UCONN HEALTH

POLICY NUMBER 2011-02

February 8, 2011

POLICY: UCONN HEALTH INFORMATION SECURITY - ACCEPTABLE USE

PURPOSE:
The purpose of this policy is to define the acceptable use of Health Center electronic resources with respect to confidential electronic data.

SCOPE:
This policy applies to all UConn Health workforce:

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

DEFINITIONS:
Electronic resources are computing and telecommunications devices that can execute programs or store data; examples of which may include, but are not limited to: computers, mobile computing devices, smartphones, and storage devices (USB or otherwise connected).

POLICY STATEMENT:

1. Workforce members are responsible for the appropriate use and security of confidential electronic data when using any UConn Health electronic resources authorized by the appropriate department of UConn Health.

2. Appropriate use includes using authorized UConn Health electronic resources, as assigned, in accordance with duties and responsibilities. Using UConn Health electronic resources in violation of policy, or any negligent or unlawful activity is considered inappropriate use.

3. The UConn Health Information Security policies and appropriate enterprise and departmental procedures are available to workforce members.

4. UConn Health electronic 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.

5. Workforce members shall not tamper with or disable any security devices, including but not limited to, virus protection software and login account controls.

6. Workforce members are prohibited from introducing any unauthorized electronic resources into the UConn Health environment. Furthermore, the introduction of any electronic resources that could disrupt any operations or compromise security is prohibited.

7. Any UConn Health electronic 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.

8. All workforce members are to immediately report lost or stolen UConn Health electronic resources to their department management who shall report to the UConn Health Information Security Officer (ISO).

9. Workforce members learning of or reasonably suspecting any violation of any UConn Health Information Security policy shall immediately report to their supervisor and/or the UConn Health ISO. Once the department manager has received notification of a known or suspected UConn Health Information Security policy violation, he or she shall report to the UConn Health Information Security Office, in accordance with UConn Health Information Security and/or Privacy policies.

References**:**

Data Classification and Use Policy
(Privacy & Security of Electronic Information) #2003- 31

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

Jonathan Carroll (signed) 05/31/11

Information Security Officer

Philip Austin (signed) 07/15/11

Vice President for Health Affairs **Date**

Replaces: Policy # 2005-02