Welcome to Information Privacy and Security Education

Privacy and security education is required for all newly hired UConn Health employees and annually thereafter.

When it comes to protecting confidential information, privacy and security go hand in hand—without proper security, there is no information privacy. While encryption and firewalls are a necessity, each individual’s commitment to privacy and security are crucial. We each play a key role in the protection of confidential information whether related to patients, research participants, fellow employees, students, or business processes.

As you complete this education, click on the links to view additional facts or applicable UConn Health policies.

Please review the Confidentiality policy.
The right to privacy is at the heart of laws that protect the confidentiality of personal information.
Introduction

The Health Insurance Portability and Accountability Act (HIPAA) spurred the development of electronic patient records and outlined Privacy and Security Rules to manage the increasing vulnerability of patient information. HIPAA compliance is enforced by the Office for Civil Rights (OCR).

In addition to protecting health information, the Privacy and Security Rules were enacted to facilitate the proper exchange of health information needed for quality health care and to assure that patients have appropriate access to their own health information.

The Health Information Technology for Economic and Clinical Health (HITECH) Act was subsequently enacted to promote the adoption of electronic health record (EHR) systems. Anticipating a significant expansion in the exchange of electronic protected health information (ePHI), HITECH also broadened privacy and security protections under HIPAA, included more stringent enforcement of the Privacy and Security Rules and increased the potential liability for non-compliance.
Key Definitions

Click each term below for more information

Individually Identifiable Health Information

Protected Health Information

Use

De-identified Information

Minimum Necessary

Access

Disclosure
Key Definitions

Individually Identifiable Health Information

Health, demographic and financial information relating to an individual’s past, present or future physical or mental health condition or payment for health care that identifies the individual or can reasonably be used to identify the individual.

Once information can be linked in any way to a specific person, it becomes “identifiable.”
Protected Health Information

Individually Identifiable Health Information that is maintained or transmitted in any form (written text, photos, recordings, images, slides etc.) in any medium (verbal, paper, electronic etc.)
Key Definitions

Individually Identifiable Health Information

Protected Health Information

De-identified Information

Health information that excludes certain specific identifiers such that there is no reasonable way the information can be used to identify the individual.

Access

Disclosure
Key Definitions

Individually Identifiable Health Information

Protected Health Information

De-identified Information

Access

To obtain, examine or retrieve data.

Disclosure
Use

Sharing, employment, application, utilization, examination, or analysis of Individually Identifiable Health information within UConn Health.
Individually Identifiable Health Information

Protected Health Information

De-identified Information

Access

Disclosure

Release, transfer, providing access to, or divulging in any other manner information outside of UConn Health.
Key Definitions

Individually Identifiable Health Information

Protected Health Information

De-identified Information

Access

Disclosure

Minimum Necessary

The least amount of PHI needed to accomplish the intended use or disclosure.
Health information becomes “identifiable” if it can be associated with a person through *any* of these links:

- Name
- Address (mailing, email or internet)
- Zip Code
- Phone and fax number
- Social security number
- Medical record number
- License number
- Account numbers (bank, retirement, credit card, etc.)
- Fingerprints
- Full or partial photo - any picture in which an individual could be identified
- Vehicle identifier (license plate or serial number)
- Dates (birth, death, admission and discharge)
- URL and IP addresses
- Device identifiers and serial numbers
- Any codes related to the individual or codes that can be translated into identifiable information
- Any other unique number or characteristic
Patient Rights

What Does HIPAA Mean for Patients?
Look at privacy from a patient’s perspective

Privacy should be seen as important as other aspects of patient care.

Respect for patient privacy reflects respect for an individual’s dignity.

Assure patients and demonstrate in your care that their privacy is important.

Respond to any patients privacy questions and concerns.

Be mindful of potential privacy implications when using video monitoring equipment in patient care.

Ask yourself: “Am I doing everything I can to protect this individual’s privacy?”
Notice of Privacy Practices (NOPP)

The Notice of Privacy Practices explains patients’ rights and holds UConn Health accountable to patients for the use and disclosure of their Protected Health Information (PHI).

The **NOPP** must be displayed where it is readily visible to patients in each clinical area.

The **Consent to Treatment** is signed by patients:
- new to UConn Health (except patients in Correctional Managed Health Care).
- at each inpatient admission.
- at every encounter in the Farmington Surgery Center, Procedure Center, Same Day Surgery, and Emergency Department.

The consent to treatment also serves the purpose of the patient’s acknowledgment of receipt of the NOPP.
HIPAA: Patients Rights

Patients are entitled to:

- be informed of their rights under HIPAA and how their PHI will be used or disclosed.
- have access to or obtain copies of their health information. Under HIPAA, facilitating patient access to their PHI is just as important as protecting the privacy of that information.
- request corrections of information in their records.
- restrict certain disclosures of their information.
- receive an accounting of certain disclosures of their health information.
- be notified if the privacy or security of their information has been compromised.
Right to View Records

Patient requests to view their health record must be made in writing using approved forms.

The record is 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.
Right to Obtain Record Copies

Most requests for record copies should be referred to Health Information Management (HIM) Release of Information (ROI).

Individual clinics may provide copies of a patient’s information to that patient if:

- The PHI is related to care in that department.
- The treating provider approves.
- Information is needed immediately for the patient’s care.

Patient Right to Request Copies of His/Her Medical/Dental/Research and/or Billing Record
Requests for Record Amendments

Patients can request record amendments at any time during or after treatment.

_Whether granted or denied, all amendment requests must be acted upon no later than 60 days after the request is made._

For assistance with amendment requests in:

- Medical/Dental records, refer to Health Information Management (HIM).
- Research records, refer to HIM or the study’s Principal Investigator.
- Billing records, refer to Patient Services.

_Patient Right to Amend His/Her Medical/Dental/Research and/or Billing Record_
Restrictions and Confidential Communications

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.

*Patient Right to Request Confidential Communications*

*Patient Right to Request Restrictions on Use And Disclosure of Protected Health Information*
Accounting of PHI Disclosures

An accounting must be completed when PHI is released outside of UConn Health for reasons other than treatment, payment or health care operations and of which the patient is otherwise unaware (e.g. to regulatory agencies, for judicial proceedings, to medical examiners, or to report abuse, neglect and domestic violence).
Patient Authorization

Patient permission 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 including the PHI involved, who is requesting PHI, the purpose of the requested use or disclosure, and the right to revoke an authorization.

Patient authorization may also be required to use or disclose identifiable non-textual data such as patient photos, radiology images, pathology slides, physiological tracings and audio/video recordings.

**Authorization for Release of Information**

**Visual, Audio, or Other Recording of Patient Data Obtained Through Any Other Medium**
Minimum Necessary

PHI that is accessed, used or shared for any purpose other than treatment, should be limited to the “minimum necessary” information needed to accomplish the task at hand.

HIPAA also allows the minimum necessary information to be accessed and used in the academic setting for the purpose of student education.

Students at UConn Health may access and use the minimum necessary PHI consistent with clinical assignments or educational work under the supervision of an authorized faculty or staff teacher.
Patient Complaints

Patient complaints related to the privacy or security of their PHI should be directed to the UConn Health Patient Relations Department or to the University/UConn Health Office of Privacy Protection and Management.

Patients may also file a complaint with the Department of Health and Human Services Office for Civil Rights.
Keeping the “protect” in Protected Health Information
General Reminders

Wear your ID badge *at all times* and especially to enter restricted areas. This not only protects confidential information but helps to keep everyone safe.

Ensure vendors or others with approved access have current, UConn Health ID badges and remain in an approved area unless given permission to access another location.

*Do not* hold a door open or allow anyone without proper identification to access a restricted area, especially if you do not recognize the person.

If you see anyone in your department without proper ID, *ask questions or notify your department manager or person in charge*. Do not assume an individual has authorized access just because he or she is there.

Notify UConn Health police if you have any immediate safety concerns.
Conversations involving PHI

The Privacy Rule is not intended to interfere with normal communications. “Incidental disclosures” around patient care may be unavoidable but, safeguards are required to minimize opportunities for inadvertent verbal disclosures.

Discuss PHI in a private area whenever possible.

If not in a secluded area, be aware of your surroundings and anyone that may overhear your conversation. It is natural for patients and visitors to listen to care provider discussions.

Speak quietly when discussing a patient with colleagues or family members in areas such as visitor lounges, hallways, open clinical areas and around work stations.

Avoid using patient names in public areas.
Speaking with patient family and friends

Patients have the right to choose whether their PHI may be disclosed to family members or others involved in their care.

To communicate with family and friends, follow the policies that apply to your area of practice:

- Inpatient
- Outpatient
- Outpatient Psychiatry
- Dental

Even if permission to communicate is granted, patient authorization must be obtained in situations where it is normally required.

*Use and Disclosure Involving Family and Friends* which references additional policies for the areas of care listed above.
Speaking with patient family and friends

“Permission to Communicate” covers disclosures needed to assist with coordination of a patient’s care but does not necessarily grant the right to disclose PHI that is unrelated to the current care of a patient.

Patients must also be given the opportunity to object to specific disclosures of PHI.

When others are present during a discussion with a patient, ask for the patient’s permission at that time before sharing PHI. Do not assume it is OK to discuss patient information in front of family or other visitors.

If circumstances make it impossible to obtain patient permission, share only information you believe to be in the patient’s best interest.
Sharing PHI with personal representatives

PHI may be shared with a patient’s personal representative who has verified legal authority to act on behalf of that patient.

It is *not* necessary for personal representatives to be designated on the “Permission to Communicate” form.

HIPAA recognizes that a personal representative has the same rights as the patient and should be treated in the same manner with regard to PHI use and disclosure.
**Calling a patient**

PHI should not be shared during any phone conversation unless you verify that you are speaking with the patient or someone that has permission to communicate.

Use the phone number designated by the patient — *remember, if the patient designates an “alternate” phone number, that number should be used for all telephone communications.*

Confirm that you are speaking with the patient or someone that has permission to communicate about the patient.

Do not leave PHI on answering machines or with individuals not authorized by the patient.

*Telephone/Voicemail/Answering Machine Disclosure of PHI*
When someone calls about a patient

Unless a John Dempsey Hospital (JDH) patient “opts out,” hospital directory information may be disclosed including:

- hospital room and telephone number to persons that inquire about that patient by name (except patients on the Psychiatric and Department of Correction units).
- a patient’s religious affiliation to members of the clergy.

All inquiries about JDH patients must be forwarded to the UConn Health Information Desk or telephone operators.

All media requests for patient information must be forwarded to Health Marketing and Multimedia.

Directory Information: Disclosure of a Patient’s Information

Media Relations
Verifying Callers

Before sharing any PHI, verify:

- the identity of the individual requesting information, including patients who call about themselves.
- that individuals other than the patient have the right to obtain the requested PHI.
- Ask open ended questions such as “Can you please verify your address?” rather than “Is your address still….?”
- 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 all law enforcement PHI requests (including those by UConn Health Police Department) to your supervisor.

Verification of Individuals or Entities Requesting Disclosure of Protected Health Information
Protecting Paper PHI

Do:
- Keep documents that contain confidential information in locked areas or cabinets.
- Keep notes/papers with PHI with you at all times if you must carry them and avoid taking into public areas. *Shred* as soon as possible.
- Dispose of paper with PHI in locked shredder bins only.

Do Not:
- Leave documents with PHI in your personal vehicle.
- Personally transport or ask a patient to transport a paper medical record from one UConn Health location to another. Only personnel authorized to transport records or approved courier services may remove records from a building or move those records from one location to another.

*Medical/Dental Patient Records: Transportation of Paper and Other Media Records*
Faxing PHI

Take extra precautions when faxing PHI:

- Verify that you are sending a document to the correct number before faxing.
- Use only UConn Health approved cover sheets for both external and internal faxes.
- Remember to dial “9” followed by the number when faxing outside of UConn Health.
- Collect papers when you leave a fax machine.
- When dictating a note or discharge summary, provide the full name and spelling as well as location of each individual designated to receive copies.

Faxing of Protected Health Information
Mailing or handing documents to patients

Handle papers with PHI carefully to ensure patients receive correct documents such as discharge instructions and prescriptions.

Check and initial each page before mailing or handing documents with PHI.

Use *two forms* of identification when preparing and when handing documents to a recipient.

Be careful with shared printers to avoid inadvertently including unrelated documents with those being mailed.

*Handling Paper Communications About Patients including PHI*
Paper Storage and Disposal

Store PHI in locked cabinets or offices, especially when you leave the area.

Do not leave boxes of archived documents or documents to be shredded unattended or in non-secure areas.

Dispose of PHI only in *locked shredder bins*.

Never discard PHI in wastebaskets or recycling bins for convenience or because a shredder bin is full.
Electronic Health Information
Protecting ePHI
Using electronic systems appropriately

UConn Health electronic resources are *university property* to be used for business purposes only.

Confidential electronic data should be accessed only as needed for assigned UConn Health responsibilities.

*There should be no expectation of privacy.* All data stored on UConn Health systems is discoverable under certain circumstances.

*Data may not be removed from UConn Health without Privacy and Security Office approval.*

[Information Technology Computer/Electronic Resource Use Policy](#)
[UCHC Information Security: Acceptable Use](#)
[UCHC HIPAA Security Virus Protection Policy](#)
Password Security: The First Line of Protection

Create strong but easy to remember passwords by replacing letters with numbers and special characters such as:

- MyD0GJon@th@n
- N0!Pr0mises?
- Ph0t0gr@ph!

Do not share your password with others or allow anyone to access electronic systems using your login information.

Never write your password on a piece of paper taped to your monitor or kept where it is accessible to others.

UCHC Information Security: Systems Access Control
Using patient electronic systems

Search for patients by medical record number instead of name whenever possible to avoid clicking on several patients or the wrong patients to find the correct record.

Choose names carefully from patient lists and confirm before opening a record.

Do not walk away while still logged on to a computer.

Remember, you will be held responsible for electronic accesses or any activity conducted under your login.
Mobile Computing Devices (MCDs)

Any device used to access confidential UConn Health data and/or clinical network must have security controls as defined by Information Technology.

Personal smartphones or tablets used for email or any other UConn Health business must be registered and secured using Bring Your Own Device (BYOD).

Report any lost or stolen mobile devices to the UConn Health Police Department immediately.
HealthONE

HealthONE is UConn Health’s electronic medical record (EMR).

The EMR puts all inpatient and outpatient health care providers, physicians, nurses, pharmacists, and other clinical staff on one electronic platform and allows the entire care team to have immediate access to the same patient data.

HealthONE also allows UConn Health to exchange patient data with other health care institutions.

For more information:
http://uconnhealthexpress.uchc.edu/
Emailing Confidential Information or PHI

Encrypt all emails containing confidential information that are sent outside of the UConn Health network.

Check the “To” and “cc” lines carefully before hitting “Send.”

Remember, recipient names often auto-populate when you type the first few letters.

Use “Reply to All” only if you really mean to reply to all.

Do not email confidential information or PHI to non-secure sites such as your home email address.

Electronic Communication of Confidential Data

Email Communication with Patients/Research Participants

Guidelines for Outlook Email Encryption
Encrypting email messages

Click the secure icon in the upper left of the screen *or* type `[secure] (brackets and the word)` in the subject line or body of the email.
Encryption: Remember “SAFE”

Stolen or lost devices are protected from data theft.

Access and transmit data securely.

Follows HIPAA regulations.

Ensures data integrity and maintains privacy.
Texts and Social Media

For texting, use one of the following UConn Health approved secure applications:

- Voalte Personal Communicator
- TigerText application

For instant messaging, use Skype for Business.

Report any texts sent without appropriate software immediately to your program director and the IT Security Office.

Information related to your UConn Health work should not be shared on social media. Remember, individuals may be identified with minimal posted data, especially when information is associated with highly publicized events or treatment of a public figure.
Cyber Security
Social Engineering

Social engineering describes a range of malicious activity designed to trick individuals into giving away personal information and/or installing harmful software onto their electronic devices or network.

Common scams:

**Phishing**: email that invites users to click on links leading to malicious websites in order to steal IDs and passwords.

**SMiShing (SMS Phishing)**: uses SMS services to send bogus texts.

**Social Media Phishing**: phishing on social media sites like Facebook and LinkedIn.

**Vishing (Voice Phishing)**: traditional phone scams.

**USB drop**: malware-infected USB thumb drives left on the ground waiting to be picked up and used by unsuspecting passers-by.
How to spot a phishing expedition

The request is urgent and asks for some type of credentials. There are penalties for not complying with the request.

Spelling errors in the message.

The email and signature are generic, such as “Thank you—The Helpdesk” and are missing logos, accurate phone numbers, names and titles.

The URL web address doesn’t make sense and is unrelated to the supposed requesting party.
Ransomware

Ransomware, usually loaded by clicking on email links or attachments, is malicious software designed to block access to a computer system until a sum of money (ransom) is paid.

Healthcare has been targeted by attackers and is especially vulnerable as ransomware can block access to electronic patient records.

Patient care services may be disrupted and the confidentiality of patient information is jeopardized.
Protect Yourself and UConn Health

Be wary of suspicious emails, texts or phone calls that request confirmation of your personal information, offer help or direct you to act immediately.

Stop and think before clicking on unsolicited links, attachments or downloads.

Ask questions before acting on any request.

Keep up to date with anti-virus and anti-spyware security.

Never use USB drives or CDs that are free or found if you don’t know the source of the device.

For more information: Cyber Security Awareness
Identity Theft

There are certain “red flags” that signal possible ID theft such as:

- suspicious documents that appear to be forged or altered.
- inconsistent personal information such as address and phone number.
- individuals that are unable to provide identity authentication such as answers to challenge questions.

Synthetic identity theft often includes a combination of real and fake credentials that are used to create new, "synthetic“ identities.

*Trust your gut*. If something doesn’t seem right, contact the Office of Privacy Protection and Management.
Remember, the rule of thumb is to use caution when opening links or attachments.

If it doesn’t make sense, seek IT’s guidance.....*before* opening.
Managing Privacy and Security Violations
Privacy/Security Incidents

If you know of, or suspect an improper access to or disclosure of PHI or a security risk such as hacking, *immediately* notify your program director and the appropriate office:

The Office of Privacy Protection and Management: 860.486.5256
privacyoffice@uchc.edu (online *HIPAA Privacy Incident Report* is available).

IT Security Office: 860.679.2295 or cagray@uchc.edu

REPORTLINE: 888.685.2637

*Breaches of Privacy and Security of PHI and Confidential Information*
Privacy and Security Violations

Every individual is accountable to properly manage confidential information.

Individuals responsible for privacy or security policy or other violations may receive sanctions including progressive discipline:

- Counseling
- Oral Warning
- Written Reprimand
- Suspension
- Termination

Sanctions Policy for Privacy and Security Violations for Faculty and Staff
Other Privacy and Security Considerations
Research Data Privacy

A valid authorization is required to use or disclose PHI in any form for research purposes.

Research HIPAA authorizations are separate from consent unless the UConn Health Institutional Review Board (IRB) grants an exception.

Authorizations must clearly state how participants’ PHI will be used and with whom it will be shared. Waivers or alterations must be IRB-approved.

Data that includes PHI may not be transferred/disclosed outside of UConn Health until the IRB determines if authorization is required or a waiver is granted.

PHI accessed, used or disclosed without proper authorization or outside of IRB protocol parameters is considered a privacy incident and must be reported immediately to the Office of Privacy Protection and Management and to the IRB.

Use and Disclosure of Protected Health Information for Research Purposes

Limited Data Set- Creation, Use and Disclosure

Data Ownership Policy
Business Associates

Business Associates (BAs) are entities outside of the UConn Health workforce that may create, receive, maintain, or transmit PHI on behalf of UConn Health.

A Business Associate must have processes in place to safeguard the PHI it creates or receives but UConn Health may also be held legally responsible for the actions of its BAs.

Business Associate Agreements (BAAs) outline the responsibilities of UConn Health and the BA as well as document the BA’s assurances to safeguard PHI.

Business Associate Contracts
Marketing and Fundraising

UConn Health fundraising is coordinated through the UConn 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.

*HIPAA Fundraising Compliance*

*HIPAA Marketing Compliance*
Protecting Student Information

Student information is protected under the Family Educational Rights and Privacy Act (FERPA).

Under FERPA students have the right to:

- know the purpose and content of their educational records.
- expect their information to remain confidential.
- generally control disclosure of information from their records.
- request information changes and appeal a request denial.
- challenge and possibly correct record inaccuracies.
- receive copies of records supporting enrollment or transfer to another school.
- review record disclosure logs.
- report suspected or known violations to the UConn Health Schools of Medicine or Dental Medicine.
- file a complaint with the U.S. Department of Education.

In general, assume a student’s permission is needed to share any information.

“When in doubt, don’t give it out” ---- without seeking guidance.
Social Security and Credit Card Numbers

Whenever possible, eliminate or limit use of social security numbers as individual identifiers. Use other unique identifiers.

If processes absolutely require the use of social security numbers, handle with the utmost care and follow proper procedures to protect numbers from unauthorized access or disclosure.

Hide or remove social security numbers from communications unless specifically needed by recipients.

Credit card account numbers should never be collected, stored or transmitted on UConn Health devices or networks.

Credit card information may not be sent via email for any reason.
Resources and Contacts

Office of Privacy Protection and Management
Rachel Rudnick, Chief Privacy Officer
860.486.5256
rrudnick@uchc.edu

IT Security Office
Carrie Gray, Director
860.679.2295
cagray@uchc.edu

IT Help Desk
860.679.4400
helpdesk@uchc.edu

PRIVACY POLICIES
SECURITY POLICIES
We wish to acknowledge the following individuals for their assistance and contributions to this education:

Shannon Kelmelis
Michelle Mendocha
Carrie Gray
Justin Hickey
You’ve finished!

Please complete the training attestation.