materials Containing PHI and Receipt, Tracking and Disposal of Equipment and Electronic Media Containing Electronic Protected Health Information.

Working with Outside Entities: Business Associates, Marketing and Fundraising

- Business Associates (BAs) are entities that may create, receive, maintain, or transmit PHI on behalf of UConn Health.
  - Business Associate Agreements (BAAs) outline the respective responsibilities of UConn Health and the BA.
- UConn Health fundraising is coordinated through the UConn Foundation.
  - Only certain patient information may be shared with the Foundation.
  - Patients may ***opt out*** of fundraising communications and treatment cannot be conditioned on an individual's choice to opt out.
- Marketing is communication that encourages individuals to use a particular product or service.
  - Specific HIPAA Privacy rules apply.
- Contact the Privacy Office for guidance.

Refer to policies:

Business Associate Contracts
HIPAA Fundraising Compliance
HIPAA Marketing Compliance

How does UConn Health monitor HIPAA compliance?

- Accesses to electronic patient information systems are monitored and reviewed regularly.
- *You may be notified and asked to justify your electronic accesses as part of a routine monitor.*
- Privacy and Security "walk rounds" are also conducted to educate, assist with questions and ensure that employees and students have the information and tools needed to protect patient privacy.

Do your part….

- Always wear your ID badge.
- Protect PHI in areas accessible to visitors and others not authorized to view PHI.
- Remind others when they may be overheard discussing PHI.
- Lock doors and file cabinets when offices or other areas are unoccupied.
- Look around you for documents or computers with PHI that may be accessible.
- Report any Privacy or Security concerns to your supervisor and/or the Privacy or Security Office immediately.

Managing Privacy and Security Incidents

When an incident occurs…

- Privacy and security incidents can take many forms such as misdirected faxes or emails, documents given or mailed to the incorrect recipient, lost or improper disposal of papers or electronic devices, inappropriate electronic accesses.
- Report any incident or potential privacy/security concern immediately to your supervisor and to the Privacy or Security office.
  - Report research incidents report to the Institutional Review Board (IRB).
- A "breach" is an impermissible use or disclosure of PHI that compromises the security or privacy of that information.
- Several factors are evaluated to determine the risk of compromise to PHI:
  - The *types of PHI* involved.
  - The *unauthorized person(s)* who accessed or used the PHI or to whom the PHI was disclosed.
  - Whether the PHI was *acquired/viewed.*
  - *Mitigation efforts* to reduce the risk.
  - *Other pertinent factors.*

Managing *Paper* Privacy Incidents

- *Notify and seek guidance from the Privacy Office.*
- Identify the documents released in error and who received them.
- Determine how many and which patients were involved----*Was patient information inadvertently switched resulting in more than one error?*
- Resend documents to the correct recipients.
- *Follow the disclosure trail* to identify all individuals that may have seen or had access to the PHI. *Consider possible further disclosures by the original recipient.*
- Determine whether recipient(s) personally know or recognize the patient's name — *Is it a relative, friend, someone that lives in the same community, well-known person or someone "in the news"?*

Managing *Paper* Privacy Incidents (cont.)

- Determine what, if any, PHI the recipient has viewed and request that he or she not view any additional information.
- Confirm that the recipient has not or will not copy, retain or further disclose the PHI.
- Arrange for the *original documents* to be returned to UConn Health--*Offer to send a self-addressed stamped envelope as needed.*
- If the recipient has already discarded the papers, confirm the documents have been *shredded.*
- Once the documents are returned or recreated, if needed, check the patient identifiers and types/sensitivity of PHI disclosed.
- Forward returned documents to the Privacy Office.

Managing *Verbal* Privacy Incidents

- *Notify and seek guidance from the Privacy Office.*
- Identify who heard or may have heard the disclosure—*Was a conversation overheard, did a discussion occur in front of others or over the phone without patient permission, was PHI left on an answering machine?*
- Determine patient identifiers and types of PHI involved.
- Determine whether the individual hearing the PHI knows or recognizes the name of the patient.
- Confirm that the recipient has not or will not further disclose the PHI.
- If PHI is disclosed on an answering machine, verify that the message has been or will be deleted.

Managing *Email* Privacy Incidents

- *Notify and seek guidance from the Privacy Office.*
- Identify who received the email in error—*Was it within the UConn Health network or outside of UConn Health?*
- Check the patient identifiers and the types of PHI disclosed in the subject line, body of the email or in attachments.
- Contact the recipient(s) via phone or *separate email* to:
  - alert them to the erroneous email and to prevent opening, if possible.
  - confirm they have or will delete the email *and* empty their "Deleted Items" folder, whether or not the email and attachment have been opened.
  - clarify whether they know the patient or recognize the patient's name.
  - confirm that they have not and will not print, retain or further disclose the PHI.

Patient Complaints

- Direct all patient complaints related to the privacy or security of their PHI to the UConn Health Patient Relations Department or to the Privacy or Security office.
- Patients may also elect to file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights.

Refer to policy: *Patient Complaint Regarding Use and Disclosure of PHI*

Sanctions for Privacy and Security Violations

Appropriate discipline will be pursued for individuals responsible for inappropriate access, use or disclosure of PHI or other types of privacy/security incidents.

Wrongful and purposeful disclosure of protected health information carries fines and can result in incarceration.

Privacy and Security Contacts and Resources

- Privacy Office:
  - Main Number: 860-679-4180
  - Email: privacyoffice@uchc.edu
  - Iris Mauriello, Privacy Officer
    - 860-679-3501 or mauriello@uchc.edu
- Security Office:
  - Main Number: 860-679-4255
  - Tom Murphy, Chief Information Security Officer
    - 860-679-2295 or tpmurphy@uchc.edu
- **REPORTLINE** (to report concerns anonymously): 1-888-685-2637
- UConn Health HIPAA *Privacy* and *Security* policies
- University of Connecticut *Identity Theft Prevention Program*

Privacy and Security are doggone important…

and need a team effort!!

Thank you for completing Privacy and Security training.

Training Questions?
Contact Ginny Pack at 860-679-1280 or pack@uchc.edu

Please complete and sign the training acknowledgment. Return the completed acknowledgement to your appropriate school and/or UConn Health supervisors.

Knowledge Check ✓

1. Which of the following is <u>not</u> considered Protected Health Information under HIPAA?
A. An EKG report for a participant in a human subject research study.
B. A discharge summary for a John Dempsey Hospital patient.
C. A photo used for student education showing only a wound on the hand of an unidentified patient.
D. A patient invoice that includes a listing of diagnostic lab tests completed.

The correct answer is "C". Only information that cannot be linked in any way to a particular individual would not be considered PHI

2. Maria is a nursing student and has cared for a patient who had a minor procedure done in the surgery center. The patient's neighbor has come to give the patient a ride home after the procedure and is waiting with the patient. Maria needs to review the procedure and discharge instructions with the patient. Maria isn't sure if the patient has given permission to communicate with her neighbor. What should Maria do?

A. Review the information privately with the neighbor first since she is taking the patient home.
B. Review the information with the patient and neighbor together since the patient must approve if the neighbor is in the room.
C. Discharge the patient and plan to review the information during her next clinic appointment.
D. Ask the patient's permission to review the information in front of her neighbor.

The correct answer is "D". Unless you are sure the patient has given permission to communicate PHI with another individual always check with the patient before sharing any information.

3. When mailing documents containing PHI to a patient, each page must be checked and initialed to ensure that the documents do, in fact, pertain to the intended recipient.

True False

The correct answer is "true." UConn Health policy ***Handling Paper Communications About Patients Containing PHI*** *requires that all pages be checked and initialed by the individual preparing the documents to ensure the correct papers are being mailed to the correct recipient.*

4. While eating lunch in the cafeteria, you overhear a group of students discussing a patient, including diagnosis, treatment plan and prognosis. You notice other employees as well as visitors at nearby tables.
What should you do?

A. Move to another table so you won't hear the discussion.
B. Stare at the group in hopes that they get the message to end their conversation.
C. Politely remind them that they should not discuss patients in a public area.
D. Sit down and join them since the discussion sounds really interesting.

The correct answer is "C". Patient information should only be discussed in a private area and only with those that have a right to know the information.

5. Sarah is a staff member in the Cancer Center. At the request of her patient, she calls the patient to report her recent lab results. The patient has indicated on the UConn Health "Permission to Communicate" form that information may be shared with her husband, who she has identified by name. When Sarah calls the patient's home, she reaches the patient's sister who tells her that the patient is not at home. What should Sarah do?

A. Tell the patient's sister that she is calling from the UConn Health and ask that the patient return her call.
B. Tell the patient's sister that she is calling from the UConn Health Cancer Center with lab results and ask that the patient call her back.
C. Ask the sister to get a pen and paper to write down the results to give to the patient.
D. Hang up and call back at another time.

The correct answer is "A". Never leave a message containing specific information if the patient has not given permission to communicate with that particular individual.

6. Bert and Ernie are students and friends who are completing an internship on the same patient care unit. Ernie runs into a problem with his username and password and finds that he cannot log onto the computer to document in a patient's record. To save time, he asks to borrow Bert's username and password until he has a moment to contact the Information Technology Helpdesk.

What should Bert do?

A. Give Ernie his username and password to log on.
B. Offer to log on himself to allow Ernie to write his note.
C. Explain to Ernie that UConn Health policy does not allow him to share his username and password.
D. Get another student to log on and let Ernie complete his note.

The correct answer is "C". Never allow another student to use your password or ask to use a

fellow student's log on information. Remember, you will be held responsible for any electronic accesses or work completed under your username and password.

7. Jeremy, a Social Work student, is searching in an electronic system for the record of a clinic patient. The patient happens to have the same last name as a fellow student, Jill. During his search he sees Jill's name on the list of patients and notes that she has a medical record in the system. Jeremy is curious about Jill's medical information so he looks and finds that she recently had surgery.
Did Jeremy do the right thing?

A. Since Jeremy "inadvertently" discovered that Jill is a patient, it's OK to view her record.
B. Jeremy may view Jill's medical record, but he shouldn't tell her that he knows she had surgery.
C. Because Jill is a student, she cannot expect her information to be kept private. Anyone with access to a patient information system is allowed to access her record.
D. Jeremy may not access ***any*** patient's record, unless the reason is specifically related to his student responsibilities.

The correct answer is "D". Students who are also UConn Health patients are entitled to the same privacy as any patient.

8. While answering the phones in a busy clinic, you receive a phone call from a patient who reports that, in addition to her own lab results, she received the lab results of another patient in the mail. What should you do?

A. Apologize for the error and tell the recipient to throw the other individual's results in the trash. Notify your supervisor of the call when you have a chance.
B. Ask the recipient to tell you the name of the other patient and any specific PHI that was sent in error. Notify your supervisor and review the PHI that was released in error.
C. Tell the recipient to call back at another time when a staff member is available.
D. Thank the recipient for calling to report the error. Notify the unit manager or another staff member while the patient is on the phone as this is a potential privacy breach that must be managed immediately.

The correct answer is "D". The manager or staff must address the situation immediately to minimize the risk to the patient's information that was improperly disclosed.

9. An outside practitioner will be following a UConn Health patient with whom you have been working. Your preceptor/manager confirms that it is permissible to share PHI related to the patient's follow-up care with this particular practitioner. The practitioner sends you an email asking for a summary of the patient's condition and treatment.
Which of the following should you do?

A. Simply reply to the email with the information requested.
B. Reply and click the "Secure" button prior to sending the email.
C. Reply and type [secure] in the subject line or message.
D. Either B or C.

The correct answer is "D". Always click the "Secure" button or type [secure] when sending PHI outside of the institution via email.

10. Denise is a nursing student who recently assisted with a patient in the UConn Health Emergency Department (ED) that had been involved in a serious car accident. The accident was reported on the local news and on the front page of several newspapers. Denise can't wait to tell her friends about her ED experience so she posts details about the accident, the patient's injuries and a picture she took with her cell phone on her Facebook page. She is careful not to disclose the patient's name or to expose the patient's face but assumes it is OK to share other information including the patient's age, sex and town of residence.

Did Denise breach this patient's confidentiality?

Yes No

The correct answer is "Yes". Students should never photograph patients with a personal cell phone or post any photos related to their work at UConn Health on social media. In addition, even though Denise did not include the patient's name or photo of the patient's face, it is possible for others reading her post to identify the patient, given the information that was shared and the fact that the accident was highly publicized. This, therefore, would need to be evaluated as a potential breach under the HIPAA/HITECH regulations.