



University of Connecticut Health Center

POLICY NUMBER 2005-01

January 28, 2005

**POLICY: UCHC HIPAA IT SECURITY:
DATA AUTHENTICATION, PHYSICAL SAFEGUARDS**

PURPOSE:

University of Connecticut Health Center (UCHC) is committed to maintaining formal policies and procedures to protect electronic protected health information (ePHI) from improper alteration or destruction. This includes mechanisms to ensure that electronic protected health information has not been altered or destroyed in an unauthorized manner.

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:

1. This policy applies to all forms of electronic protected health information (ePHI) maintained or transmitted by UCHC.
2. UCHC workforce members must report to the UCHC Information Security Officer (ISO) any suspected or known unauthorized data modification or destruction.

Data Authentication

1. ePHI shall be protected by authentication controls on all IT resources
2. Authentication controls shall minimally include a unique user logon and password combination
3. A UCHC organization-wide procedure shall be developed and maintained by the UCHC ISO for transmitting secure electronic messages.
4. A UCHC organization-wide procedure shall be developed and maintained by the UCHC ISO for transmitting secure files.

5. ePHI shall be encrypted while stored on IT resources whenever available and feasible or whenever deemed necessary by the risk analysis or evaluation in accordance with UCHC Policy #2005-08, HIPAA Security Risk Management, Evaluation and Audit..
6. ePHI shall be encrypted while in transit across an open communications network. Files containing ePHI intended to be transmitted outside the UCHC Intranet shall be encrypted and transmitted using the approved secure file transfer product(s) determined by the UCHC ISO.
7. Mail messages containing ePHI intended to be transmitted outside the UCHC Intranet shall be encrypted and transmitted using the approved secure messaging product(s) determined by the UCHC ISO.
8. All other ePHI 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 UCHC Policy #2005-08, HIPAA Security Risk Management, Evaluation and Audit.
9. ePHI 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 UCHC Policy #2005-08, HIPAA Security Risk Management, Evaluation and Audit.

Physical Safeguards

1. IT 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 IT resources, e.g. laptops, desktops, consoles.
3. Portable IT resources, e.g. laptops, shall be physically secured when not in use.
4. A decentralized procedure shall be developed and implemented for securing portable IT resources.
5. Virus protection shall be installed and activated on all IT resources containing ePHI where available. Additional mechanisms shall be implemented to further protect IT resources from malicious software whenever deemed necessary by the risk analysis or evaluation in accordance with UCHC Policy #2005-08, UCHC HIPAA Security Risk Management, Evaluation and Audit.

References: 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)

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