Name of Policy: **Security and protection of patient information – both paper and electronic**

Policy Number: 3364-90-12

Approving Officer: President

Responsible Agent: Privacy Officer and Director of Health Information Management

Scope: Hybrid and affiliated covered entity of University of Toledo

THE UNIVERSITY OF TOLEDO 1872

Effective date:
September 13, 2023

Original effective date:
October 8, 2003

Keywords:

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

(A) Policy statement

All patient information, whether in paper or electronic format, will be protected from natural and environmental hazards or from unauthorized intrusion.

(B) Purpose of policy

To apply reasonable safeguards to ensure the confidentiality, integrity and availability of all protected health information (PHI) whether created, received, maintained or transmitted by the hybrid and affiliated covered entity of UToledo (hybrid and ACE of UToledo), and to protect against threats or hazards to the security of the information.

(C) Procedure

UToledo has implemented the following procedures as safeguards for the protection of PHI or student treatment records covered by family educational rights and privacy act (FERPA). This is not an all-inclusive list. Information security policies will provide more in- depth protections.

(1) Security of computer workstations

(a) Computers should not be left active and unattended at any workstation.
(b) Computer screens should not be visible to unauthorized persons. If screen is viewable, change the screen to one that does not display PHI or turn from the public.
(c) Passwords may not be shared.
(d) Persons accessing a computer system must have unique ID and password.

(2) Security of the hybrid and ACE of UToledo records

(a) Electronic records

1. PHI maintained on the computer will be accessed via a unique login ID and password to the computerized record application as stated in policy 3364-65-02, Information security and technology administrative safeguards.
2. Access to electronic PHI is permitted based on the role of the individual and follows the minimum necessary as per policy 3364-90-02, minimum necessary guidelines for use/disclosure of protected health information.
3. It is the department manager's responsibility to contact the system administrator when someone leaves, moves departments or changes responsibilities for provision and de-activation of their access into computer systems, including those containing PHI.
4. Electronic PHI on the network is backed up nightly and stored in a separate facility that is fireproof and secured.
5. Virus protection software is updated and distributed via the network. External alerts are protected by user ID and password.
6. Physical access to the main data center and back up data center is controlled and monitored by the clinical information technology department.
7. Audit trails on various systems, including but not limited to, STAR, the clinical portal, horizon ambulatory care, Athena, EPIC etc. permit periodic monitoring of user access.
8. Encryption of electronic mail containing PHI.

(b) Paper records

1. PHI maintained on paper will be stored in a secured, climate controlled area.
2. Paper documents containing PHI must not be left in public view or left unattended in public areas.
3. Delivery and transportation of large numbers of paper records to the hybrid and ACE of UToledo are transported to secure storage following boxing and labeling.
4. When transporting medical records for treatment purposes a secure, locked case must be used and medical records may not be left unattended in the employee's vehicle.
5. In the event of a disaster, recovery of hard copy or microfilm records damaged by water/fire, HIM will contact a document restoration service whereby records would be freeze-dried within forty eight hours to prevent mold or further loss. Further restoration options will be investigated and initiated as deemed appropriate by the hybrid and ACE of UToledo.

Approved by: /s/ Gregory Postel, MD President **Date:** September 13, 2023 **Review/revision completed by:** • *Privacy and Security Committee* • *Senior Leadership Team*	**Policies superseded by this policy**: • *7-90-12 Security and protection of patient information – both paper and electronic* **Original effective date:** *October 8, 2003* **Review/revision date:** *February 9, 2005* *April 23, 2008* *November 15, 2010* *February 1, 2014* *September 1, 2016* *October 16, 2017* *October 6, 2020* *September 13, 2023* **Next review date:** *September 13, 2026*