UCONN HEALTH

POLICY NUMBER 2011-03

May 13, 2014

POLICY: UCONN HEALTH INFORMATION SECURITY - SYSTEMS ACCESS CONTROL

PURPOSE:
UConn Health is committed to maintaining formal procedures to ensure that all persons who have been authorized to have access, have appropriate levels of access to confidential electronic data. UConn Health shall verify that an individual or entity seeking access to confidential electronic data is the one claimed. UConn Health shall also implement controls for systems that maintain confidential electronic data to assure access only to authorized users.

SCOPE:
This policy applies to all UConn Health workforce, UConn Health Business Associates, and UConn Health-sponsored business affiliates subject to a remote access agreement.

DEFINITIONS:
Electronic resources:

- 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).
- Computing services used by UConn Health, whether housed on-premises or remotely.

UConn Health Workforce includes:

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

UConn Health Business Associate is:

- A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, UConn Health.

UConn Health Non-Workforce includes:

- UConn Health-sponsored Business Affiliates subject to a separate remote access agreement.

POLICY STATEMENT:

Access to Confidential Electronic Data

1. The use and access of UConn Health's information systems is restricted to appropriately identified, validated and authorized individuals. Unauthorized access is a violation of applicable UConn Health policies.

2. Valid business reasons are the only reasons for accessing confidential electronic data.

3. A UConn Health sponsor, who is an employee at the level of manager or above, is responsible for ensuring appropriate clearance and authorization to access to confidential electronic data prior to granting access requests to electronic resources for all types of users (workforce, business associates, and non-workforce members.)

4. Access rights shall be properly authorized and documented by the authorized approver.

5. Access rights shall be periodically audited as required by the system owner with assistance from the UConn Health Information Security Office, as may be necessary.

6. The authorized approver shall reevaluate access rights when an account holder's access requirements to confidential electronic data change (e.g., job assignment change, change to remote access agreement). Modifications to account-holder's access to electronic resources shall be properly authorized, documented, and processed in accordance with the appropriate system access control procedures.

7. Minimum necessary access will be assured such that access to systems, assigned views or roles, and remote access ability will be consistent with the authorized user's valid business purpose only.

8. UConn Health organization-wide procedures shall be developed and implemented by the system owner and/or UConn Health IT, and approved by the UConn Health ISO for authorizing any person's access to electronic resources..

9. Procedures for authorizing access to UConn Health electronic resources shall be maintained by the system owner and/or UConn Health IT.

10. Only UConn Health IT staff or designated system administrators for systems not administered by UConn Health IT, are permitted to create or change access control settings.

User ID and Password Administration

UConn Health will implement user authentication mechanisms for access to information systems. Each individual user will have a unique user name or number sign-on. This unique sign-on shall be coupled with, including but not limited to, one of the following second level authentication mechanisms:

- Passwords
- Biometric devices
- Token

Persons authorized to have access to electronic resources shall not share assigned unique system identifiers (or login names) with any other person, unless for authorized IT support purposes.

Anonymous access, including the use of guest and public accounts, to any UConn Health electronic resource is prohibited.

Passwords:

a. Must be at least six characters long and include at least one number or symbol; they must not contain the user's ID.

b. Passwords must be different from previous passwords used for at least 5 cycles, and changed at least once every 90 days.

c. Passwords shall not be shared with any other person.

d. Passwords shall be encrypted for storage and transmission whenever available, or whenever deemed necessary by the risk analysis or evaluation in accordance with the UConn Health Information Security Risk Management, Evaluation, and Audit Policy.

e. System administrator or system supervisor passwords will be changed every 90 days.

f. Password controls shall force periodic password changes every ninety days whenever available.

g. Password controls shall lockout login accounts after three unsuccessful login attempts, whenever available. Electronic sessions will be automatically terminated after period of time deemed appropriate by the UConn Health Information Security Office.

Additional Controls:

a. Screen locks (e.g., session timeouts, auto logoff) with password controls shall be activated on electronic resources.

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

c. Staff are reminded that they should not leave electronic resources unattended while still logged on. Additionally, staff should not use an electronic resource under another person's log on credentials.

Termination of System Access – Workforce

1. The authorized approver shall be responsible for making appropriate and timely requests for UConn Health systems account deactivation.

2. Upon separation from employment or change of job responsibilities within UConn Health, Human Resources in coordination with Information Technology, shall make necessary changes to security levels within a reasonable time for those systems administered by UConn Health IT; except in the case of adverse separation which will be addressed immediately. Departments which administer their own systems will be responsible for account deactivation in the same timeframes

Termination of System Access – Non-Workforce

1. Non-workforce Participants shall be responsible for making appropriate and timely requests for UConn Health electronic resource account deactivation as noted in the signed remote access agreement.

References:

2003-31 Data Classification and Use Policy
2007-07 Information Technology Computer/Electronic Resource Use Policy
2011-02 UConn Health Information Security – Acceptable Use Policy
2011-01 UConn Health Information Security Data Authentication, Physical Safeguards

State of Connecticut HIPAA Security Policy
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)

Jonathan Carroll (Signed) 6/5/14

Jonathan Carroll **Date**
Interim Chief Information Officer

Frank M. Torti (Signed) 7/3/14

Frank M. Torti, M.D., M.P.H. **Date**
Executive Vice President for Health Affairs

Replaces: Policy # 2005-05 UCHC HIPAA Security Information- Systems Access Control
Revised: 2/8/11; 5/13/14