BREACH PREVENTION AND RESPONSE: REPORTING REQUIREMENTS, SANCTIONS & MITIGATION

Policy: It is the policy of the University of Connecticut to make all efforts to prevent data breaches of protected health information (PHI), and to properly report and respond to breaches when the occur.

Rationale: The University's policies regarding the privacy and security of PHI reflect its commitment to protecting the confidentiality of Individual health records, account information, clinical information from management information systems, confidential conversations, and any other sensitive material as a result of doing business in our HIPAA-Covered Components and beyond. While a commitment to privacy and security of PHI is an expectation, there remains a possibility that an inappropriate or unintended disclosure of PHI may result in a data breach. This policy will determine the procedure to mitigate all breaches, both willful violations and unintended actions, consistent with guidance described by the HIPAA and HITECH rules.

POLICY STATEMENT:

1. PHI is confidential and must be treated with respect and care by any person with access to this information. Any violation or breach of confidentiality by members of the University's HIPAA-Covered Components 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 persons 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) Disciplinary sanctions and appeals
    E) The University's duty to mitigate damages created by breaches
    F) Documentation requirements of these processes
    G) Other Examples

A. Breach Defined

A **"Breach"** means 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

BREACH PREVENTION AND RESPONSE: REPORTING REQUIREMENTS, SANCTIONS & MITIGATION

"Access" means the ability to read, write, modify or communicate data in any form or otherwise use any system resource

"Breach" does not mean:

- 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 or Security Rule, or

- Inadvertent disclosure by an authorized person to another authorized person within the same Covered Entity or Business Associate and the information is not further used or disclosed in a way that is inconsistent with the requirements of the HIPAA Privacy or Security Rule, or

- A disclosure of PHI where a Covered Entity or Business Associate 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 without a functional "need to know"
    - Release of patient information 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
    - "Dumpster diving" and finds PHI
    - Unauthorized user using another authorized person's ID/password to access patient information
    - Unauthorized access to PHI, paper or electronic, that is neither protected by encryption nor properly destroyed.

Other examples of violations of privacy and security of PHI are included at the end of this Policy. It is important to note that some violations may rise to the level of breach as defined by the HITECH Law.

B. Initial Reporting Responsibilities:

1. Anyone who is aware of or suspects a violation of privacy/security policy or a breach of patient/client information is required to report it immediately to:

    - The HIPAA-Covered Component Director

- Department Head or Manager of the area in which the individual works
- Assistant or Associate Dean or Dean of Appropriate School

Reports of suspected breaches and/or security incidents may also be made to:

- The University's Privacy Officer, or
- The University's Chief Information Security Officer (CISO), or
- The confidential REPORTLINE at 1-888-685-2637

These individuals shall immediately perform an initial review utilizing the "Suspected Breach Analysis Form."

Supervisors/managers and/or the University Privacy Officer/CISO shall start from the presumption that the security incident and/or suspected breach that has been identified constitutes a reportable breach under the HIPAA/HITECH Act unless they are able to demonstrate and document that there is a low probability that the PHI has been compromised. The supervisors/managers and/or the University Privacy Officer/CISO shall conduct the following risk assessment by assessing for specific factors and document the result on the "Suspected Breach Analysis Form:"

i. To whom the information was impermissibly disclosed;
ii. Whether the information was actually accessed or viewed;
iii. The potential ability of the recipient to identify the subjects of the data; and
iv. Whether the recipient took appropriate mitigating action.

Once the initial review by the above supervisor/manager has been completed and documented, the supervisor/manager shall immediately submit the completed "Suspected Breach Analysis Form" to the University's Privacy Officer. The University's Privacy Officer shall maintain copies of the "Suspected Breach Analysis Forms" for a minimum of six (6) years from the date of the form.

2. **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, suspected breach violations and security incidents will be assessed by the University's Privacy Officer and/or CISO and may be escalated to the attention of the University's Security Breach Team where appropriate.

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

    a. This Protocol includes assembling key University stakeholders and is also used to review the contents of completed "Suspected Breach Analysis Forms," the investigation into the matter completed by the University Privacy Office, CISO and/or relevant staff, and the risk assessment completed as part of that review and as identified under the HIPAA/HITECH regulations, as amended.

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 University's Privacy Officer, CISO and relevant staff 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. Disciplinary Sanctions and Appeals:

1. When a violation/breach is verified, existing University procedures for disciplinary action shall be utilized; For example:

    a. If the individual responsible for the violation/breach belongs to a collective bargaining union, the Office of Faculty & Staff Labor Relations (OFSLR) and union representation will be involved.

    b. If the individual responsible for the violation/breach is a faculty member or non-faculty professional, the process followed will be as outlined under applicable by-laws.

2. Sanctions may include, but are not limited to:

    - Counseling
    - Oral Warning

- Written Warning
- Suspension
- Termination

3. Disciplinary sanctions and appeals are handled in accordance with applicable University procedures, depending on the type of workforce member being disciplined.

4. If the individual responsible for the violation/breach is a Business Associate, the University will take reasonable corrective steps in accordance with the Business Associate Agreement signed between the University and the Business Associate. The University reserves the right to terminate contracts if it becomes clear that the business partner cannot be relied upon to maintain the privacy/security of information we provide to them.

E. Duty to Mitigate:

1. The University maintains this policy for mitigating to a practical extent, harmful or injurious effects of unauthorized access, use or disclosure of all forms of protected health information (paper, electronic, or oral). The Security Breach Team makes a recommendation to the appropriate department head for corrective action.

2. The University Privacy Officer, CISO and/or Security Breach Team shall be prepared to contact law enforcement, regulatory, accreditation, and licensure bodies as necessary, appropriate and/or required by law in order to properly report and mitigate policy and or law violations.

F. Notification of Breach

Where the risk analysis leads the University to the determination that a reportable breach has occurred, the University will follow appropriate and applicable notification standards.

1. Notification to Individuals

a. Where appropriate and/or required, the University shall notify each Individual whose unsecured PHI has been, or is reasonably believed by the University to have been accessed, acquired, used, or disclosed as a result of a breach. The University will provide the required notification without unreasonable delay and in accordance with timelines required by law.

b. The required notification shall be written in plain language and shall include, to the extent possible and/or permitted by law:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(2) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(3) Steps Individuals should take to protect themselves from potential harm resulting from the breach;

(4) A brief description of what the University has done/is doing to investigate the breach, to mitigate harm to Individuals, and to protect against any further breaches; and

(5) Contact procedures for Individuals to ask questions or learn additional information.

c. The required notification to Individuals shall be provided in the following form:

(1) Written notification by first-class mail to the Individual at the last known address of the Individual or, if the Individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(2) If the University knows the Individual is deceased and has the address of the next of kin or authorized representative of the Individual, written notification by first-class mail to either the next of kin or authorized representative of the Individual. The notification may be provided in one or more mailings as information is available.

(3) In the case in which there is insufficient or out-of-date contact information that precludes written notification to the Individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or authorized representative of the Individual. Substitute notice must consist of all of the following:

(i) E-mail notice, if the person has e-mail addresses for the Individuals to be notified;

(ii) Conspicuous posting of the notice on the University and/or HIPAA-Covered Component's website home page;

(iii) Notification to major print or broadcast media in geographic areas where the Individuals affected by the breach likely reside; and

(iv) Include a toll-free phone number that remains active for at least 90 days where an Individual can learn whether the Individual's unsecured PHI may be included in the breach.

(4) In any case deemed by the University to require urgency because of possible imminent misuse of unsecured PHI, the University may provide information to Individuals by telephone or other means, as appropriate, in addition to the other forms of notice.

2. Notification to the Media

For a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, the University will notify prominent media outlets serving the State or jurisdiction within the timeline required by law. The required notification shall be written in plain language and shall include, to the extent possible:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(2) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(3) Steps individuals should take to protect themselves from potential harm resulting from the breach;

(4) A brief description of what the University is doing to investigate the breach, to mitigate harm to Individuals, and to protect against any further breaches; and

(5) Contact procedures for Individuals to ask questions or learn additional information.

3. Notification to the Secretary of DHHS

A University will, in accordance with the breach notification requirement of the HIPAA/HITECH Act, notify the Secretary of the U.S. Department of Health and Human Services (DHHS) of breach.

For breaches of unsecured PHI involving 500 or more Individuals, the University shall provide notification to the Secretary contemporaneously with

the notice provided to Individuals and in the manner specified on the HHS Web site.

For breaches of unsecured PHI involving less than 500 Individuals, the University shall maintain a log and/or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification to the Secretary for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

4. Law Enforcement Delay

If a law enforcement official states informs the University that a required notification, notice, or posting would impede a criminal investigation or cause damage to national security, the University will:

(1) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(2) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (1) is submitted during that time.

5. Notification to Consumer Reporting Agencies

If the University discovers a breach of security of electronic PHI that requires notification to more than 1,000 persons at a single time, the University will also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. sec. 1681a(p). Notification shall include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

6. Notification to State Regulators

The University will also provide notice to appropriate state regulators where required by law.

G. Documentation and Tracking of Breaches:

1. Documentation regarding reported privacy and/or security breaches shall be maintained by the HIPAA-Covered Component, University Privacy Officer and

CISO, and provided to University Management and/or the Security Breach Team where appropriate.

2. "Suspected Breach Analysis Forms" shall be maintained by the University's Privacy Officer and the HIPAA-Covered Component for a minimum of six (6) years from the data of the form.

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 minimum of six (6) years by the University's Privacy Officer and/or the CISO.

4. Violations that meet the definition of breach under the HIPAA/HITECH Act as amended shall be reported as required to the Department of Health and Human Services Office of Civil Rights.

H. Other Examples of Privacy and Security Incidents:

Other examples of violations of privacy and security of PHI are included below. All privacy and security incidents should be evaluated thoroughly to determine whether a breach has occurred. (This is not an all-inclusive list.):

- Persons discussing PHI in any public area where those who have no need to know the information can overhear.
- Someone leaves paper copy of any Individual's health information in a public area.
- Unauthorized access to health records areas and health records.
- Someone leaves a computer unattended in a publically accessible area with health record information unsecured.
- Failure to log off computer terminal.
- For purposes unrelated to job duties:
    - Someone improperly acquires, accesses, uses, reviews and/or discloses records of any Individual or requests another person do so.
    - Someone acquires, accesses, reviews and/or discloses a patient/client's record for the intent of giving or selling information outside of the University.
    - Someone improperly acquires, accesses, uses, reviews and/or discloses confidential information of another member of the University workforce who is also an Individual receiving services from the HIPAA-Covered Component.
- Stealing or sharing passwords or not reporting a known lost password.

BREACH PREVENTION AND RESPONSE: REPORTING REQUIREMENTS, SANCTIONS & MITIGATION

- Introduction of viruses, worms, Trojan horses, or other malicious software into the organization's computer systems.
- Unauthorized access to networks, computer systems, or facilities/equipment rooms housing the computer systems.
- Unauthorized destruction/changing of ePHI.
- Improperly discarding PHI (not physically destroying it) whether paper or electronic media.
- Loss or theft of any Mobile Computing Device with PHI that is discoverable and not properly protected/encrypted.