



University of Connecticut Health Center

POLICY NUMBER 2005-08

January 28, 2005

**POLICY: UCHC HIPAA SECURITY RISK MANAGEMENT,
EVALUATION, AND AUDIT**

PURPOSE:

University of Connecticut Health Center (UCHC) is committed to taking effective steps to minimize or eliminate any potential risks and vulnerabilities to the electronic protected health information. UCHC shall continually assess potential risks and vulnerabilities to protected health information (PHI), including electronic protected health information, in its possession, and develop, implement, and maintain appropriate security.

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:

Risk Management

1. This policy applies to all forms of electronic protected health information (ePHI).
2. UCHC department managers shall conduct, prior to the initial HIPAA Security Rule compliance date, and maintained on a routine schedule, a risk analysis process of security and access control measures using the Information Security Officer (ISO) approved UCHC risk analysis methodology.
The process shall include both technical and non-technical evaluations performed to establish the extent to which its computer systems and networks meet a pre-specified set of security requirement.
3. The ISO will develop and ensure the implementation of an organization-wide procedure for performing risk analysis. The risk analysis shall demonstrate, at a minimum, the following information:
 - a. The level of risk associated with each potential vulnerability exploitation
 - b. Steps to be taken to reduce the risk of vulnerability exploitation;
 - c. Processes for maintaining no more than the acceptable level of risk.

- d. Technical evaluations including security functional testing, penetration testing, analysis and verification as appropriate.
4. UCHC's ISO and department managers will ensure that the risk analysis and risk management procedures are conducted.
5. Non-compliance and unacceptable risks shall be mitigated to a reasonable and appropriate level as defined by the ISO and department managers.
6. Results of all risk analysis shall be securely stored using authorized mechanisms determined by the ISO.
7. The ISO and appropriate HIPAA review committees will review the outcome of the risk analysis findings.

Evaluation

1. The ISO and System Owners shall conduct an evaluation of UCHC compliance with technical and non-technical HIPAA security standards on a scheduled basis.
2. Technical and non-technical evaluations shall be conducted when there is an environmental or operational change that possibly affects the security (confidentiality, integrity, or availability) of ePHI.
3. Results of non-compliance shall be remediated as soon as practicable, depending on specific circumstances and the acceptability of the risk determined by the ISO and department managers.
4. Results of all technical and non-technical evaluations shall be securely stored using authorized mechanisms determined by the UCHC ISO.
5. The ISO will develop and ensure the implementation of an organization-wide procedure for performing evaluations.

Audit

1. The ISO shall approve and execute an audit program for the purposes of measuring departmental compliance with UCHC HIPAA Security Policies

References: State of Connecticut HIPAA Security Policy
45 C.F.R. §164.308(1) (ii) (A) (B)

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