



University of Connecticut Health Center

POLICY NUMBER 2005- 02

January 28, 2005

POLICY: UCHC HIPAA SECURITY ACCEPTABLE USE

PURPOSE:

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to the acceptable use of UCHC IT resources and electronic Protected Health Information (ePHI).

SCOPE:

This policy applies to all UCHC workforce:

- Employees (including faculty and staff)
- Volunteers
- Students and Residents
- Temporary staff
- Agency and contracted staff
- Credentialed staff
- Members of the Board of Directors

POLICY STATEMENT:

1. Workforce members are responsible for the appropriate use and security of ePHI when using any IT resource authorized by the appropriate department of UCHC.
2. Appropriate use includes using authorized IT resources, as assigned, in accordance with duties and responsibilities. Using IT resources in violation of policy, or any negligent or unlawful activity is considered inappropriate use.
3. The UCHC HIPAA Security policies and appropriate enterprise and departmental procedures are available to workforce members.
4. Departmental procedures shall be developed and implemented for workforce acknowledgement.
5. IT resources shall be protected from misuse, including, but not limited to: theft, unauthorized access, fraudulent manipulation and alteration of data, attempts to circumvent security controls, and any activity that could compromise the confidentiality, integrity, or availability of data.

6. Workforce members shall not tamper with or disable any security devices, including but not limited to, virus protection software and login account controls.
7. Workforce members are prohibited from introducing any unauthorized IT resources into the UCHC environment. Furthermore, the introduction of any IT resources that could disrupt any operations or compromise security is prohibited.
8. Any IT resources assigned to or in the possession of a workforce member shall be returned to a designated individual within his department when it is determined by department management that the use of those resources is no longer necessary.
9. All workforce members are to immediately report lost or stolen IT resources to their department management who shall report to the UCHC Information Security Officer (ISO).
10. Workforce members learning of or reasonably suspecting any violation of any UCHC HIPAA Security policy shall immediately report to their supervisor and/or the UCHC ISO.

Once the department manager has received notification of a known or suspected UCHC HIPAA Security policy violation, he or she shall report to the UCHC ISO, in accordance with the UCHC Breaches of Privacy and Security of PHI: Reporting Requirements, Sanctions and Mitigation Policy.

References: State of Connecticut HIPAA Security Policy
45 CFR 164.308 (a) (4) (i)

Jonathan Carroll (signed)

2/16/05

Information Security Officer

Date

Peter Deckers, MD (signed)

2/23/05

Executive Vice President for Health Affairs

Date

REPLACES: New Policy