UCONN HEALTH

POLICY NUMBER 2003-09

July 8, 2014

POLICY: BREACHES OF PRIVACY & SECURITY OF PROTECTED HEALTH INFORMATION (PHI) AND CONFIDENTIAL DATA

PURPOSE: UConn Health policies regarding the privacy and security of Protected Health Information (PHI) as well as other confidential data reflect its commitment to protecting the data as defined in UConn Health Policy 2003-31 Data Classification and Use Policy. While all types of confidential data are covered in this policy, the federal HIPAA and HITECH Rules specifically require procedures for management of breaches of patient information. This policy is intended to address those requirements.

While a commitment to privacy and security of patients' medical records, patient accounts, and clinical information from management information systems, confidential conversations, and any other sensitive material as a result of doing business is an expectation, there remains a possibility that an inappropriate or unintended disclosure of information may result in a privacy breach. This policy describes the procedure to mitigate all breaches, both willful violations and unintended actions, and is also consistent with guidance described by the HIPAA and HITECH Rules.

SCOPE: This policy applies to all members of the UConn Health workforce, UConn Health Business Associates as defined by HIPAA, all UConn Health Contractors/Vendors, and UConn Health sponsored business affiliates subject to remote access agreements.

POLICY STATEMENT:

1. Confidential data must be treated with respect and care by any individual with access to this information. Under HIPAA, as a medical/dental health care provider, UConn Health is entrusted with demographic, financial and clinical information regarding our patients. Any violation or breach of confidential data, including PHI, by workforce members is subject to formal discipline up to and including termination. Policy guidelines shall be observed by the entire organization, and sanctions applied fairly and consistently to all individuals in violation of the policies.

2. This policy covers the following:
    A) Definition of breach
    B) Required reporting process for breaches
    C) Investigation process followed
    D) UConn Health 's duty to mitigate damages created by breaches
    E) Documentation requirements of these processes

A. **<u>Breach Defined:</u>** A **"Breach" is defined by HIPAA as** the unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule, which compromises the security or privacy of that information. This standard is considered when addressing breaches of other types of confidential data in UConn Health's possession.

There are three exceptions to the definition of "breach" under HIPAA.

- Unintentional acquisition or use in good faith within the course and scope of employment by someone authorized to access PHI and the information is not further used or disclosed in a way that is inconsistent with the requirements of the HIPAA Privacy rule, or
- Inadvertent disclosure by an authorized person to another authorized person within UConn Health or our Business Associate, or sponsored business affiliate and the information is not further used or disclosed in a way that is inconsistent with the requirements of the HIPAA Privacy rule, or
- A disclosure of PHI where a UConn Health, our Business Associate or sponsored business affiliate, has a good faith belief that an unauthorized person who receives the information would not reasonably have been able to retain such information.

Examples of a Breach (this is not an all inclusive list):

- Authorized user accesses a patient's information or other confidential data without a functional "need to know"
- Release of patient information or other confidential data to an outside party for any unauthorized purpose – examples may include releases to the media, to relatives or friends of a patient, or sale of PHI
- Electronic hacking or theft of patient file or database or other confidential data
- "Dumpster diving" and finds confidential data
- Unauthorized user using another authorized person's ID/password to access patient information or other confidential data
- Unauthorized access to PHI or other confidential data, paper or electronic, that is neither protected by encryption nor properly destroyed.

Under the Department of Health and Human Services Final Breach Rule an acquisition, access, use or disclosure of protected health information in a manner not permitted by HIPAA's Privacy Rule is presumed to be a breach unless UConn Health demonstrates that there is a "low probability that the protected health information has been compromised."

B. Initial Reporting Responsibilities:

1. Anyone who is aware of or suspects a violation of privacy/security policy or a breach of patient information or other confidential data is required to report it immediately to:
   - The Privacy Office or
   - The Information Security Office or
   - The confidential REPORTLINE at 1-888-685-2637

2. Once the initial report is made, others should be informed including:
   - Immediate supervisor
   - Department Head or Manager of the area in which the individual works
   - Assistant or Associate Dean or Dean of Appropriate School

3. Bad Faith Reports: Reporting a violation or 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.

C. Investigations of Reported Breaches:

1. All reported violations will be assessed by the Privacy and/or Information Security Offices and may be escalated to the attention of the Privacy /Security/ Breach Team.

2. When applicable, the Privacy /Security/ Breach Team will invoke the Data Privacy/Security Breach Protocol which outlines the necessary steps to take in the event that any confidential data is compromised.

    a. This Protocol includes assembling key UConn Health stakeholders to perform a full assessment of the compromise of the confidential data.
    b. If the confidential data in question is not indecipherable, unreadable, or unusable and falls into unauthorized hands, UConn Health will determine through a risk assessment whether or not there was a low probability that the confidential data had been compromised.
    c. Outcomes of the analysis are documented and acted upon accordingly, as outlined in the Data Privacy/Security Breach Protocol.

3. Information pertaining to investigations of breaches will only be shared with those who have a need to know. Confidentiality of all participants in the reported situation shall be maintained to the extent reasonably possible throughout any resulting investigation. 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 individuals involved, interviewing other individuals, obtaining specific facts surrounding the violation/breach and reviewing pertinent documentation.

D. Discipline for Violations of Sanctions and Appeals:

1. When a violation/breach is verified, existing UConn Health procedures for disciplinary action shall be utilized.

2. Disciplinary sanctions and appeals are handled in accordance with applicable UConn Health policy procedures, depending on the type of workforce member being disciplined.

E. Duty to Mitigate Valid Breaches:

1. UConn Health will mitigate to a practical extent, harmful or injurious effects of unauthorized access, use or disclosure of all forms of PHI (paper, electronic, or oral) or other confidential data. The Privacy and/or Information Security Offices or the Privacy/ Security/Breach Team make recommendations to the appropriate department manager/administrator for corrective action.

2. The manager of the area responsible for the breach is required to develop and implement a corrective action plan to address valid breaches.

F. Reporting and Tracking of Breaches:

1. UConn Health officials will contact state agencies, law enforcement, regulatory, accreditation, and licensure bodies as necessary in order to properly report and mitigate policy and or law violations.

2. A summary of reported privacy and/or security breaches is prepared by the Privacy Office and/or Security Office on a routine basis and reported to the Executive Compliance Committee.

3. All information documenting the process required under HIPAA Privacy and Security and HITECH law regarding the violation or breach will be retained for a period of six years by the Privacy and/or Security Offices.

4. Violations that meet the definition of a breach that compromises the security or privacy of a patient's PHI under the HITECH Act are reported as required to the Department of Health and Human Services Office of Civil Rights.

Reference(s):

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) at 45 C.F.R.
- § 164.308; § 164.530
- The HITECH Act as amended in § 164.402 (2) (i)-(iv)
- Confidentiality Policy 2002-43
- UConn Health Information Security Policies
- Sanctions Policy for Privacy and Security Violations for Faculty and Staff 2014-04
- Connecticut General Statutes § 36a-701b

Jonathan Carroll (Signed) 7/18/14

Jonathan Carroll **Date**
Interim Chief Information Officer

Iris Mauriello (Signed) 7/16/14

Iris Mauriello **Date**
Compliance Integrity/Privacy Officer

Frank Torti (Signed) 8/12/14

Frank M. Torti, M.D., M.P.H. **Date**
Executive Vice President for Health Affairs

Revised & Renamed: 1/28/05. Original policy name was "Sanctions for Breaches of Privacy & Security of PHI & UCHC's Duty to Mitigate Such Breaches" which was a new policy on 1/14/03
Revised: 4/16/10, 9/23/13, 7/8/14