UCONN HEALTH

POLICY NUMBER 2011-01

February 8, 2011

POLICY: UCONN HEALTH INFORMATION SECURITY: DATA AUTHENTICATION, PHYSICAL SAFEGUARDS

PURPOSE:
UConn Health is committed to maintaining formal policies and procedures to protect confidential electronic data from improper alteration or destruction. This includes mechanisms to ensure that confidential electronic data have not been altered or destroyed in an unauthorized manner.

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 which may include but are not limited to computers, mobile computing devices, smartphones, and storage devices (USB or otherwise connected).

POLICY STATEMENT:

1. This policy applies to all forms of confidential electronic data maintained or transmitted by UConn Health.

2. UConn Health workforce members must report to the UConn Health Information Security Office any suspected or known unauthorized data modification or destruction.

<u>Data Authentication</u>

1. Confidential electronic data shall be protected by authentication controls on all electronic resources.

2. Authentication controls shall minimally include a unique user logon and password combination.

3. The UConn Health Information Security Office will maintain policies for transmitting secure electronic messages and files.

4. Confidential electronic data shall be encrypted while stored on electronic resources whenever available and feasible or whenever deemed necessary by the risk analysis or evaluation in accordance with UConn Health Policy #2005-08, HIPAA Security Risk Management, Evaluation and Audit.

5. Confidential electronic data shall be encrypted while in transit across an open communications network. Files containing confidential electronic data intended to be transmitted outside the UConn Health Intranet shall be encrypted and transmitted using the approved secure file transfer product(s) determined by the UConn Health Information Security Office.

6. Mail messages containing confidential electronic data intended to be transmitted outside the UConn Health Intranet shall be encrypted and transmitted using the approved secure messaging product(s) determined by the UConn Health Information Security Office.

7. All other confidential electronic data transmissions, e.g. client/server connections, shall be encrypted using approved mechanisms, e.g. virtual private networks, whenever available and feasible, or whenever deemed necessary by the risk analysis or evaluation in accordance with UConn Health Policy #2005-08, HIPAA Security Risk Management, Evaluation and Audit.

8. Confidential electronic data integrity shall be sustained using approved mechanisms, e.g. hashing algorithms, electronic signatures and digital signatures, whenever available and feasible or whenever deemed necessary by the risk analysis or evaluation in accordance with UConn Health Policy #2005-08, HIPAA Security Risk Management, Evaluation and Audit.

Physical Safeguards

1. Electronic resources shall be secured using physical safeguards for protection from unauthorized access.

2. Screen locks, e.g., session timeouts, auto logoff, with password controls shall be activated on electronic resources, e.g. laptops, desktops, consoles.

3. Electronic resources shall be physically secured when not in use.

4. Virus protection shall be installed and activated on all electronic resources containing confidential electronic data where available. Additional mechanisms shall be implemented to further protect electronic resources from malicious software whenever deemed necessary by a risk analysis or evaluation.

References:

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

State of Connecticut HIPAA Security Policy
45 C.F.R. § 164.312(c) (1)
45 C.F.R. § 164.312(c) (2)
45 C.F.R. §164.308(3) (i)
45 C.F.R. §164.308(4) (i)
45 C.F.R. §164.312(d)
45 C.F.R. §164.312 (a) (1)
45 C.F.R. §164.312 (a) (2)

Jonathon Carroll (Signed)	5/31/11
Information Security Officer	**Date**
Philip Austin (Signed)	7/15/11
Vice President for Health Affairs	**Date**

Replaces: Policy #2005-01 UConn Health HIPAA IT Security: Data Authentication, Physical Safeguards