Name of Policy: Security and Protection of Patient Information – Both Paper and Electronic
Policy Number: 3364-100-90-12
Department: Hospital Administration
Approving Officer: Interim Executive Director and Associate Vice President
Chief of Staff
Responsible Agent: Privacy and Security Officer and Director of Health Information Management
Scope: The University of Toledo Medical Center and its other Health Care Components, Medical Staff

New policy proposal
X Major revision of existing policy
Minor/technical revision of existing policy
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 all of The University of Toledo Medical Center (“UTMC”) covered entities and to protect against threats or hazards to the security of the information.

(C) Procedure
UTMC implements the following procedures as safeguards for the protection of Protected Health Information or student treatment records covered by Family Educational Rights and Privacy Act (FERPA):

1. 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.
   c. Passwords may not be shared.
   d. Persons accessing a computer system must have unique ID and password.

2. Health Science Campus
   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 the Access Control policy 3364-65-02.
      2) Access to electronic PHI is permitted based on the role of the individual and follows the minimum necessary policy (#3364-100-90-02).
      3) It is the department managers’ 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 information security policy.
7) Audit trails on various systems, including but not limited to, STAR, the Clinical Portal, Mysis, HAC etc. permit periodic monitoring of user access.
8) Encrypt email 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 UTMC involves the use of the secured documentation telelift system or through hand carts or mobile locking carts which are not left unattended.
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 employees vehicle.
5) In the event of a disaster, recovery of hard copy or microfilm records damaged by water/fire, the Health Information Management Department will contact a document restoration service whereby records would be freeze dried within 48 hours to prevent mold or further loss. Further restoration options will be investigated and initiated as deemed appropriate by Hospital Administration.

3. All Other Health Care Components

a. Paper Records

1) Must store records in a secure area with controlled access.
2) Paper Documents with PHI must not be left in public view or left unattended in public areas.
3) Visitors must not be left unattended in areas where they may gain access to PHI.

All documents containing PHI will have a confidentiality statement attached as follows:

CONFIDENTIALITY OF PATIENT INFORMATION: This document contains confidential patient information, which must be protected at all times. Misuse or inappropriate disclosure, even though inadvertent is a serious violation of law and UTMC policy. Discard only in a secure manner according to Disposal of Confidential Information policy #3364-15-09.

For further information regarding administrative safeguard procedures and sanctions for violations of confidential patient information and security breaches, please see Policy 3364-100-90-12.