3364-90-12 Security and protection of patient information – both paper and electronic.

(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 "ACE" of the university of Toledo (hybrid and ACE of the university of Toledo "UT"), and to protect against threats or hazards to the security of the information.

(C) Procedure

The university of Toledo 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 identification and password.

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

(a) Electronic records.

(i) PHI maintained on the computer will be accessed via a unique login identification and password to the computerized record application as stated in rule 3364-65-02 of the Administrative Code (access control).

(ii) Access to electronic PHI is permitted based on the role of the individual and follows the minimum necessary in this rule.

(iii) 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.

(iv) Electronic PHI on the network is backed up nightly and stored in a separate facility that is fireproof and secured.

(v) Virus protection software is updated and distributed via the network. External alerts are protected by user identification and password.

(vi) Physical access to the main data center and back up data center is controlled and monitored by information security policy.

(vii) Audit trails on various systems, including but not limited to: star, the clinical portal, mysis, hac, athena, etc. permit periodic monitoring of user access.

(viii) Encryption of electronic mail containing PHI.

(b) Paper records

(i) PHI maintained on paper will be stored in a secured, climate controlled area.

(ii) Paper documents containing PHI must not be left in public view or left unattended in public areas.

(iii) Delivery and transportation of large numbers of paper records to the hybrid and ACE of UT involves the use of the secured documentation telelift system or through hand carts or mobile locking carts which are not left unattended.

(iv) When transporting medical records for treatment purposes a secure, a locked case must be used and medical records may not be left unattended in the employee's vehicle.

(v) In the event of a disaster, recovery of hard copy or microfilm records damaged by water/fire, the HIM department 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 UT.

Effective: 7/9/2018

CERTIFIED ELECTRONICALLY

Certification

06/29/2018

Date

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