Name of Policy: Reporting of security breach of protected health information including personal health information Policy Number: 3364-90-15 Approving Officer: President Responsible Agent: Privacy Officer and Director of Health Information Management Scope: Hybrid and affiliated covered entity of University of Toledo	Effective date September 13, 2023 Original effective date: November 15, 2010
Keywords	

	New policy		Minor/technical revision of existing policy
	Major revision of existing policy	X	Reaffirmation of existing policy

(A) Policy statement

The hybrid and affiliated
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 compromi
2. Ensure compliance with notification and reporting requirements

A report of an unauthorized use, access, disclosure or acquisition of unsecu
which has occurred, or which is reasonably believed to have occurr
investigated, notifications provided, and the incident(s) reported in compliance
federal and state laws. Please refer to policy # 3364-90-01, Release of Health Infor
for guidance for permissible uses and disclosure of PHI or contact the privacy offi

(C) Procedure

(1) Initial

ii.

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) above 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) above 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 UMC 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

Notification must be submitted online using the HHS website and following the instructions.

(ii) If the breach affects less than five hundred individuals, the university will report such occurrences to the secretary of health and human services at approximately the same time the individual is notified. The university will maintain sufficient documentation of the occurrence and ensure that the s

(d) Encrypted PHI. PHI that 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)]01 8 -0

Approved by:

Gregory Postel, MD