PURPOSE OF THE SELF LEARNING PACKET (SLP)

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

UNIVERSITY COMPLIANCE

- The Office of University Compliance
- UConn Health Policies
- Reporting a Compliance Concern

HEALTHCARE COMPLIANCE

- The Office of Healthcare Compliance and Privacy
- Preventing and Detecting Fraud, Waste and Abuse

HEALTHCARE PRIVACY

- Healthcare Insurance Portability and Accountability Act (HIPAA)
- Healthcare Privacy Policies and Rules

INFORMATION SECURITY

- The Office of Information Security
- Protecting Electronic Protected Health Information (PHI)
The Office of University Compliance has the responsibility for the coordination of the compliance program at UConn and UConn Health. The compliance program is decentralized, 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
- identifying and investigating compliance concerns

For more information regarding the Office of University Compliance, please go to [https://www.compliance.uconn.edu](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](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/](https://policy.uconn.edu/2011/05/17/employee-code-of-conduct/).

Per the University’s [Compliance Training Policy](https://policy.uconn.edu/2011/05/17/employee-code-of-conduct/), 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

UConn 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, which may occur in conjunction with other offices. In addition to reporting concerns to your supervisor or manager, any individual may 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 individuals 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.

Report a Concern

https://uconncares.alertline.com/gcs/welcome

UConn’s REPORTLINE
1-888-685-2637
The Office of Healthcare Compliance and Privacy is a decentralized compliance unit at UConn Health focusing on healthcare compliance and health information privacy in the clinical environment.

The Healthcare Compliance team serves as a resource for all members of the UConn Health community, providing education and guidance on healthcare compliance matters, responding to reports of alleged non-compliance with related laws, federal healthcare program requirements and institutional policies.

The Healthcare Privacy team is a resource to UConn Health employees and patients alike, responding to privacy-related questions and concerns and investigating and responding to suspected privacy incidents.

HEALTHCARE COMPLIANCE
Preventing and Detecting Fraud, Waste and Abuse
As a member of the UConn Health community, you play an important role in our organization’s efforts to prevent fraud, waste and abuse.

- **Fraud** is an intentional misrepresentation of information for unauthorized financial gain or to derive some other benefit.
- **Waste** is the misuse of resources or practices that result in needless expenditure of state and/or federal funds. It often stems from individuals being uninformed or careless, or from poor decision-making.
- **Abuse** is an improper use of funds, resources or authority that results in higher costs to the federal or state government, including UConn Health. It is often the result of “bending the rules,” or ignoring established policies or procedures.

Examples of fraud, waste and abuse include (but are not limited to):

- Falsifying or altering documents such as checks, time cards, travel expense reports or purchase orders
- Making travel choices or procurement/vendor selections that are contrary to existing policies or are unnecessarily extravagant or expensive
- Billing customers, patients or third party payers for services when it is known that the services were not provided
- Misusing paid time, or manipulating expense reimbursements
- Offering or receiving bribes or kickbacks
- Accepting gifts or favors in exchange for awarding contracts to vendors
- Misuse of UConn Health vehicles, mail systems, IT equipment or other resources or property
- Buying unnecessary materials or equipment, or holding onto materials that could be returned or reused

Individuals who engage in these and similar activities may be liable under federal and/or state law, including but not limited to the federal False Claims Act and its Connecticut equivalent.
Federal False Claims Act

The federal False Claims Act prohibits any person from knowingly presenting, or causing to be presented, a false or fraudulent claim for payment to the federal government.

"Knowing" means you have actual knowledge that the information is false, or you are acting in deliberate ignorance or reckless disregard of the truth or falsity of the information.

Examples of practices that may violate the federal False Claims Act if done knowingly include:

- Billing for the same service more than once
- Billing for multiple services separately when payment rules require bundling the services in a single payment (a practice known as “unbundling”)
- Billing for a higher level (and more expensive) service than was performed
- Falsifying documentation to make it appear that the patient received Medicare-covered services when they did not, or to otherwise justify services that were not medically necessary

Any person who violates the False Claims Act may be liable to the federal government for:

- Civil monetary penalties of several thousands of dollars for each false claim submitted,
- And up to three times the amount of damages sustained by the government as a result of the fraud.

The federal False Claims Act permits a person with knowledge of fraud against the federal government to file a lawsuit on behalf of the government against those that committed the fraud. The person filing the lawsuit is also known as the "whistleblower" or "qui tam" plaintiff, and they may be entitled to a portion of the money recovered by the government. The law protects the "qui tam" plaintiff from retaliation that may result from their involvement in the case.

The University’s [Non-Retaliation Policy](#) likewise prohibits retaliation against any individual who, in good faith, reports or participates in the investigation of alleged violations of state or federal law or University/UConn Health policies or procedures.

Connecticut False Claims Act

Connecticut has its own false claims act that applies to fraud against Connecticut Medicaid and other medical assistance programs administered by the Connecticut Department of Social Services. Like the federal False Claims Act, the Connecticut False Claims Act permits a person with knowledge of the fraud to file a lawsuit on behalf of the State against those that committed the fraud, and in certain circumstances, to receive a portion of the money recovered by the State.

Penalties under Connecticut’s False Claims Act are also similar, and may include:

- Civil penalties of thousands of dollars per false claim
- Three times the amount of damages that the State sustains because of the fraud
- The costs of investigating and prosecuting the case

For more information about these laws and UConn Health’s policy on Fraud, Waste and Abuse Prevention and Education in Healthcare, visit [Policy_2018_02.pdf](#)
Minimizing the opportunity for Fraud, Waste and Abuse

All members of the UConn Health community are responsible for ensuring that UConn Health resources within their domain are used for authorized purposes only and in accordance with institutional policies and procedures and applicable legal requirements.

To minimize the opportunity for fraud, waste and abuse at UConn Health:

- Follow established policies and procedures
- Avoid shortcuts or other practices that compromise processes
- Assume responsibility only for activities for which you are authorized
- Ask questions and seek guidance if you are unsure of or uncomfortable with a particular task or activity
- Ensure data is accurate and timely, and verify information provided to you
- Do your part to address potential issues before they become problems, and fix processes that are deficient or prone to error

Reporting Compliance Concerns

UConn Health encourages the reporting of known or suspected compliance concerns to:

- A manager or supervisor
- The Office of Healthcare Compliance and Privacy
- UConn’s 24/7 anonymous REPORTLINE

https://health.uconn.edu/healthcare-compliance-privacy/

When in doubt, reach out!

We are here to help!
HEALTHCARE PRIVACY

Health Insurance Portability and Accountability Act (HIPAA)
HIPAA is a federal law that:
- Governs how we may use and disclose protected health information (PHI)
- Requires us to secure PHI
- Gives patients certain rights with respect to their PHI (e.g., right to access PHI)
- Requires us to notify certain parties in the event of a HIPAA “breach”

Protected Health Information (PHI)
PHI is any type of individually identifiable health information that is created, received, transmitted or maintained by a HIPAA covered entity (such as UConn Health), through which a patient may be identified in any way. It relates to past, present or future physical or mental health condition, the provision of health care, or payment for health care. PHI includes information in any format or medium, such as electronic, paper, and oral information.

Examples of PHI include:
- Name
- Social Security Number
- Address or any geographic subdivision smaller than a State
- Email address
- Phone/fax numbers
- Dates: birth, death, admissions, discharge, appointment
- Full face or other identifying photographs
- Biometric identifiers
- IP/URL address
- Driver’s License Number
- Medical record number or similar (e.g., account, insurance, certificate, license plate/vehicle)

Minimum Necessary
Access to PHI generally must be limited to the minimum PHI necessary to perform the job-related task that necessitates the access. Some exceptions apply.

EXAMPLE: HIPAA’s “minimum necessary” rule does not apply when we share PHI for treatment purposes.

Accessing Your Own or a Family Member’s Medical Record
- You may not access the medical information of family, friends, co-workers, students or others unless your job requires it
- If you are a patient of UConn Health, you may not access your own medical record except through the same mechanisms available to all other patients: the MyChart patient portal or by requesting your records through Health Information Management (HIM).

These rules apply to ALL UConn Health electronic systems and applications that contain patient information.
No Snooping!

*Snooping* is intentionally accessing patient information without a job-related need to do so. At UConn Health:

- You must have a specific **job-related reason** to view or access patient information.
- Accessing patient information out of curiosity or without a job-related need is prohibited.
- This includes coworkers’ and family/household members’ records. **Do not access their records unless your job requires it, even if they give you permission!**
- **Do not access a “VIP” or “high profile” patient’s record** (e.g., a celebrity or other person of interest) unless your job requires it.
- OHCP monitors electronic systems for snooping and other inappropriate user activity.

Privacy & Social Media

Do not post about patients on social media! Even if a patient is not identified by name within the content you wish to post, if there is any conceivable basis to believe that the individual could still be identified from that information, posting it on social media may violate HIPAA, other privacy laws and/or UConn Health policies or procedures.

**For example:**

- Describing a COVID-19 positive patient by gender, age and ethnicity only, even without using the patient’s name, may in some circumstances be enough to identify the patient.

Be sure to scan photo and video backgrounds closely before posting to ensure there is no inadvertent disclosure of patients or any information that, alone or in combination with other reasonably available information, could be used to identify a patient.

Patient Rights under HIPAA

HIPAA gives patients certain rights with respect to their PHI, including the right to:

- Access their PHI
- Request corrections to their health information
- Get a report on when and why we shared their PHI for certain purposes
- Receive a notice explaining how we may use and disclose their health information
- File a complaint with the federal government if they believe their HIPAA rights have been violated.

For more information, please review the [Patients’ Right to Access PHI](#) policy along with UConn Health’s [Notice of Privacy Practices](#).

Other Tips for Protecting Patient Privacy & Avoiding HIPAA/Privacy Policy Violations

- When emailing PHI, double check email addresses before hitting “Send.” Watch out for autocomplete!
- Be on the alert for phishing emails! Do not respond, and report phishing emails using the “Report Phish” feature in Outlook.
- When handing patients documents containing PHI, make sure the right document goes to the right patient!
- Use a shredder bin to dispose of paper PHI
- Avoid discussing PHI in high traffic areas (elevator, cafeteria, hallway, etc.)
Privacy Incidents & Breaches

HIPAA violations are serious business and may result in:

- Loss of patient trust
- Reputational harm
- Financial penalties imposed by the federal and/or State government
- Government monitoring and mandatory corrective action

Violations that constitute a "breach" as defined by HIPAA must be reported to the federal government and are published online. Depending on the nature of the information involved, a breach may also need to be reported to the CT Attorney General’s Office. We are also required to notify individual patients who are impacted by a HIPAA breach.

For more information, please review the UConn Health policy on Breaches of Privacy and Security of Protected Health Information.

Privacy Incident Report and Response

Report actual or suspected privacy incidents:

- To OHCP at privacyoffice@uchc.edu
- Report a Privacy Incident online
- UConn’s 24/7 anonymous REPORTLINE

Contact us as soon as you become aware of a potential issue or question. We are here to answer your questions and provide guidance on all privacy-related matters.

When in doubt, reach out! We are here to help!
The Office of Information Security assures the confidentiality, integrity, and availability of information 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
- N0!Pr0mises?
- IL<3EdSh33ran!
- H1ker$GuiDe42,
- h0t0gr@ph!

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 at this time, 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 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](mailto:UConn Health Public Safety) immediately.

Personally owned devices are not permitted on the Secure UConn Health network. UConn Health provides a guest network that provides internet access for personal devices.

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](mailto:HIPAA Privacy), [HIPAA Security](mailto:HIPAA Security), and [Information Technology](mailto: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 UConn Health’s Office of University Compliance, Office of Healthcare Compliance and Privacy, and the Office of Information Security and their efforts to ensure an environment of compliance as it pertains to UConn Health policies and state and local laws.

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

Click here to open the online Training Attestation form

- Provide your name, UConn Health affiliation, and if applicable, your associated UConn Health Department
- Review and select the appropriate checkboxes to confirm your agreement with each of the statements on the form
- Click the “Submit” button to finalize this process

For questions or comments related to this SLP, please contact the Office of Healthcare Compliance and Privacy at ohcp@uchc.edu