UCONN HEALTH

POLICY NUMBER 2005-04
January 28, 2005

POLICY: UCONN HEALTH HIPAA SECURITY FACILITY ACCESS CONTROL (Privacy and Security of Protected Health Information (PHI))

PURPOSE:
UConn Health is committed to maintaining formal procedures to limit physical access to all forms of protected health information (PHI) and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. UConn Health will safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

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

POLICY STATEMENT:

1. This policy applies to all forms of PHI maintained or transmitted by UConn Health pertaining to an individual.

2. This policy applies to all UConn Health campus and off-site exterior and interior premises and buildings.

3. The Campus Security Master Plan serves as the standard for safeguarding facilities and premises from unauthorized physical access, tampering or theft, including the equipment contained therein. Each location containing PHI shall have a Facility Security Plan (FSP) specifically designed to protect those facilities, premises and equipment which contain PHI. The plan, or any changes to the plan, should be submitted and approved by the department head.

4. Each FSP shall include:
   - Specific location of PHI
   - Access control procedures
   - Servers/record rooms containing PHI must be under constant observation or secured from unauthorized access.

5. Options available to restrict access include but are not limited to:
   - Restricted room keys
   - Electronic keypad / card reader type locks

6. Any location with department server(s) not located in the IT Data Center shall assure that Telecommunications has an updated list of department emergency contacts.

7. Any departmental server(s) not located in the IT Data Center shall adhere to the public safety restricted room policies, which requires:
   - A list of authorization persons submitted to public safety
   - List of emergency contacts
   - Contact information for the administrative owner of the server.

8. A procedure shall be implemented to maintain service logs that track:
   - Date
   - Time
   - Vendor Employee name
   - Company
   - Reason for access.
   - Hours of operation
   - Emergency contact for off hours accessibility

Reference: 45 C.F.R. §164.310(a)(1)
45 C.F.R. §164.310(a)(2)
Facility Access Control Procedure
Computer Equipment Installation, Maintenance and Repair Log procedures
State of Connecticut *"State HIPAA Security Policy"* Release 2.0 November 30, 2004

Jonathan Carroll (signed)	2/16/05
Information Security Officer	**Date**
Iris Mauriello (signed)	2/10/05
Privacy Officer	**Date**
Steven Strongwater, MD (signed)	2/23/05
Associate Dean for Clinical Affairs	**Date**
Susan Whetstone (signed)	2/23/05
Chief Administrative Officer	**Date**
Peter Deckers, MD (signed)	2/23/05
Executive Vice President for Health Affairs	**Date**

Replaces: NEW POLICY