


Name of Policy: <u>Disposal of protected health information (PHI)</u>		 Effective date: August 1, 2008	
Policy Number: 3364-15-09			
Approving Officer: President			
Responsible Agent: Compliance/Privacy Officer			
Scope: All University of Toledo Campuses			
	New policy proposal	<input checked="" type="checkbox"/>	Minor/technical revision of existing policy
	Major revision of existing policy		Reaffirmation of existing policy

(A) Policy statement

It is the policy of The University of Toledo to ensure the privacy and security of protected health information in the maintenance, retention, and eventual destruction and disposal of such media. Destruction and disposal of protected health information will be carried out in accordance with federal and state law, and as defined in the university’s retention policy. The schedule for destruction and disposal shall be suspended for records involved in any open investigation, audit, or litigation.

(B) Purpose of policy

To establish guidelines to ensure that confidential information is destroyed and disposed in a manner consistent with the federal and state laws and ensure the confidentiality of protected health information (PHI).

(D) Procedure

This policy shall apply to health information that is generated during provisions of health care to patients in any of the university’s patient care units, patient care centers or faculty practices as well as human subjects research under the auspices of the university or by any of its agents in all university schools, units, departments and university owned or operated facilities.

The destruction and disposal of PHI will be carried out in accordance with Health Insurance Portability and Accountability Act (HIPAA) regulations and university policy. All PHI will be destroyed in a manner in which it cannot be recovered or reconstructed. Medical records will be maintained and destroyed in accordance with the university policy, records management, 100-70-50-40.

PHI must not be discarded in trash bins, unsecured recycle bags and other publicly-accessible location. Instead this information must be personally shredded or placed in a secure recycling bag.

Confidential information includes that which contains PHI of a patient, relative or household member of a patient. The following methods of destruction should be followed for the specific type of media;

- (1) Paper documents may be destroyed through shredding or pulverizing through the institution's contracted destruction company.
- (2) Confidential information on computerized media must be destroyed by reformatting, magnetization or actual physical destruction of the media as to prevent retrieval of data. Destruction of information on clinical or other health care related devices are to be coordinated with technology support services. All other items must be processed by information systems.
- (3) Disposal of radiology films containing PHI are destroyed by the contracted film recycler.
- (4) Disposal of labels containing PHI on material other than paper will be handled through the appropriate waste stream.
- (5) Contracts between the university and its business associates will provide that, upon termination of the contract the business associate will return or destroy and dispose of all consumer health information. The destruction of PHI by the business associate will be documented in writing and sent to the university.
 - (a) Date of destruction/disposal
 - (b) Method of destruction/disposal
 - (c) Description of the destroyed/disposed record series or medium
 - (d) A statement that the consumer information records were destroyed/disposed of in the normal course of business.
 - (e) The signatures of the individuals supervising and witnessing the destruction/disposal.

If such return or destruction or disposal is not feasible, the contract will limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.

(E) Definitions

Protected health information (PHI). Health information that identifies or can be used to identify an individual is considered protected health information under HIPAA. Any of the following information pertaining to a patient or the relatives, employees or household members of the patient can be used to identify a patient which include: name, street address, city, county, precinct, zip code, geocode, birth date, admission date, discharge date, date of death, age, telephone number, fax number, e-mail, social security number, medical records number, health plan number, account number, certificate/license number, vehicle identification number and license plate, device identifier, web location, Internet

Address, biometric identifier, photographs or any unique identifier.

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>July 8, 2008</u> Date</p> <p><i>Review/Revision Completed by: Compliance/Privacy Officer</i></p>	<p>Policies Superseded by This Policy:</p> <ul style="list-style-type: none">• <i>01-082 Disposal of protected health information (former Health Science Campus Policy review/revision date 7/1/03)</i> <p>Initial Effective Date: August 1, 2008 Review/Revision Date: Next review date: August 1, 2011</p>
--	--