Policy 2003-09: Procedures for Responding to Breaches of Privacy or Security of Protected Health Information (PHI) and/or Personal Information

I. Breaches of PHI – General Information

An impermissible acquisition, access, use, or disclosure of PHI is presumed to be a Breach of Unsecured PHI (Breach) under HIPAA unless (i) UConn Health demonstrates through a risk assessment that there is a low probability that the PHI has been compromised, **or** (ii) the acquisition, access, use, or disclosure of PHI meets a specific exception under HIPAA to the definition of "Breach".

The following are examples of potential Breaches. This is not an exhaustive list.

- Intentional access of PHI by an authorized user without a work-related reason (i.e., snooping)
- Release of PHI to an unauthorized recipient
- A hacking or data security incident (e.g., phishing)
- Theft or loss of PHI
- Improper disposal of PHI
- Use of another individual's ID/password to access PHI
- Transmitting PHI using an unsecured method

II. Reporting

Workforce members must promptly report any suspected or known incident that raises concerns about the privacy or security of PHI and/or Personal Information to:

- The Office of Healthcare Compliance and Privacy (OHCP) (privacyoffice@uchc.edu or x7226);
- The UConn Health Information Security Officer (ISO); or
- The confidential REPORTLINE at 1-888-685-2637

Other individuals should be also be notified, as applicable, including the reporter's:

- Immediate supervisor;
- Department Head or Manager of the area in which the individual works; or
- Assistant Dean, Associate Dean and/or Dean of the appropriate School.

Suspected or known incidents that raise concerns about the privacy or security of Confidential Data *other than* PHI should be reported to the UConn Health Information Security Officer (ISO) or the confidential REPORTLINE.

III. Investigating

OHCP and/or the ISO, in consultation with the Office of the General Counsel (OGC) and/or other departments or external resources as appropriate, investigates known and suspected incidents involving the privacy or security of PHI and/or Personal Information. OHCP and the ISO will tailor the investigation to the scope and complexity of the incident. An investigation may include (among other things) interviewing relevant individuals, reviewing activities involving IT resources (including forensic review), examination and analysis of audit trails, and review and analysis of policies and procedures, laws and regulations and contractual obligations, as applicable.

Based on the results of the investigation, OHCP performs a risk assessment as outlined in HIPAA to determine whether the incident constitutes a Breach as defined. OHCP additionally analyzes the incident to determine whether it constitutes a Breach of Security under the Connecticut breach notification statute (Conn. Gen. Stat. § 36a-701b), or otherwise implicates any other state law reporting obligations based upon the laws of all states of residence for individuals affected by the Breach.

IV. Mitigating Harm

UConn Health will mitigate any harmful effects of a Breach to the extent practicable based on the particular facts and circumstances. Examples of mitigation efforts may include, but are not limited to:

- Retrieving, deleting, or destroying improperly disclosed PHI;
- Obtaining satisfactory assurances from an unauthorized recipient of PHI that the information will not be further used or disclosed;
- Terminating access or changing passwords;
- Modifying policies, procedures or practices;
- Modifying or enhancing physical and/or technical safeguards;
- Providing additional Workforce education or training; and/or
- Providing credit monitoring to impacted individuals.

V. Breach Notification

For incidents determined to constitute a Breach, OHCP will ensure that notification of the incident is provided to affected individual(s), the Secretary of the Department of Health and Human Services, the media, the Connecticut Office of the Attorney General, and other individuals, entities or regulatory bodies as required (including law enforcement and regulatory authorities in other states when required). Notification will be provided in the time and manner required by law, and may be provided by a Business Associate as specified in the accompanying

policy. UConn Health will delay notification when instructed to do so by law enforcement (i.e., to maintain the integrity of a criminal investigation or to protect national security).

Breach notification is not required when, in OHCP's determination, the risk assessment demonstrates a low probability of compromise or that an exception has been met. Breach notification also is not required when the PHI and/or Personal Information involved has been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of encryption or destruction.

For incidents that meet an exception or demonstrate a low probability of compromise, OHCP, in its discretion, may provide voluntary notification to impacted parties and/or regulatory bodies.

VI. Notice to Connecticut Office of the Attorney General and other State Notifications

When an incident is determined to be a "breach of security" under Conn. Gen. Stat. § 36a-701b as amended by Section 1 of Public Act No. 21-59 An Act Concerning Data Privacy Breaches (i.e., unauthorized access to or unauthorized acquisition of information in electronic form or format that contains a patient's first name or first initial and last name in combination with other elements in Conn. Gen. Stat. § 36a-701b(a)(2)(A) or (a)(2)(B), which includes user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account), UConn Health will notify the Connecticut Attorney General's Office as required and will comply with all other obligations set forth in Conn. Gen. Stat. § 36a-701b (e.g., provide identity theft protection services to individuals whose Social Security or taxpayer identification number is implicated). Notification requirements may be found here.

OHCP, in consultation with OGC, shall determine whether a Breach implicates any other state law reporting obligations, including notifications to state attorneys general or consumer protection agencies, and shall provide such notifications as required, in consideration of the laws of all states of residence for individuals affected by the Breach.

VII. Documentation

OHCP will maintain all documentation concerning breach analysis, and/or reporting for no less than six (6) years.