UCONN
HEALTH

Office of Healthcare and Regulatory Compliance
Compliance and Privacy/Security Training
Academic Year 2018-19

Dear Student,

Welcome to UConn Health. This training packet includes a general overview of compliance principles, UConn Health's Compliance Program and Privacy and Security.

Please review the training and complete and sign the training attestation. Return the signed attestation to your instructor, host, preceptor or the individual that is responsible for your student experience here at UConn Health.

The Compliance, Privacy and IT Security Offices are available to answer any questions or to address any compliance or privacy/security-related concerns during your work at UConn Health. Specific resource and contact information may be found in the training packet.

Thank you in advance for your cooperation.

Shannon Kelmelis,
Administrative Officer

UCONN
HEALTH

Healthcare Compliance and Privacy/Security Training

Unpaid Student Experience
2018-2019

Office of Healthcare and Regulatory Compliance

Compliance and Privacy/Security Training

Compliance as well as Privacy and Security training are required by federal, state, University of Connecticut and UConn Health mandates for employees and students new to UConn Health and annually thereafter.

As you complete this training, click on the available links to view applicable University or UConn Health policies.

policies

UCONN
HEALTH

Introduction to Compliance and Ethics

REQUIREMENTS
RULES
STANDARDS
GOVERNANCE
LAW
COMPLIANCE
POLICIES
TRANSPARENCY
REGULATIONS

Compliance

Compliance is about "doing things right" according to:

- Laws and regulations
  - Federal, State and Local
- Standards
  - Accreditation and Research
- Policies
  - University, UConn Health and Departmental

Ethics

Ethics is about “doing the right thing” regardless of what the law says and reflects the University’s core values:

- Knowledge
- Honesty
- Integrity
- Respect
- Professionalism

A culture of ethics facilitates compliance.

Healthcare Compliance and Ethics

Healthcare 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.

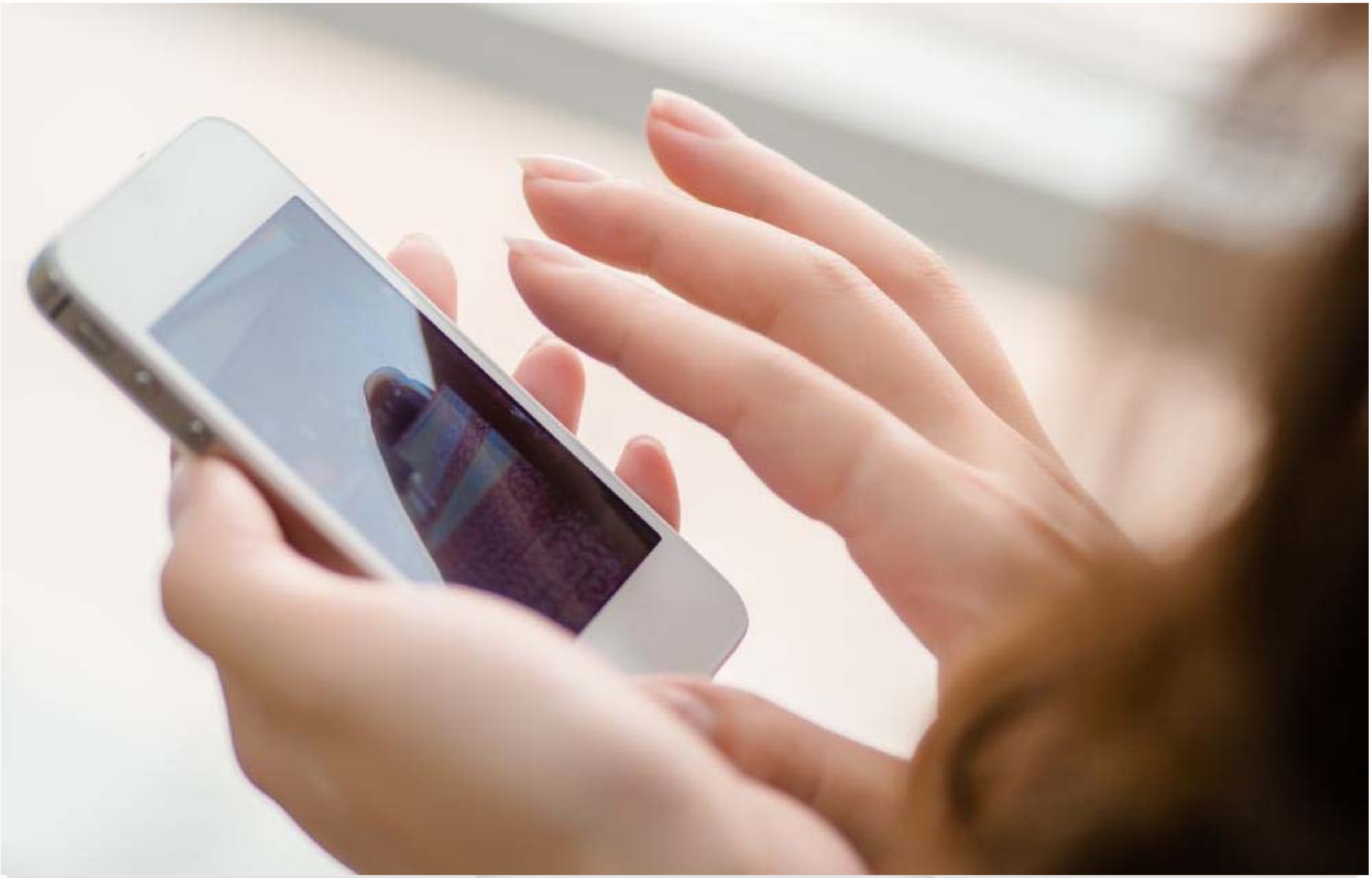
As healthcare becomes increasingly complex, institutions must understand and adhere to applicable laws to avoid consequences such as negative publicity, fines or loss of funding.

How can we help you?

The UConn Health Office of Healthcare and Regulatory Compliance facilitates individual and institutional compliance, ethics and integrity through education, consultation, monitoring of risks and investigation of potential violations.

Contact our office with any questions or concerns related to healthcare laws and regulations or UConn Health policies and procedures at 860.679.4180 or compliance.officer@uchc.edu

Reporting Compliance Concerns



Employees and students have an obligation to report known/suspected non-compliance or unethical practice.

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

Non-retaliation

UCONN HEALTH

Office of Healthcare & Regulatory Compliance

860.679.4180

compliance.officer@uchc.edu

REPORTLINE:

1.888.685.2637

You can report to:

- Your supervisor
- The Office of Healthcare and Regulatory Compliance

UCONN HEALTH

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**
- **Systems IDs and passwords**

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

Confidentiality

HIPAA
HITECH
Compliant

HIPAA

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

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

Protected Health Information (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 (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.

Creation, Use and Disclosure of De-identified PHI

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.

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

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.

Minimum Necessary Data
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 and Management 860.486.5256 rrudnick@uchc.edu

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

Patient Complaint Regarding Use and Disclosure of PHI

UCONN
HEALTH

Managing Confidential Information and PHI

General Reminders

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

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 the department manager.* Do not assume an individual has authorized access.

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.

Telephone/Voicemail/Answering Machine Disclosure of PHI

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.

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.

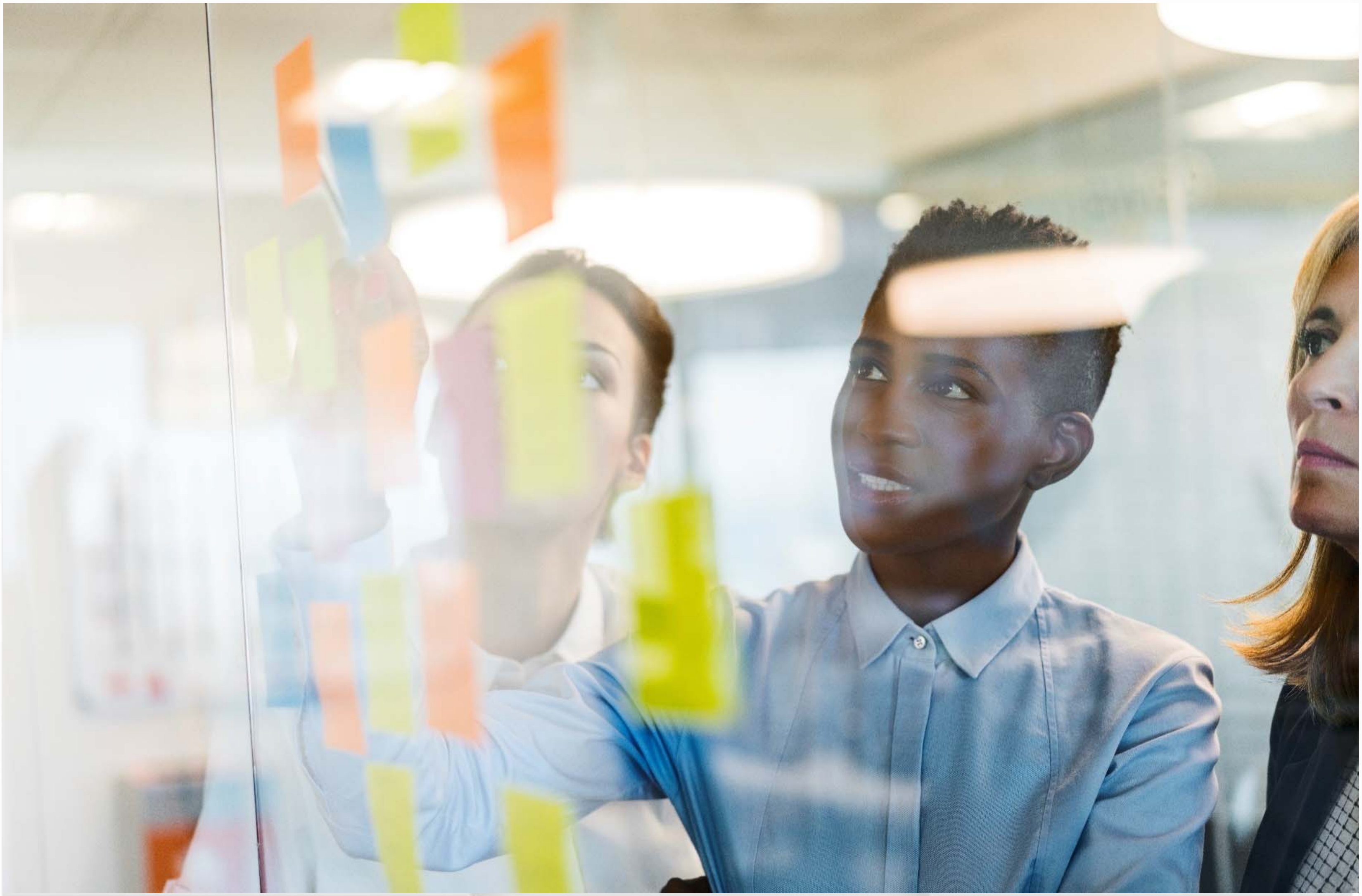
Ask open ended questions such as “Can you please verify your address?” rather than “Is your address still….?”

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 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.

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

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.

Handling Paper Communications About Patients including PHI

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 Privacy Office immediately.

If you receive a misdirected fax from another entity, notify the sender.

Faxing of PHI

UCONN
HEALTH

Protecting Electronic PHI (ePHI)

Including information from IT Security's educational brochure: "Cyber Awareness"

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.

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

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

Information Technology Computer/Electronic Resource Use Policy

UCHC Information Security: Acceptable Use

UCHC HIPAA Security Virus Protection Policy

Password Security:
The First Line of Defense

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

- MyD0GJon@th@n
- 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.

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

UCHC Information Security: Systems Access Control

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/

UCONN
HEALTH
ONE

One Place.
One Record.
One Reason.
You.

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.

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

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*.

Mobile Computing Device (MCD) Security

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.

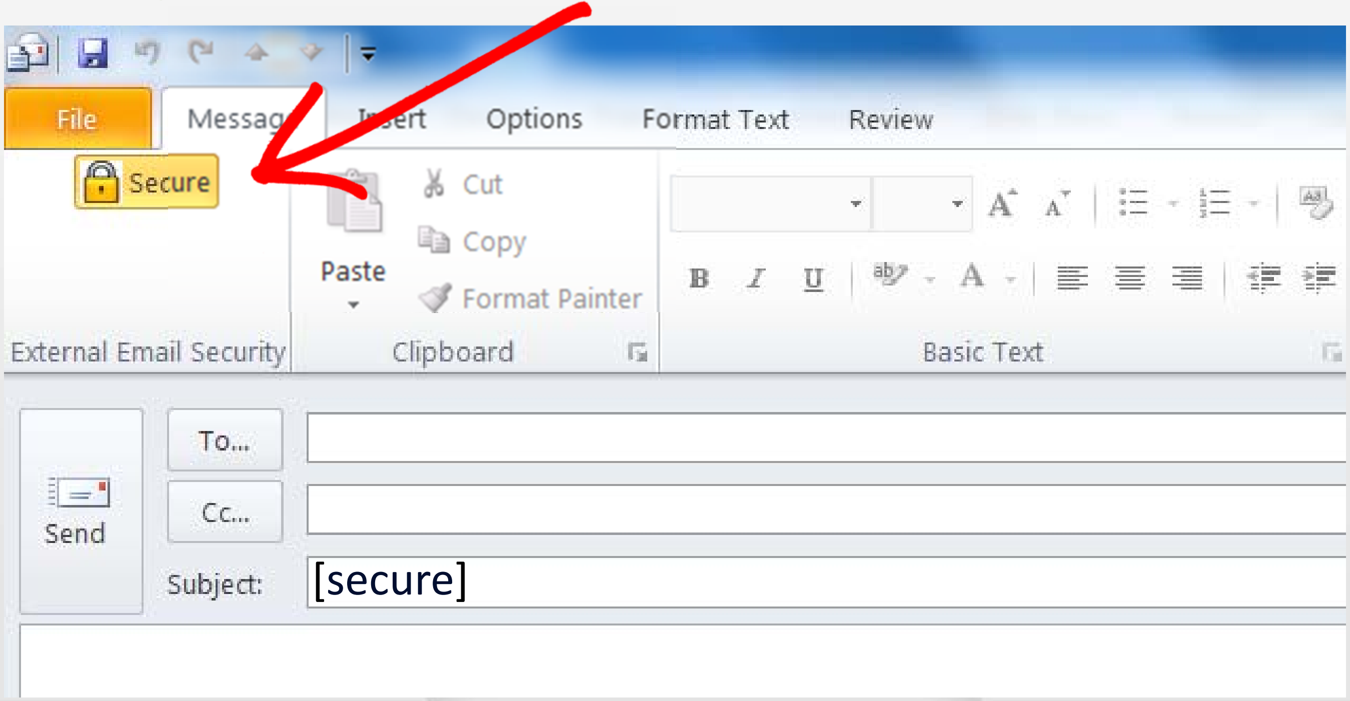
Remember, recipient names may auto-populate the "To" or "cc" lines, so check all names to be sure you are sending to the correct individual(s).

Electronic Communication of Confidential Data
Email Communication with Patients/Research Participants
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.



Subject: [secure]

Encryption: Remember “SAFE”

- **S**tolen or lost devices are protected from data theft.
- **A**ccess and transmit data securely.
- **F**ollows HIPAA regulations.
- **E**nsures 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.

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.

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

UCONN HEALTH

Managing Privacy and Security Incidents

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 (completely anonymous)

Breaches of Privacy and Security of PHI and Confidential Information

Privacy and Security Resources

Office of Privacy Protection and Management

Rachel Rudnick, Chief Privacy Officer

860.486.5256 or rrudnick@uchc.edu

IT Security Office

Carrie Gray, Director

860.679.2295 or cagray@uchc.edu

IT Help Desk

860.679.4400 or helpdesk@uchc.edu

PRIVACY POLICIES

SECURITY POLICIES

Training Questions?

Contact:

Office of Healthcare and Regulatory Compliance

860.679.4180

compliance.officer@uchc.edu

UCONN
HEALTH

Office of Healthcare and Regulatory Compliance
Unpaid Student Experience
Training Attestation
Academic Year 2018-2019

I have completed the following trainings:

- **Compliance and Ethics Overview**
- **Privacy and Security**

✓ I have read, understood and will abide by the University of Connecticut *Code of Conduct*.

✓ 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.

✓ I have been informed about how to ask questions of, or to report concerns to, the UConn Health Compliance/Privacy and IT Security Offices.

✓ I have read and understand the UConn Health HIPAA Privacy/Security/HITECH training materials.

✓ I understand that the location of additional information about UConn Health policies and procedures related to patient privacy have been detailed in the training documents.

✓ I agree to abide by all policies referenced in these trainings.

Signature:____

Printed Name:____

Date:____