3364-90-15 Reporting of security breach of protected health information including personal health information.

(A) Policy statement

The hybrid and affiliated covered entity is committed to ensuring the privacy and security of protected health information “PHI” and are aware of the inherent vulnerabilities that exist in the maintenance of such information. The university of Toledo “UT” recognizes the need for safeguards to protect PHI and the importance of notifying individuals when their unsecured PHI is subject to a breach.

(B) Purpose of policy

The purpose of this policy is to outline the processes and procedures to:

(1) Determine whether the security or privacy of PHI has been compromised.

(2) Ensure compliance with notification and reporting requirements.

A report of an unauthorized use, access, disclosure or acquisition of “unsecured" PHI which has occurred or which is reasonably believed to have occurred will be investigated, notifications provided and the incident(s) reported in compliance with federal and state laws. Please refer to rule 3364-90-01 of the Administrative Code (release of health information), for guidance for permissible uses and disclosure of PHI or contact the privacy office.

(C) Procedure

(1) Initial report of suspected breach

All unauthorized access/acquisition or impermissible use/disclosure, whether actual or suspected, must be reported to the privacy office or information technology “IT” security office. Any access, acquisition, use or disclosure which violates the health insurance portability and accountability act “HIPAA,” privacy and/or security rules, may constitute a breach and must be investigated. The privacy office, with the assistance of IT security, health science campus security and other relevant departments, will conduct an initial investigation into the reported

violation. Depending on the nature of the assessment, other employees of the university may be called upon to assist in the investigation. General counsel will perform a risk assessment based on information gathered from the investigation to determine the probability of compromise to PHI.

(2) Breach and risk assessment

(a) Generally, all unauthorized acquisition/access or impermissible use/disclosure must be presumed to be a breach unless the outcome of a risk assessment determines otherwise.

(b) Risk assessment. A risk assessment must determine the following:

(i) Whether there was an acquisition/access or impermissible use/disclosure of PHI.

(ii) Whether the reported acquisition/access or impermissible use/disclosure of PHI does not fall under any of the exceptions provided by law.

(iii) The probability that the PHI that has been compromised is low using the following factors:

(a) The nature and extent of PHI involved, including the types of identifiers and likelihood of re-identification.

(b) The unauthorized person who used or to whom the disclosure was made.

(c) Whether the protected information was actually viewed or acquired.

(d) The extent to which the risk to the PHI has been mitigated.

(e) Any other relevant factors.

(c) Exception to breach. Where the acquisition/access or use/disclosure of PHI falls under any of the categories below, there is no breach. Sufficient documentation must be maintained to support the categorization.

(i) Any unintentional acquisition, access, or use of identifiable health information by a workforce member or person acting under the authority of the hybrid and affiliated covered entity, if it was in good faith and within the scope of employment and the information is not further acquired, accessed, used or disclosed in a manner not permitted by law.

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at the hybrid and affiliated covered entity to another person authorized to access PHI at the same healthcare component or business associate or organized healthcare arrangement in which UT participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.

(iii) Where there is a good faith belief that the unauthorized recipient of the unsecured PHI would not reasonably have been able to retain such information.

(d) Outcome of risk assessment. If the outcome of a risk assessment determines that a breach has occurred, notification must be provided. If the outcome of a risk assessment determines that there is no breach, notification is not required, however, sufficient documentation must be maintained to support the basis for a finding of no breach.

(3) Notification

(a) Generally

(i) If the outcome of a risk assessment indicates that a

breach has occurred, notification must be provided. Notification must be provided to the individual and to the office of the secretary of the U.S. health and human services "HHS." Under certain circumstances, notification must also be given to the media.

(ii) Notification must be provided without unreasonable delay. In all cases, notification must be provided within the time frame specified by law. The time frame should be measured from the first day the act(s) constituting the breach was noticed or should have been noticed through exercise of reasonable diligence by a workforce member or agent of the university other than the one whose action(s) brought about the breach.

(iii) The time frame for notification should not be measured from the date a risk assessment determined that a breach had occurred except where a determination of breach was made on the same day the action(s) constituting the breach was noticed or should have been noticed as described in the preceding paragraph.

(iv) Risk management should be consulted to determine the need to notify the current cyber liability insurance carrier. The carrier can provide advice on notification issues. If the breach is covered within the terms of policy, notification and resolution services will be provided within the limits of the insurance coverage.

The privacy officer will notify appropriate administrative executives, including the chief compliance officer, after a conclusive determination that a breach event occurred.

(b) Notification to individuals

(i) Timelines – Each individual whose PHI has been breached or is reasonably believed to have been breached must be notified.

Notification of a breach shall be provided without unreasonable delay and in no case later than sixty calendar days from the date referenced in (C)(3)(a)(ii) of this rule except where a law enforcement agency or official has requested a delay.

(ii) Contents of notification – Notifications shall be written in plain language and include to the extent possible the following elements:

(a) A brief description of what happened, including the date of the breach and the date of the discovery of the breach (C)(3)(a)(ii) of this rule if known.

(b) A description of the types of PHI involved in the breach such as full name, social security number, date of birth, home address, account number, diagnosis, disability code and other types of information.

(c) Any steps the individual should take to protect themselves from potential harm.

(d) A brief description of what the university of Toledo medical center "UTMC" is doing to investigate the breach, mitigate harm and protect against further breaches.

(e) Contact information for individuals to ask questions and learn additional information. The contact information shall include: a toll free telephone number, an e-mail address, web site or postal address.

(iii) Method of notification – Notification must be in writing and delivered by first class mail to the individual's last known address. Where the

individual is known to be deceased, the notification must be sent to the address of the next of kin or legally recognized personal representative. If the individual has agreed to receive electronic notice and has not withdrawn such agreement, notification by electronic mail is appropriate. Notification may be provided in one or more mailings as information becomes available.

(iv) Substitute notice – In a situation where there is insufficient or out-of-date contact information that precludes written notification, a substitute notification must be provided. Substitute notification must be reasonably calculated to reach the individual. Substitute notice is not required in a case where there is insufficient or out-of-date contact information for the next of kin or legally recognized representative of the individual. The means of substitute notification given will depend on the number of individuals who cannot be contacted through first class mail.

(a) If ten or more individuals are unable to be contacted due to insufficient contact information or out-of-date contact information then substitute notice will be in the form of a conspicuous posting on the home page of the web site of UT for a period of ninety days or a conspicuous notice in a major print or broadcast media in geographic areas where the individuals likely affected by the breach reside. The posting must contain a toll-free number which will remain active for at least ninety days where an individual can learn whether his/her PHI is included in the breach.

(b) If less than ten individuals are unable to be contacted due to insufficient or out-of-date contact information then such substitute notice will be provided by an alternative

form of written notice, telephone, or other means.

(c) Urgent notice

If the university deems the situation to be urgent, the individuals may be notified by telephone or other means, as appropriate, in addition to providing written notice.

(d) Notification to the media

If a breach of PHI affects more than five hundred individuals residing in a particular state, the university shall notify prominent media outlets serving the area. The university shall provide notification without unreasonable delay and no later than sixty calendar days after discovery as described in section (3)(a)(ii) of this rule unless a law enforcement delay is requested. The notification shall follow the same format that is set forth in section (C)(3)(b)(ii) of this rule. Notification of media outlets will be provided in addition to individual notification requirements and should not be regarded as a substitute for individual notification.

(e) Notification to secretary of health and human services

The secretary of HHS must be notified of all breaches of PHI. Notification must be provided without unreasonable delay except at the request of a law enforcement officer and will be provided as follows:

(i) If the breach affects five hundred or more individuals, notification must be provided contemporaneously with notification of the individuals affected as set forth in section (C)(3)(a)(ii) of this rule. Notification must be submitted online using the hhs website* (accessible at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html) and following the instructions.

(ii) If the breach affects less than five hundred individuals, UT will report such occurrences to the secretary of HHS at

approximately the same time the individual is notified. UT will maintain sufficient documentation of the occurrence and ensure that the secretary is notified of all breaches which occur in a given calendar year within sixty days of the start of a new calendar year. The report will be submitted online using the hhs website* and following the instructions.

(f) Notification by a business associate

A business associate "BA" must notify the university following the discovery of a breach of unsecured PHI. Discovery of a breach by a BA follows the guideline outlined in (C)(3)(a)(ii) of this rule. The BA must notify the university within sixty calendar days after the date of discovery except where law enforcement delay is requested. The BA shall provide the university with available information that is required to include in the notification to the individual(s) affected by the breach. The notification of the individuals follows the same procedures as outlined within this policy (e.g., law enforcement delay).

(g) The university will delay a notification, notice or posting of a breach of PHI at the request of a law enforcement official where not doing so will impede a criminal investigation or cause damage to national security.

(i) If a request is made in writing and specifies the time period for which delay is required, the university will delay the notification, notice or posting by the specified time period requested in the writing.

(ii) If the statement is made orally, the university will document the statement, including the identity of the official making the request. The notification, notice, or posting will be delayed temporarily for a period no longer than thirty days from the date of the oral request, unless a written request is submitted during that time.

(4) Training

The university shall train all employees whose functions are affected by this policy on the requirements of the notification of an unsecured breach.

(5) Complaints

Complaints regarding breaches of unsecured PHI and failure to follow this policy and procedures shall be addressed to the privacy officer and shall be handled in the same manner as any other privacy-related complaint as set forth in university policy.

(6) Reporting

See rule 3364-15-05 of the Administrative Code (protected disclosures and anonymous reporting line) for information regarding the anonymous reporting line.

(7) Sanctions

Employees and other members of the university workforce who fail to comply with these policies and procedures will be disciplined in the same manner as set forth in applicable university policies.

(8) Non-retaliation/waiver

The university shall not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual who exercised his or her rights under these policies and procedures. The university shall not require any individual to waive his or her rights under this policy as a condition to receiving treatment, payment, enrollment in a plan, or benefits. See rule 3364-15-04 of the Administrative Code (non-retaliation policy).

(9) Revision

This policy shall be revised as necessary to comply with the law or reviewed every three years as required by UT policy.

(10) Definitions

(a) “Access” and “acquisition” are synonymous with the regulatory definitions of “use” and "disclosure" set forth in the privacy rule.

(b) Breach – the acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted by the HIPAA privacy and/or security rules that compromises the security or privacy of the protected health information.

(c) Destroyed – PHI in paper form that has been shredded or otherwise destroyed such that the PHI cannot be read or otherwise be reconstructed; and if in electronic form, it has been cleared, purged or destroyed consistent with the standards set forth by national institute of standards and technology “NIST.”

(d) Encrypted – PHI, through the use of an algorithmic process, has been transformed into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such process or key has not been breached.

(e) Law enforcement official – An officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe who is empowered by law to:

(i) Investigate or conduct an official inquiry into a potential violation of law, or

(ii) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

(f) Protected health information – Information including demographic and genetic information relating to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual

or the past, present or future payment for the provision of healthcare to an individual and is:

(i) Created or received by a healthcare provider, health plan, employer, or health care clearinghouse.

(ii) Transmitted or maintained in electronic or any other form.

(iii) Used to identify the individual or where there is a reasonable basis to believe that it can be used to identify the individual.

(iv) Except:

(a) Employment records held by a covered entity under HIPAA acting in a capacity as an employer.

(b) Where the information concerns an individual who is known to be deceased for more than fifty years.

(c) The information is contained in education records covered by the family educational rights and privacy act "FERPA."

(g) Unsecured – Information that is rendered usable, readable or decipherable to unauthorized persons through encryption or destruction of the media containing the information as approved by the NIST guidelines.

(h) Workforce member – Employees, volunteers, trainees, and other persons whose conduct in the performance of work for the university or a business associate of the university is under the direct control of the university or a business associate of the university.

Effective: 7/9/2018

CERTIFIED ELECTRONICALLY

Certification

06/29/2018

Date

Promulgated Under:	111.15
Statutory Authority:	3364
Rule Amplifies:	3364