



University of Connecticut Health Center

POLICY NUMBER 2003-09

January 28, 2005

POLICY: BREACHES OF PRIVACY & SECURITY OF PROTECTED HEALTH INFORMATION (PHI): REPORTING REQUIREMENTS, SANCTIONS AND MITIGATION (Privacy and Security of Protected Health Information (PHI))

PURPOSE: UCHC's (University of Connecticut Health Center) policies regarding privacy and security of protected health information reflects its commitment to protecting the confidentiality of patient's medical records, patient accounts, clinical information from management information systems, confidential conversations, and any other sensitive material as a result of doing business. To ensure compliance with these policies and to ensure that the disciplinary actions taken as a result of breach of patient confidentiality are applied consistently, UCHC has adopted the disciplinary process in this policy.

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. The process outlined in this policy includes initial reporting responsibilities, the investigation process followed, sanctions and appeals, UCHC's duty to mitigate damages created by breaches and the documentation requirements of these processes.
2. PHI is confidential and must be treated with respect and care by any individual with access to this information.
3. A breach of confidentiality is defined as violating the provisions of UCHC's Confidentiality Policy or the HIPAA Privacy or HIPAA Security Policies. As a medical/dental health care provider, UCHC is entrusted with demographic, financial and clinical information regarding our patients. Any breach in confidentiality by workforce members is subject to formal discipline up to and including termination as set forth in this policy. Policy guidelines shall be observed by the entire organization, and sanctions applied fairly and consistently to all individuals in violation of the policies.

Examples of breaches of confidentiality and security; *this is not an all-inclusive list.*

- Individuals discussing patient information in any public area where those who have no need to know the information can overhear.
- Individual leaves a copy of patient medical information in a public area.
- Individual leaves a computer unattended in an accessible area with medical record information unsecured.
- Failure to log off computer terminal.
- Sharing or exposing passwords.
- An individual improperly accesses, reviews and/or releases birth dates, addresses of friends or relatives, or requests another individual to do so.
- An individual improperly accesses, reviews and/or releases the record of a patient out of concern or curiosity, or requests another individual to do so.
- An individual improperly accesses, reviews and/or releases a patient record to use information in a personal relationship.
- An individual accesses, reviews and/or releases the patient record of a public personality for the intent of giving or selling information to the media.
- An individual improperly accesses, reviews and/or releases confidential information of another member of the UCHC workforce that is also a patient.
- An individual improperly accesses, reviews and/or releases confidential information that may bring harm to the organization or individuals associated with it.

1. Initial Reporting Responsibilities

- A. Breaches by persons or behaviors resulting in breaches of confidentiality or security: The individual who observes or is aware of some type of improper disclosure of information or security incident is required to report it in one of the following ways:
- Immediate supervisor
 - Department Head or Manager of the area in which the individual works
 - Assistant or Associate Dean or Dean of Appropriate School
 - Privacy Officer
 - UCHC Corporate Compliance Integrity Officer
 - UCHC Information Security Officer (ISO)
 - Human Resources
 - Confidential "Reportline" (1-888-685-2637)

The original contact person notified under Section A must notify the UCHC ISO for breaches technological in nature or the Privacy Officer for breaches behavioral in nature.

- B. Security Incident: Once a security incident or suspected incident has been reported, the UCHC ISO shall immediately execute its incident response procedures. Harmful effects of security incidents that are known to the Department and/or UCHC ISO shall be mitigated, to the extent practicable, by the UCHC ISO, department staff and management, and any other designated agents, where appropriate.

- C. Confidentiality: Confidentiality of all participants in the situation shall be maintained to the extent reasonably possible throughout the investigation. Some circumstances may dictate notification to staff and third parties, but this is at the discretion of the designated Health Center administrative official. Such official may direct such other persons conduct the inquiry, as they deem appropriate.
- D. Bad Faith Reports: Reporting a breach in bad faith or for malicious reasons may be interpreted as a misuse of the reporting mechanism(s) and may result in disciplinary action.

2. Investigations of Reported Breaches

- A. Information pertaining to investigations of breaches will only be shared with those who have need to know. The investigator(s) will conduct the necessary and appropriate investigation commensurate with the level of breach and the specific facts. This investigation may include, but is not limited to, interviewing the individual accused of the breach, interviewing other individuals, and reviewing pertinent documentation.
- B. Existing UCHC procedures for disciplinary action shall be utilized; For example:
 - 1.) If the individual accused of the breach belongs to a collective bargaining union, Human Resources and union representation will be necessary to protect the rights of the individual.
 - 2.) If the individual accused of the breach is a faculty member or non-faculty professional, the process will be as outlined under applicable by-laws.

3. Disciplinary Sanctions and Appeals

- A. Sanctions may include, but are not limited to:
 - Counseling
 - Oral Warning
 - Written Warning
 - Suspension
 - Termination
- B. Disciplinary sanctions and appeals are handled in accordance with applicable UCHC procedures, depending on the type of workforce member being disciplined.

4. Duty to Mitigate Valid Breaches:

- A. UCHC maintains this policy for mitigating to a practical extent, any harmful or injurious effect of unauthorized uses or disclosures of all forms of protected health information (paper, electronic, or oral). To this end, oversight, detection, and reporting mechanisms have been established to know when violations occur. Additionally, processes are in place to limit the damage incurred.
- B. UCHC also has a duty to take reasonable corrective steps when notified of breaches of contract terms by business associates. While UCHC is not required to monitor the activity of

our business associates, we will address problems as we become aware of them and request that our associates remedy their behavior. UCHC reserves the right to terminate contracts if it becomes clear that the business partner cannot be relied upon to maintain the privacy of information we provide to them.

- C. Health Center officials shall be prepared to contact law enforcement, regulatory, accreditation, and licensure bodies as necessary in order to properly mitigate policy violations.

5. Documentation and Tracking of Breaches

- A. An analysis of reported privacy and/or security breaches is prepared by the Privacy Officer and/or ISO at least twice per year and reported to the Board of Directors.
- B. All information documenting the process noted in this policy regarding the incident or violation will be retained for a period of six years.

Reference: § 164.530 (e) Health Insurance Portability and Accountability Act of 1996
45 C.F.R. § 164.308 (a & c)
UCHC Confidentiality Policy
UCHC Information Security Policy

Jonathan Carroll (signed)	2/16/05
_____	_____
Information Security Officer	Date
Iris Mauriello (signed)	2/10/05
_____	_____
Privacy Officer	Date
Peter Deckers, MD (signed)	2/23/05
_____	_____
Executive Vice President for Health Affairs	Date

Replaces: Policy 12/13/04