UCONN

Administrative Policy
2014-04 Sanctions for Privacy and Security Violations

Title	Sanctions for Privacy and Security Violations
Policy Owner and Contact Information	Information Technology Security itsecurity@uchc.edu Healthcare Compliance and Privacy
Applies to	All UConn Health workforce members and other individuals with approved access to UConn Health systems and confidential information.
Campus Applicability	UConn Health
Effective Date	9/14/2020

PURPOSE:
To provide a framework of appropriate sanctions for violations of Privacy and Information Security policies and procedures and to inform workforce members of UConn Health's sanction policy, which will be enforced against workforce members in violation of the organization's Privacy and Information Security policies.

POLICY STATEMENT:
All workforce members shall comply with UConn Health's Privacy and Information Security policies. Workforce members shall be subject to sanctions up to and including termination for failure to comply with the established policies and procedures.

Violations of Privacy or Information Security policies and procedures or applicable regulatory requirements will result in appropriate sanctions to be determined on a case by case basis, depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper use or disclosure of confidential information, and/or other relevant considerations. UConn students and residents/fellows will follow applicable education policy or policies and work in conjunction with UConn Health's Office of Healthcare Compliance and Privacy.

The Privacy or Security Officer will investigate reported violations of Privacy and Information Security policies and procedures or the HIPAA Rules with the assistance of the workforce member's department, General Counsel, Labor Relations, or others as deemed necessary.

REFERENCES:
45 C.F.R. §§ 164.308 and 164.530(e)
Examples of Security and Privacy Violations

RELATED POLICIES:
Confidentiality Policy 2002-43
UConn Health Information Security Policies
Residents/Fellows Policies and Procedures Manual
Academic Policies and Procedures Manual

ENFORCEMENT:

Violations of this policy or associated procedures may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, the University of Connecticut Student Code, other applicable University Policies, or as outlined in any procedures document related to this policy.

For those not employed by UConn Health, violations of this policy or associated procedures may result in appropriate sanctions including removal of access and/or termination of contract.

For students and residents/fellows, please see the policies in the applicable handbook(s).

APPROVAL:

Andrew Agwunobi (Signed)	10/27/2020
UConn Health Chief Executive Officer	Date
Kiki Nissen (Signed)	10/27/2020
Administrative Policy Committee Vice-Chair	Date
Janel Simpson (Signed)	10/27/2020
Administrative Policy Committee Chair	Date

POLICY HISTORY:

New Policy Approved:	02/17/2015
Revised:	9/14/2020

Examples of Security and Privacy Violations

The following are examples of potential privacy and security violations. **This is not an exhaustive list.**

EXAMPLE VIOLATIONS

- Sending Confidential Data* to the wrong fax, postal mail or email address
- Leaving Confidential Data, in any format, in public areas
- Discussing Confidential Data in public or inappropriate areas
- Releasing PHI without proper patient authorization
- Failure to logoff an IT application
- Failure to implement appropriate safeguards for electronic Confidential Data
- Sharing user ID and/or passwords
- Transmitting Confidential Data using an unsecured method
- Improper disposal of paper or electronic devices containing Confidential Data
- Failure to report a privacy or security violation
- Leaving detailed PHI on an answering machine
- Discussing PHI in a public area inside or outside of UConn Health without a legitimate business reason
- Installing unauthorized software with potential to harm systems
- Failure to register an information system for certification
- Research conducted on human subjects without IRB approval
- Unauthorized access of Confidential Data or electronic resources without a business need, without harmful intent
- Posting PHI to a social media account without written authorization
- Unauthorized disclosure of Confidential Data, including PHI for identity theft, fraud, or other intent to use or sell for personal or financial gain
- Unauthorized access of PHI to use against the patient in a dispute, legal proceeding or to otherwise extort, embarrass or humiliate a patient
- Introduction of malware or other malicious software into the organization’s computer systems

*Pursuant to UConn Health Policy 2002-43 Confidentiality, Confidential Data includes PHI.