



# University of Connecticut Health Center

**POLICY NUMBER: 2005-05**

**January 28, 2005**

**POLICY: UCHC HIPAA SECURITY INFORMATION  
SYSTEMS ACCESS CONTROL**

**PURPOSE:**

University of Connecticut Health Center (UCHC) is committed to maintaining formal procedures to ensure that all workforce members have appropriate levels of access to all forms of electronic protected health information (ePHI) and to prevent those personnel who should not have access to such information from obtaining access to ePHI. UCHC shall verify that an individual or entity seeking access to ePHI is the one claimed. UCHC shall also implement technical policies and procedures for electronic information systems that maintain electronic ePHI to allow access only to those persons or software programs that have been granted access rights.

**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:**

Access to ePHI

1. The use and access of UCHC's information systems is restricted to appropriately identified, validated and authorized individuals. Unauthorized access is a violation of UCHC's policies.
2. Valid business reasons are the only reasons for accessing ePHI.
3. Department managers are responsible for ensuring that workforce clearance and authorization to access to ePHI shall be performed for all workforce members prior to granting access requests to IT resources.
4. Access rights shall be properly authorized and documented by the department manager.
5. Access rights shall be periodically audited as required by the UCHC Information Security Officer (ISO).

6. The department manager shall reevaluate access rights when a workforce member's access requirements to ePHI change (e.g., job assignment change). Modifications to workforce member's access to IT resources shall be properly authorized, documented, and processed in accordance with the appropriate system access control procedures.
7. Access rights shall not exceed the minimum necessary for a workforce member's assigned duties.
8. UCHC organization-wide procedures shall be developed and implemented by UCHC IT Department, and approved by the UCHC ISO for authorizing workforce members and requirements in this subpart.
9. Security configurations shall be maintained on IT resources to restrict access to ePHI to only those workforce members or software programs that have been granted access.
10. Only Information Technology Department staff or system administrators are permitted to create or change access control settings.

#### User ID and Password Administration

1. UCHC will utilize user authentication mechanisms for access to information systems. Each individual user will have a unique user name or number sign-on. This unique name or number sign-on shall be coupled with, including but not limited to, one of the following second level authentication mechanisms:
  - Passwords
  - Biometric devices
  - Token
2. Workforce Members shall not share assigned unique system identifiers (or login names) with any other person, unless for authorized support purposes.
3. Anonymous access, including the use of guest and public accounts, to any IT resource is prohibited.
4. Passwords must be at least six characters long and include at least one number or symbol; they must not contain the user's ID. Passwords must be different from previous passwords used for at least 5 cycles, and changed at least once every 90 days. Passwords shall not be shared with any other person.
5. Passwords shall be encrypted for storage and transmission whenever available, or whenever deemed necessary by the risk analysis or evaluation in accordance with the UCHC HIPAA Security Risk Management, Evaluation, and Audit Policy
6. System administrator or system supervisor passwords will be changed every 90 days.
7. Password controls shall force periodic password changes every ninety days whenever available
8. 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.
9. Password protected screen savers shall be used on all systems when available.

#### Termination of System Access

1. UCHC organization-wide procedures shall be developed and implemented for terminating Workforce Member access.
2. The Workforce Member's direct supervisor shall be responsible for making appropriate and timely requests for IT resource account deactivation.

3. Upon separation from employment or affiliation or change of job responsibilities within UCHC, Human Resources in coordination with Information Technology, shall make necessary changes to security levels within a reasonable time; except in the case of adverse separation which will be done immediately.

Reference      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)

2/16/05

---

**Information Security Officer**

---

**Date**

Peter Deckers, MD (signed)

2/23/05

---

**Executive Vice President for Health Affairs**

---

**Date**

**Replaces:      NEW POLICY**