2020-2021
Compliance Self-Learning Packet
PURPOSE OF THE SLP

This Self-Learning Packet (SLP) was created to help educate and orient you to some of UConn Health’s offices and efforts to ensure an environment of compliance as it pertains to UConn Health policies and standards as well as state and local laws. Included herein is information regarding the Office of University Compliance, the Office of Healthcare Compliance, and the Office of Healthcare Privacy. As a member of the UConn Health community, it is important that you carefully review this document and the referred to resources. This document is designed to help all whether it be in the learning environment, the clinical patient care environment, or the administrative working environment. Thank you, in advance, for your efforts toward promoting and contributing toward an environment of compliance at UConn Health.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>TOPIC</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Office of University Compliance</td>
<td>2</td>
</tr>
<tr>
<td>UConn Health Policies and Standards</td>
<td>2</td>
</tr>
<tr>
<td>Reporting a Compliance Concern</td>
<td>3</td>
</tr>
<tr>
<td>The Office of Healthcare Compliance</td>
<td>4</td>
</tr>
<tr>
<td>Fraud, Waste, and Abuse</td>
<td>4</td>
</tr>
<tr>
<td>Preventing Fraud, Waste, and Abuse</td>
<td>4</td>
</tr>
<tr>
<td>Privacy and IT Security</td>
<td>5</td>
</tr>
<tr>
<td>Privacy Responsibilities</td>
<td>7</td>
</tr>
<tr>
<td>IT Security – Protecting Electronic PHI</td>
<td>10</td>
</tr>
<tr>
<td>General Reminders</td>
<td>11</td>
</tr>
<tr>
<td>Training Attestation Form</td>
<td>13</td>
</tr>
</tbody>
</table>
I. ABOUT THE OFFICE OF UNIVERSITY COMPLIANCE

The Office of University Compliance has the responsibility for the coordination of the compliance program at UConn and UConn Health. The compliance program is de-centralized, meaning several offices and employees have compliance-related responsibilities that are specific to their area of expertise. The Office of University Compliance works to promote a culture of integrity and compliance throughout the institution and to ensure compliance with University policy and applicable state and federal laws.

The Office of University Compliance has responsibility at all campuses, including UConn Health, and is committed to supporting the community in several ways, including: serving as a resource regarding various ethics and compliance matters; offering ongoing training and educational initiatives; coordinating compliance monitoring activities; developing and reviewing policies; as well as, identifying and investigating compliance concerns.

For more information regarding the Office of University Compliance, please go to https://www.compliance.uconn.edu.

UCONN HEALTH POLICIES AND STANDARDS

As a member or affiliate of the UConn Health Community, it is important to familiarize yourself with the policies and procedures that govern the daily operations, including research, patient care, health and safety, regulatory requirements, and academics. Policies can be accessed at https://www.health.uconn.edu/policies. Policies are searchable and categorized by topic or policy owner.

In addition, the University's Code of Conduct for faculty and staff provides a thorough overview of how UConn and UConn Health strive to operate, as well as the core values of the institution. The Code of Conduct sets the standards for workplace behavior and the environment. As a member of the UConn Health community who will be working and learning in this environment, it is important to familiarize yourself with the Code of Conduct, found at https://policy.uconn.edu/2011/05/17/employee-code-of-conduct/.

Per the University’s Compliance Training Policy, as a member or affiliate of the UConn Health Community, you may be required to complete specific compliance related trainings in an effort to ensure compliance with University policies, as well as applicable laws and regulations.

Failure to comply with University policies, procedures, and standards may result in disciplinary action up to and including dismissal or termination of contract.
REPORTING A COMPLIANCE CONCERN

The University of Connecticut and UConn Health (Collectively “UConn”) are dedicated to the highest standard of ethical and professional conduct in its research, education, clinical service, and public service activities. Each individual associated with UConn is expected to conduct themselves according to this standard and ensure that their actions comply with UConn policies and relevant laws. To further this end, UConn welcomes and encourages reporting of compliance concerns and/or seeking guidance regarding compliance issues. The review and investigation of compliance inquiries is the responsibility of the Office of University Compliance. In addition to reporting concerns to your supervisor or manager, any individual may directly contact the Office of University Compliance directly regarding a request for guidance or to report a compliance concern.

Individuals who report possible compliance issues in good faith will be accorded privacy and/or anonymity to the extent possible under the law, unless doing so prevents UConn from fully and effectively investigating or responding to the reported concerns. The reporting individual’s identity may also become known during the normal course of the investigation. While the highest level of privacy will be maintained, anonymity and confidentiality cannot be guaranteed. With that said, individuals who report in good faith, or who participate in a compliance investigation, are protected from retaliation per the University’s Non-Retaliation Policy.

In addition to reporting concerns directly to the Office of University Compliance, you may report your concern through the 24/7 anonymous REPORTLINE. The REPORTLINE serves as an anonymous resource for employees to report or seek guidance on possible compliance issues. It is supported by a third-party vendor and staffed by professionals. It is available to anyone, including UConn employees, through phone or by an online web form with discrete intake and anonymous reporting options. You do not have to reveal your identity when you call or submit a report to the REPORTLINE.

For more information regarding the reporting process, including answers to frequently asked questions, please visit https://www.compliance.uconn.edu.

https://uconncares.alertline.com/gcs/welcome
1-888-685-2637

1-888-685-2637
Healthcare compliance is about providing safe, high-quality patient care. Healthcare organizations such as UConn Health are held to strict standards, regulations, and laws from the federal and state governments. Violations of these laws can result in lawsuits, hefty fines, or the loss of licenses. Complying with industry standards and regulations helps UConn Health to continue to improve the quality of care.

The Office of Healthcare Compliance office works to ensure compliance with federal and state laws and regulations as well as University policies. Healthcare compliance at UConn Health encompasses patient care, billing and reimbursement practices and employee and student education.

FRAUD, WASTE AND ABUSE (FWA)
Every year millions of dollars are improperly spent because of fraud, waste and abuse. It affects everyone – including you. You are a part of the effort to prevent, detect, and report non-compliance as well as possible fraud, waste, and abuse. The purpose of this training is to create awareness, understanding and prevention of Fraud, Waste and Abuse at UConn Health.

Fraud - Fraud is an intentional misrepresentation of information for unauthorized financial gain or to derive some other benefit.

Waste - Waste is a misuse of resources or practices that result in needless expenditures of UConn Health, state and/or federal funds. It often stems from individuals being uninformed, careless, or from poor decisions.

Abuse – Abuse is the improper use of funds, resources or authority that results in higher costs to UConn Health or to the state and federal governments.

There are differences between fraud, waste, and abuse. One of the primary differences is intent and knowledge. Fraud requires the person to have an intent and the knowledge that their actions are wrong. Waste and abuse does not require the same intent and knowledge as fraud.

PREVENTING FWA
Waste can be prevented by avoiding purchases or other practices that unnecessarily consume time, money or resources. Purchasing and contract decisions should be made only by individuals with adequate information and appropriate authority.
Abuse can be prevented by using UConn Health/state time, personnel and resources appropriately and only for approved *business* purposes.

To minimize the opportunity for fraud at UConn Health it is crucial that you follow established policies and appropriate departmental procedures.

You should avoid short cuts or other practices that compromise processes. Ask questions and seek guidance if you are unclear or uncomfortable with a task or responsibility. If you suspect someone is engaging in fraud, waste, or abuse, please utilize the University’s REPORTLINE to submit a report.

### III. ABOUT PRIVACY AND IT SECURITY AT UCONN HEALTH

**Office of Healthcare Privacy Office**

- Website: privacy.uconn.edu
- Email: privacyoffice@uchc.edu
- Phone Number: 860-679-7226

**IT Security**

- Website: https://health.uconn.edu/information-technology/about-us/divisions/it-security/
- Email: itsecurity@uchc.edu
- Phone Number: 860-679-4400

The UConn Health Privacy Office is responsible for developing and updating policies and procedures; training and education; monitoring and auditing compliance; investigating, analyzing and responding to privacy concerns and incidents; advising our workforce members on various projects, initiatives and contracts, and working proactively to ensure that confidential information here at UConn Health is protected.

UConn Health is committed to protecting the privacy and security of our patients, students, research participants, employees, affiliates and a myriad of other individuals with whom we interact. We are committed to confidentiality not only because it is required by state, federal and international laws and regulations, but because it is the right thing to do for our community.
In your work at UConn Health, you are obligated to ensure the privacy and security of all confidential information with which you come in contact. This mandated training and linked references will help familiarize you with important privacy and security principles as well as UConn Health policies. Please read this carefully, as violations of these laws and policies may result in patient harm, institutional harm, government penalties and fines, and disciplinary action up to and including termination from your position or contract with UConn Health.

The Health Insurance Portability and Accountability Act (HIPAA) is the primary regulation that mandates how we handle the privacy and security of confidential information and is the focus of this training. HIPAA is divided into two parts, the Privacy Rule and the Security Rule, which are discussed in more detail below.

**Privacy and Security Resources**

The Privacy and Security Offices are available to assist with any questions or concerns. In addition, privacy or security incidents, suspected breaches of PHI or non-compliance with HIPAA Privacy or Security regulations must be reported to the UConn Health Privacy or Security Office immediately. Concerns also may be reported to the anonymous REPORTLINE at 1.888.685.2637.

**Office of Healthcare Privacy**
Alyssa Cunningham, AVP, Privacy Officer
860.679.1014
alcunningham@uchc.edu

Main office line: 860-679-7226
privacyoffice@uchc.edu

**Office of IT Security**
Carrie Gray, AVP, Information Security Officer
860.679.2295
cagray@uchc.edu

IT Help Desk
860.679.4400
helpdesk@uchc.edu

**PRIVACY AT UCONN HEALTH**

Confidential information that must be protected under HIPAA is called Protected Health Information, or PHI (*the health information that is linked to a patient through individual identifiers*). This includes any individually identifiable information that relates to (1) the past, present, or future health or condition of an individual, (2) the provision of health care to an individual, or (3) the past, present, or future payment for the provision of health care to an individual, that is maintained or transmitted in any media (electronic, paper, or oral, including photographs and videos).

The list of identifiers is broader than you may think. More obvious identifiers include name, addresses (including email), zip code, phone and fax numbers, Social Security Numbers, Medical Record Numbers, License numbers, account numbers, fingerprints and full/partial photos that could identify an individual. Less obvious identifiers include vehicle identifiers such as license plate numbers, dates such as birth, date, admission, URL and IP addresses, device identifiers and serial numbers, codes that can be translated into identifiable information, and any other unique number or characteristic. More detail can be found in our [Confidentiality Policy](#).
De-Identified data, in which all identifiers have been removed and there is no chance of re-identification, is not considered PHI and not covered by HIPAA. See De-Identified Data Policy. https://health.uconn.edu/policies/wp-content/uploads/sites/28/2015/07/policy_2003_29.pdf

YOUR RESPONSIBILITIES

Accessing, Using and Disclosing PHI
Across UConn Health, only PHI or confidential information related to one’s assigned work responsibilities may be accessed, used or disclosed.

In general, healthcare providers may share PHI without patient authorization for purposes of treatment, payment for treatment or for health care operations such as quality improvement, training, compliance reviews and evaluating caregiver performance. There are other circumstances where authorization is not required before disclosing PHI as long as certain criteria are met such as for public health activities, to law enforcement or for judicial proceedings.

In most situations, if access, use, or disclosure of PHI does not fall within the treatment, payment, or operations categories outlined above, the patient must give permission via a signed authorization.

Minimum Necessary Data
With the exception of treatment purposes or where required by law, you may access, use or disclose only the minimum necessary PHI to complete a work-related duty. Workforce members may not access medical information of family, friends, co-workers, students or others unless it is required for a specific work-related responsibility. Workforce members may not access their own medical records except through normal patient protocols. The Privacy Office actively monitors your access to data.

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. Speak quietly when discussing a patient in areas such as visitor lounges, hallways, open clinical areas and around work stations. Avoid using patient names in public areas.

Verifying Requests for PHI
UConn Health must verify the identity of any person requesting access to or disclosure of protected health information as well as the requestor’s authority to have the information. In the event that the identity and/or legal authority of an individual or entity cannot be verified, the requested PHI should not be disclosed.

Disclosing PHI to Friends and Family Members Involved in a Patient’s Care
When the patient is present and has the capacity to make health care decisions, always ask for the patient’s approval before disclosing protected health information to friends or family members involved in the patient’s care. Never assume that it is OK to share a patient’s information with or in front of others without first seeking the patient’s permission.
Discussions involving family or friends should include only information necessary to assist the patient with care needs. “Permission to Communicate” covers disclosures needed to assist with coordination of a patient’s care but do not necessarily grant the right to disclose PHI that is unrelated to the current care of a patient. Patients must also be given an opportunity to object to disclosures of additional specific PHI.

When the patient is not present, is incapacitated, or in emergency circumstances discuss only information you believe to be in the patient’s best interest. Refer also to area-specific policies:

- Communication With Family and Friends – Patient’s Assigned a Bed in John Dempsey Hospital
- Communication With Family and Friends – Outpatient Hospital and All UMG Ambulatory Care Settings
- Communication With Family and Friends – Outpatient Psychiatry
- Communication With Family and Friends – Dental Settings

Sharing PHI with Personal Representatives
PHI may be shared with a patient’s legal 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.

Disclosing Patient Information to the Public and Community Clergy Members
With the exception of the Psychiatric and Connecticut Department of Correction inpatient units, unless a patient objects, UConn Health may disclose directory information including the patient’s location (room number and telephone number) to persons who inquire about that patient by name. All patient inquiries should be forwarded to the UConn Health Information Desk or telephone operators. Inquiries made by the media/press must be directed to the UConn Health Communications Department.

Physical Protection of Confidential Information
Wear your UConn Health ID badge at all times and especially to enter restricted areas. This not only protects confidential information but helps to keep everyone safe. Do not hold a door open or allow anyone without proper identification to enter 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 supervisor.

Communicating PHI on Paper
Whenever paper documents containing PHI are provided directly to or mailed to a patient, the patient’s family/legally authorized representative, or another provider of care, it is extremely important to ensure that the correct documents are provided to the correct recipient and that the recipient is authorized to receive the information (consider minors, legally authorized representatives, appropriate patient care providers).

Transporting Documents with PHI
Medical records may not be removed from any building except by personnel authorized to transport records such as courier services. UConn Health faculty and staff may not transport paper records in personal vehicles, remove records from UConn Health or personally carry them from one building to another. If a record is needed urgently for patient care, obtain permission from Health Information Management (HIM) to transport records personally between UConn Health locations in the same building. Avoid carrying individual documents with PHI anywhere unless absolutely necessary. If you must do so,
keep track of the documents and double check that you have all papers when you leave an area. Do not leave documents with PHI in your personal vehicle—ever!

**Protecting Patient Data Obtained Through Photographs, Audio or Other Recordings**

UConn Health policy outlines standards for protecting patient information in all types of media including photographs, audio recordings, radiology images and other media. Consent is required to obtain this type of data except for clinical purposes or for photos to document situations of abuse, neglect or domestic violence.

**Using PHI in Education**

If using PHI for education within UConn Health or with UConn Health students, residents and fellows, patient authorization is not needed but access only minimum necessary PHI to meet the goal. If using PHI for meetings, lectures, conferences outside of UConn Health or with other non-affiliated practitioners, the information must be de-identified or patient authorization must be obtained.

**Use and Disclosure of PHI for Research**

UConn Health may use or disclose PHI in any form for the purpose of research regardless of the source of funding provided that certain processes are followed. When required, authorizations must include specific elements and a copy must be provided to the research participant.

**Disposing of Confidential Information**

Any printed documents containing PHI must be disposed in secured shredder bins. Do not discard PHI in a trash or recycle bin. Secure methods are also required for the disposal of electronic data and output.

**Patient Rights Under HIPAA**

The Notice of Privacy Practices (NOPP) explains to patients how their PHI is used and disclosed, their rights as a patient, and how to exercise those rights. The NOPP is provided to patients and displayed prominently throughout UConn Health.

**Patient Right to View, Obtain Copies, or Request Amendments to PHI**

Patients have the right to request, in writing, to review, copy or amend health information contained in their medical, dental, research and/or billing records.

**Restrictions on the Use and Disclosure of PHI**

Patient requests to restrict certain disclosures to health plans must be honored if the disclosure is to carry out payment or healthcare operations and is not required by law and the patient has paid out of pocket and in full for a service to which the PHI pertains. Patient requests for restrictions must be reviewed and honored before using or disclosing protected health information.

**Confidential Communications**

Patients have a right to receive correspondence (including billing statements) at an address other than their home address or to receive telephone calls at a number other than their home number. We may not ask for the reason.

**Accounting of PHI Disclosures**

With the exception of disclosures for treatment, payment or health care operations, patients have the right to request, in writing, an accounting of disclosures of their PHI of which they would not otherwise be aware. If you make a disclosure, follow your department’s procedures for recording the disclosure.
IT SECURITY AT UCONN HEALTH

Protecting Electronic PHI
UConn Health electronic resources are university/state property and must be used responsibly, for business purposes only and according to applicable policies. There is no expectation of privacy. Respect the confidentiality of the information that can be accessed and preserve the integrity of the information within your control. UConn Health conducts regular monitoring of its electronic patient information systems to assure confidential information is accessed only as authorized and as needed for work-related assigned responsibilities.

Every user must have a unique login and password. Create strong passwords that are easy to remember by replacing letters with numbers and special characters. Examples include:

- MyD0GJon@th@n
- H1ker$GuiDe42,
- N0!Pr0mises?
- h0t0gr@ph!
- IL<3EdSh33ran!

Do not share your login or password with any other person or allow anyone to access electronic systems using your login information. Information Technology (IT) does not need your password to provide you or your team with IT support. Do not request, store or use anyone else’s credentials. Never allow anyone to access information or complete work under your username and always log off a shared computer.

Do not write your password down and leave the paper in an area accessible to others. You will be held responsible for improper access by another individual under your username and password.

Emailing and Texting PHI
Email encryption must be used to communicate any confidential electronic information outside of the UConn Health network. To send a secure email click on the “Secure” icon in the upper left hand corner of the email message screen or include [Secure] (brackets and the word) in the subject line or body of the email. 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.

Texting confidential information is not permitted unless a UConn Health approved secure text application is installed and activated. Information about a workforce member’s UConn Health work should not be shared on social media.

Two-Factor Authentication
Two-factor Authentication (2FA) adds an extra layer of security to your username and password process. It combines something you know (your username and password) with something you have (mobile phone, tablet, text message, landline phone) to verify your identity. All users are required to enroll a device to use as a 2nd form of authentication. Although 2FA is only in place for remote access to UConn Health systems, all users are required to enroll a device to prevent an unauthorized attacker from using your credentials. Learn More About 2FA here.
**Electronic Medical Record**

Epic 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.

Epic also allows UConn Health to exchange patient data with other health care institutions. For more information: [http://uconnhealthexpress.uchc.edu/](http://uconnhealthexpress.uchc.edu/)

**Mobile Computing Devices (MCD)**

PHI kept on a MCD must be encrypted and have secure password protection approved by UConn Health. The information should be deleted from these devices only as soon as it is no longer needed. Users may configure their personally-owned MCDs by registering and securing the device via the Bring Your Own Device (BYOD) website. At the end of your association with UConn Health, you must delete all UConn Health information from your personal devices. PHI is not permitted to be stored on personally owned devices. Report any lost or stolen devices to UConn Health Public Safety immediately.

**Cybersecurity**

Email spam (“junk mail”) may pose an extreme risk to the user and to UConn Health. Phishing scams are a form of cybercrime that involve conning users by acting as legitimate companies or organizations in order to obtain personal information such as passwords and login credentials.

Ransomware is malicious software designed to block access to a computer system until a sum of money (ransom) is paid. Healthcare has been specifically targeted by attackers and is especially vulnerable as ransomware can block access to electronic patient records. Patient care services may be disrupted putting patients at risk and jeopardizing the confidentiality of patient information. Do not click on unsolicited links or attachments in messages. Report suspicious email using the “Report Phish” button in outlook or contact the IT Help Desk at 860.679.4400 if you have any doubts about received messages.

**GENERAL REMINDERS**

- Wear your UConn Health ID badge at all times to safely enter and exit restricted areas.
- Do not hold doors 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 Public Safety of any immediate safety concerns.

For additional information, please refer to the UConn Health HIPAA Privacy, HIPPA Security, and Information Technology policies and procedures.
TRAINING ATTESTATION

Thank you for carefully reviewing the materials covered in this Self-Learning Packet (SLP), which was created to help educate and orient you to some of UConn Health’s offices and efforts to ensure an environment of compliance as it pertains to UConn Health policies and standards as well as state and local laws.

To satisfy this training requirement, please review and submit your training attestation form using the following steps.

1. Click here to open the online Training Attestation form

2. Provide your name, UConn Health affiliation, and if applicable, your associated UConn Health Department

3. Review and select the appropriate checkboxes to confirm your agreement with each of the statements on the form

4. Click the “Submit” button to finalize this process

For questions or comments related to this SLP, please contact the Office of University of Compliance at: compliance@uchc.edu.