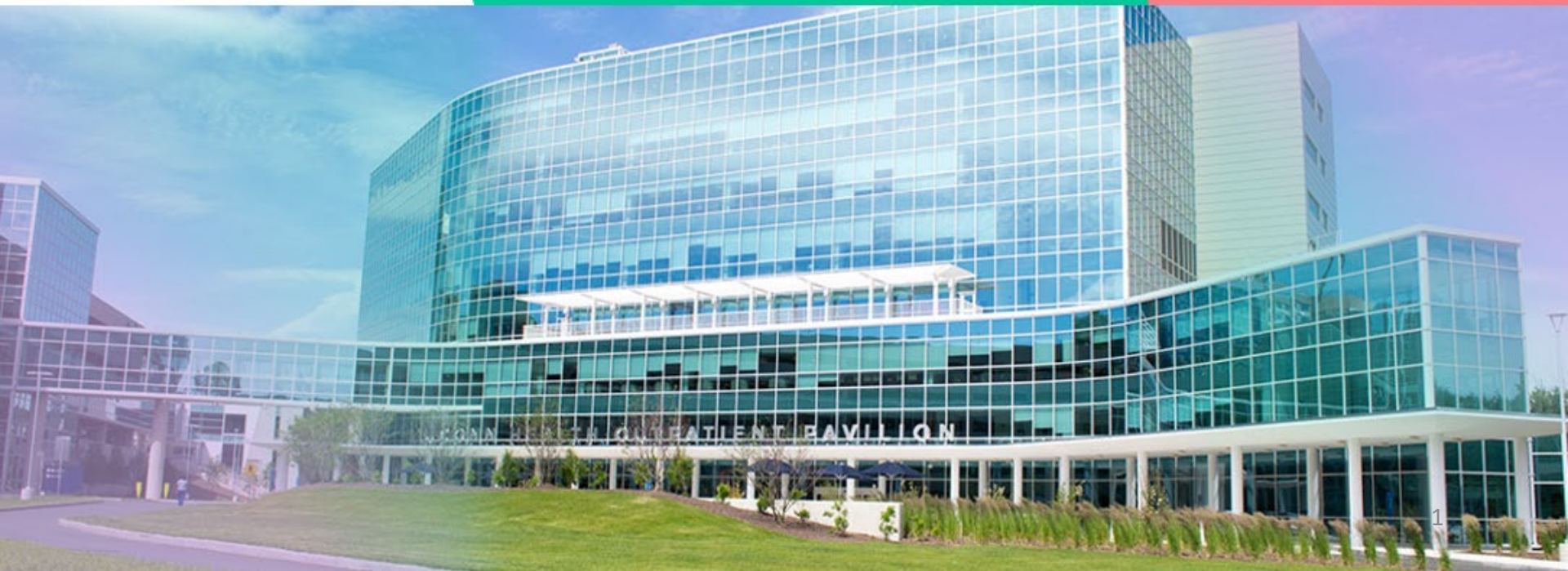
COMPLIANCE AND PRIVACY / SECURITY TRAINING

UCONN HEALTH

Unpaid Student Experience

2019 - 2020



CONTENT

This training will provide you with an overview of the Office of University Compliance, relevant laws and policies, as well as important information related to privacy and security at UConn Health.

As you complete this training, click on the available links to view applicable policies and resources.

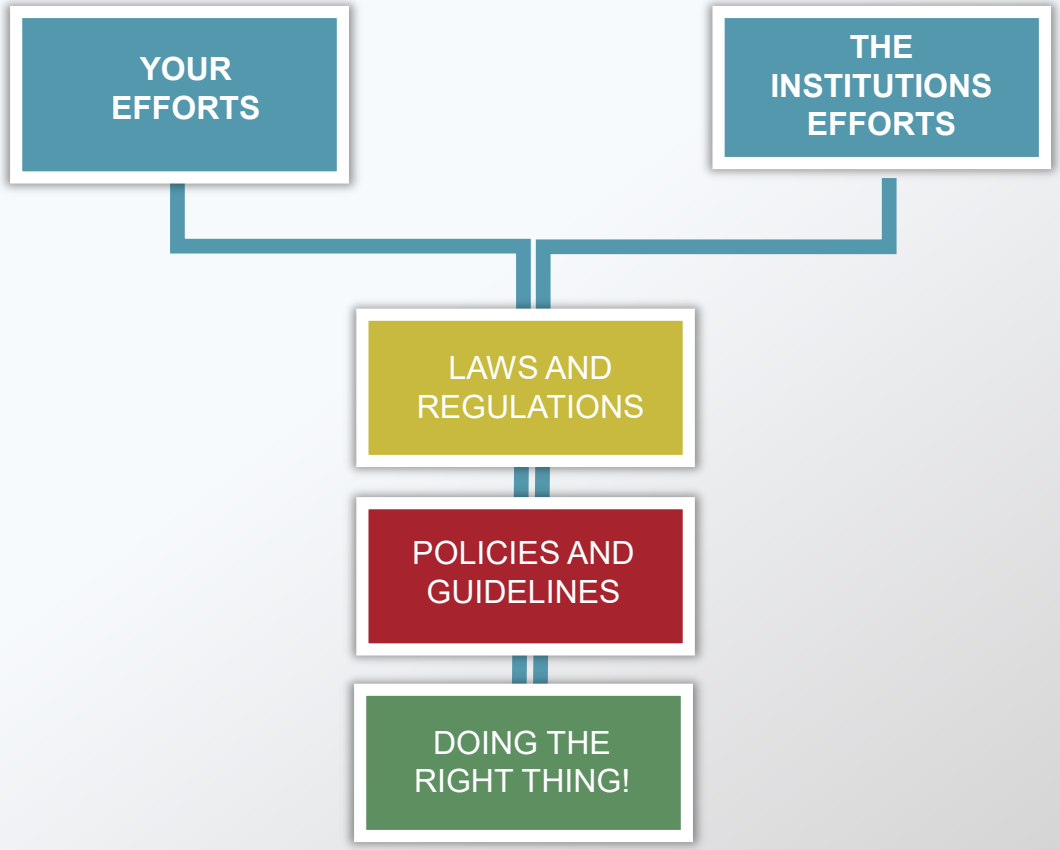
1. **Compliance at UConn Health**
2. **Information Privacy and Security**
3. **Managing Confidential Information and PHI**
4. **Protecting Electronic PHI (ePHI)**

1) COMPLIANCE AT UCONN HEALTH

WHAT IS COMPLIANCE?

In general, compliance is about your and the institutions efforts to ensure that relevant laws and regulations, as well as internal policies and guidelines are adhered to at all times.

Ultimately, compliance is about doing the right thing!



The Office of University Compliance

At the direction of the Board of Trustees, the University of Connecticut established the Office of University Compliance to assist in its efforts to promote a culture of integrity and ethical behavior, as well as to adhere to the increasingly numerous and complex federal, state, and local regulatory requirements.

At UConn Health, compliance encompasses laws, regulations, policies and standards in areas such as patient care, billing, reimbursement, student and resident education, contracting, research and information privacy and security.

WHAT WE DO

The Office of University Compliance has responsibility at all campuses, including UConn Health, and is committed to supporting the entire institution by:

- Serving as a resource regarding various ethics and compliance matters
- Providing ongoing training and education
- Coordinating compliance monitoring activities
- Developing and reviewing policies
- Identifying and investigating compliance concerns

UCONN HEALTH POLICIES

Each of us has an individual responsibility to understand and adhere to ALL UConn Health policies and procedures, and to comply with Local, State and Federal laws and regulations.

As members of the UConn Health community, we are also expected to conduct ourselves in a manner that is consistent with UConn Health's standards and core values, which include:

- **Knowledge**
- **Honesty**
- **Integrity**
- **Respect**
- **Professionalism**

REPORTING COMPLIANCE CONCERNS

We each have an obligation to report known or suspected policy violations or compliance concerns.

While you are welcomed to report concerns to your supervisor or the appropriate contact person in your department, you also have the option to report concerns to the Office of University Compliance or anonymously via the confidential **REPORTLINE**.

The **REPORTLINE** is operated by a private company and is available to accept reports anonymously 24 hours a day, seven days a week.

REPORTLINE

1-888-685-2637

Web reporting address:
uconncares.alertline.com/gcs/welcome

Available 24 hours a day, 7 days a week

NON-RETALIATION POLICY

Retaliation against any individual who, in good faith, reports a concern or participates in the investigation of alleged violations is strictly forbidden.

The Non-retaliation Policy defines how UConn Health provides for the protection of any person or group within its community from retaliation.

Anyone who believes that they have been subjected to retaliation, should either contact the office to which the initial complaint was filed or the Office of University Compliance.

View the Non-retaliation Policy

2) INFORMATION PRIVACY AND SECURITY

PRIVACY AND SECURITY

As a student, you may encounter situations in which you have access to patient health information or other types of confidential information. You are obligated to ensure the privacy and security of all confidential information with which you come in contact.

This section will familiarize you with important privacy and security principles as well as UConn Health policies and procedures.

CONFIDENTIALITY POLICY

Confidentiality applies to all types of information including:

- Patient
- Research Participant
- Student
- Employee
- Social Security / Credit Card Numbers and Other Financial Data
- System ID's and Passwords

Confidential information should only be accessed, used or shared when necessary to carry out your UConn Health responsibilities.

View the Confidentiality Policy

HIPAA - Health Insurance Portability and Accountability Act

The HIPAA *Privacy* Rule

- established standards to protect *all forms of health information* created by health care providers, health care institutions and other "covered entities."
- gives patients certain controls over their health information.

The HIPAA *Security* Rule

- established standards to protect *electronic health information* (ePHI).
- outlines security procedures to ensure the confidentiality, integrity and availability of ePHI.

HITECH - Health Information Technology for Economic and Clinical Health Act

HITECH resulted in significant changes to HIPAA Privacy and Security including widening the scope of privacy and security protections and providing incentives for health care information technology.

Protected Health Information (PHI)

PHI

PHI is any type of health information maintained or transmitted in any medium (verbal, paper, photographed, electronic, etc.) that can be linked to a specific individual by a *unique* "identifier."

ELECTRONIC PHI

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

Some individual identifiers are more obvious than others…

More Obvious	Less Obvious
Name	Vehicle identifiers e.g. license plate
Addresses including email/internet	Dates e.g. birth, death, admission
Zip code	URL and IP address
Phone and fax numbers	Device identifiers and serial numbers
Social security number	Codes related to the individual that can be translated into identifiable info
Medical record number	Any other unique number or characteristic
License numbers	
Account numbers e.g. bank, credit card	
Fingerprints	
Full/partial photo that could identify an individual	

De-identified information

Information in which ***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.

Click here to view the Creation, Use and Disclosure of De-identified PHI Policy

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.**	**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.**

For more information about patient rights under HIPAA:

Notice of Privacy Practices

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

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

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

Patient Right to Request Confidential Communications

Patient Right to Request Restrictions on Use And Disclosure of Protected Health Information

Accounting of Disclosures of Protected Health Information to Patients

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. (These are sometimes referred to as the “TPO exceptions.”)

Patient authorization may also be required to use or disclose other identifiable data such as patient photos or audio/video recordings.

Click here to view the Authorization for Release of Information Policy

Click here to view the Visual, Audio, or Other Recording of Patient Data Obtained Through Any Other Medium Policy

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.

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.

Click here to view the Minimum Necessary Data Policy
Use of PHI in Education

Patient Complaints

Patient complaints related to the privacy or security of their PHI should be directed to:

- **Patient Relations Department**
  860.679.3176 or

- **Office of Privacy Protection & Management**
  860.679.7226 / privacyoffice@uchc.edu

Patients may also file a complaint with the Department of Health and Human Services Office for Civil Rights.

Click here to view the Patient Complaint Regarding Use and Disclosure of PHI Policy

3) MANAGING CONFIDENTIAL INFORMATION AND PHI

General Reminders

Wear your UConn Health ID badge at all times to safely enter and exit restricted areas.

If you see anyone in your department without proper ID, ask questions or notify the department manager. Do not assume an individual has authorized access.

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.

Notify UConn Health Police of any immediate safety concerns.

Verbal Communications

Discuss PHI only with those that “need to know” for their assigned job or student functions.

Be sensitive to your surroundings:

Discuss PHI in a private area if possible.

Lower your voice in open areas.

Avoid discussions in public areas such as elevators and cafeterias, even if you think no one can hear you.

Calling a patient

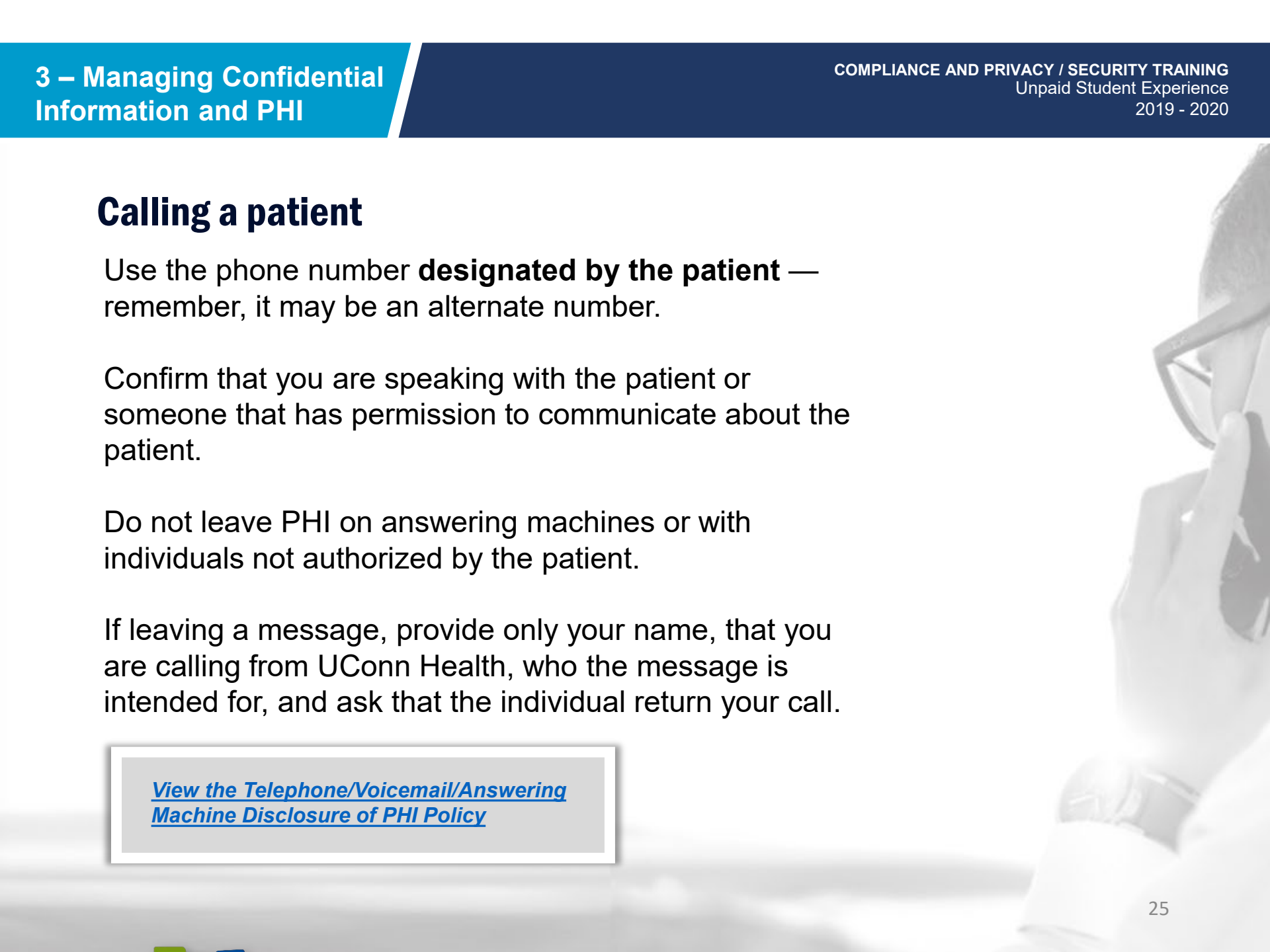
Use the phone number **designated by the patient** — remember, it may be an alternate number.

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.

If leaving a message, provide only your name, that you are calling from UConn Health, who the message is intended for, and ask that the individual return your call.

View the Telephone/Voicemail/Answering Machine Disclosure of PHI Policy



Someone calling 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.

View the Directory Information: Disclosure of a Patient's Information Policy

View the Media Relations Policy

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.

Click the view the Verification of Individuals or Entities Requesting Disclosure of Protected Health Information Policy

Protecting PHI on Paper

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.

Click here to view the Medical/Dental Patient Records: Transportation of Paper Records and Other Media Records Policy

Mailing/Handing Documents to Patients

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.

Click here to view the Handling Paper Communications About Patients including PHI Policy

Faxing Confidential Information/PHI

- Confirm the correct fax number before faxing.
- Use UConn Health cover sheets for external and internal faxes.
- When faxing outside of UConn Health, always dial “9” followed by the number.
- Collect your papers when you leave a fax machine.
- If you send a fax to the wrong recipient/location or learn of a misdirected fax sent from UConn Health, inform your supervisor or the Office of Privacy Protection & Management immediately.
- If you receive a misdirected fax from another entity, notify the sender.

Click here to view the Faxing of PHI Policy

4) PROTECTING ELECTRONIC PHI (ePHI)

Using UConn Health Electronic Systems

Electronic resources are university/state property and are to be used only for UConn Health-related business purposes.

Accesses to electronic patient information systems are monitored regularly.

UConn Health monitors usage of its electronic resources, there should be no expectation of privacy as it relates to your use of UConn Health systems and data.

Log off when you step away from a computer on which you have been working.

Click here to view the Information Technology Computer/Electronic Resource Use Policy

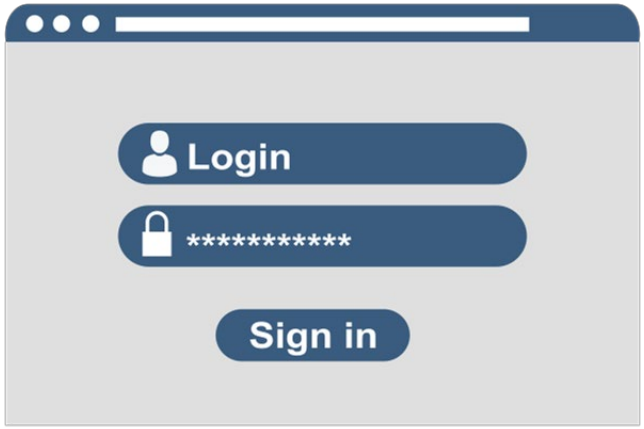
Click here to view the UCHC Information Security: Acceptable Use Policy

Click here to view the UCHC HIPAA Security Virus Protection Policy

Password Security: The First Line of Defense

Create strong but easy to remember passwords by using passphrases such as:

- Don’t3fuzzy6Bus
- stop1Hut’s2foam



Click here to view the UCHC Information Security: Systems Access Control policy

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.

You will be held responsible for all accesses by another individual using your login information.

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/

ePHI Privacy Reminders

Before you click on, open, use or disclose PHI, ask yourself “Do I need this information to complete an assigned task?

- If the answer is “yes,” it is likely OK.
- If the answer is “no,” don’t do it.

Unless related to your assigned student responsibility do not access, use or share PHI related to family, friends, employees, supervisors, and other students.

Electronic devices must be scrubbed of all UConn Health information, especially PHI, before removing from use.

Click here to view the Disposal of Documents/Materials Containing PHI and Receipt, Tracking and Disposal of Equipment and Electronic Media Containing Electronic Protected Health Information Policy

Mobile Computing Devices (MCDs)

Any device used to access confidential UConn Health data or clinical network must have approved security controls.

Personal smartphones or tablets used for email or other UConn Health business must be registered and secured through IT's Bring Your Own Device (BYOD) program.

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

Click here to view the Mobile Computing Device (MCD) Security Policy

Emailing Confidential Information/PHI

Emails containing confidential information or PHI that are sent outside of the UConn Health network must be ***encrypted***.

Communicate via email only with individuals that are properly authorized to receive the information.

Remember, recipient names may auto-populate the “To” or “cc” lines, so check all names to be sure you are sending to the correct individual(s).

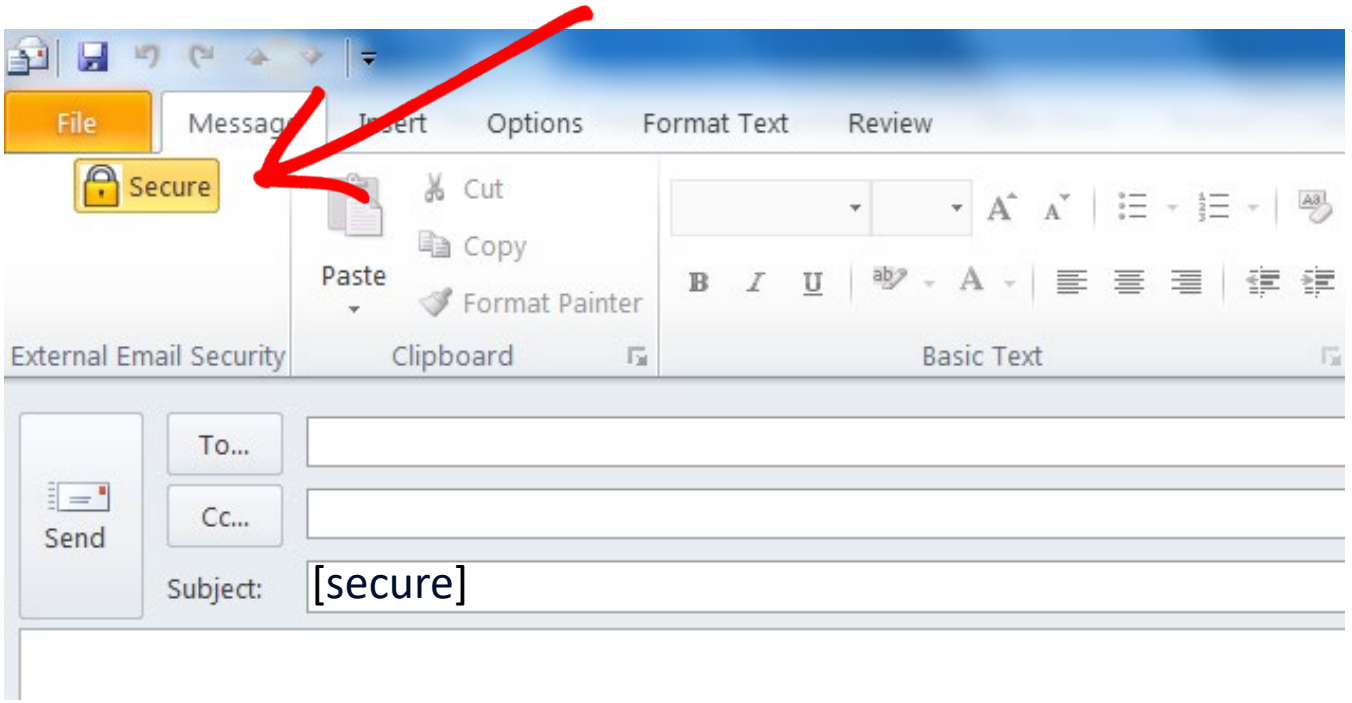
Click here to view the Electronic Communication of Confidential Data Policy

Click here to view the Email Communication with Patients / Research Participants Policy

Click here to view the Guidelines for Outlook Email Encryption

To send an encrypted 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.



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.

Texting 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. Someone may be able to identify a patient even when minimal identifying information is posted.

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.

How to report suspicious email

Helpful Resource:

PhishAlarm is a tool which allows you to easily report suspicious email.

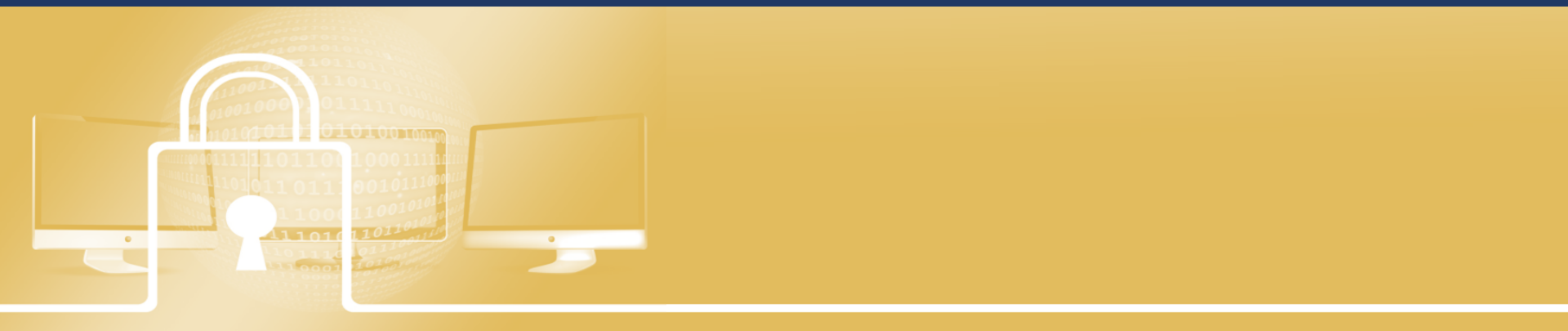
Click here to learn more about PhishAlarm.

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.
- suspected phishing and other suspicious emails should be sent to servicedesk@uchc.edu

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.**

Trust your gut. If something doesn’t seem right, contact your supervisor or the Office of Privacy Protection & Management.

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:

Office of Privacy Protection & Management:
860.679.7226
privacyoffice@uchc.edu

IT Help Desk
860.679.4400
helpdesk@uchc.edu

REPORTLINE: 888.685.2637 (completely anonymous)

Click here to view the Breaches of Privacy and Security of PHI and Confidential Information Policy

Privacy and Security Resources

Office of Privacy Protection & Management
Rachel Rudnick, Chief Privacy Officer
860.679.7334
rrudnick@uchc.edu

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

IT Help Desk
860.679.4400
helpdesk@uchc.edu

CLICK HERE TO VIEW PRIVACY POLICIES

CLICK HERE TO VIEW SECURITY POLICIES

TRAINING QUESTIONS?

Contact:

Office of University Compliance

860.679.1969

UniversityCompliance@uconn.edu

UCONN HEALTH
OFFICE OF UNIVERSITY COMPLIANCE

Unpaid Student Experience
Training Attestation

Academic Year 2019-2020

By signing below, I acknowledge that:

- I have completed this training, which covered the following:
    - **Compliance at UConn Health**
    - **Information Privacy and Security**
    - **Managing Confidential Information and PHI**
    - **Protecting Electronic PHI (ePHI)**
- I have read, understood and will abide by the University of Connecticut Code of Conduct.
- I agree to abide by all policies referenced in this training.
- I have been informed about how to ask questions of or report concerns to the Office of University Compliance, the Office of Privacy Protection and Management, and/or the IT Security Office.
- I understand that University policy prohibits retaliation toward any individual asking questions of or reporting concerns to, the appropriate authority.
- I understand that violations of the University of Connecticut Code of Conduct and/or University/UConn Health policies may result in disciplinary measures, as appropriate.

Signature: _____

Printed Name: _____

Date: _____