


<p>Name of Policy: Transmission control policy.</p> <p>Policy Number: 3364-65-03</p> <p>Approving Officer: President</p> <p>Responsible Agent: Information Security Officer</p> <p>Scope: All campuses – all institutional members</p>	 <p>Effective Date: October 11, 2007</p>
<p>X New policy proposal</p> <p> Major revision of existing policy</p>	<p>Minor/technical revision of existing policy</p> <p>Reaffirmation of existing policy</p>

(A) Purpose of policy

To implement reasonable measures in protecting the university network against unauthorized communications, modifications or abuse.

(B) Policy statement

To provide the necessary direction for transmission of sensitive and confidential information externally and internally to the university personnel.

- (1) External transmission of sensitive or confidential information, including but not limited to PHI or student information, which may traverse non-university computer networks:
 - (a) Will only include the minimum information necessary to satisfy institutional objectives;
 - (b) Must be secured by encryption, passwords, or other technology which prevents unauthorized viewing, sharing, or modification during transmission. Clear text or unsecured information transmission is prohibited;
 - (c) Requires a valid attempt to verify recipient addresses prior to transmitting information to prevent wrongfully addressed communications;
 - (d) Transfer of PHI with external entities is prohibited without prior authorization through contracts or business agreements.

- (2) Internal transmission of sensitive or confidential information, including but not limited to PHI or student information, which traverses university-owned computer networks is authorized, however:
 - (a) It will only include the minimum information necessary to satisfy institutional objectives;
 - (b) Requires a valid attempt to verify recipient addresses prior to transmitting information to prevent wrongfully addressed communications.

- (3) Institutional members are prohibited from installing or operating network equipment, whether physical, logical, or virtual, that specifically performs network service functions on the university network without first acquiring information technology approval, including but not limited to:
 - (a) Hubs, switches, routers, firewalls, or wireless access points;
 - (b) Network address distribution or resolution;
 - (c) Intrusion detection, packet sniffers, network analyzers, protocol analyzers.

(C) Procedure

(1) Delegation of responsibilities

- (a) Information technology has the authorization to ban, block, disconnect, disable, prevent or remove equipment or terminate connections when any of the following occurs:
 - (i) Law enforcement requests such action or illegal activities are suspected;
 - (ii) Unauthorized copyrighted or inappropriate material is being accessed or distributed;
 - (iii) Institutional members are circumventing safeguards, abusing network access, creating suspicious activities, including spoofing or masking identities, causing major interruptions in network services, or using excessive network resources;
 - (iv) Rogue equipment is detected or suspected of distributing network access or services, or interrupting the service of the network;
 - (v) Any external force creates a detrimental condition on university operations, either intentionally or unexpectedly;
 - (vi) Commercial activities not sponsored by the university are being hosted on the university network.
- (b) Applications which do not support the university's missions or objectives will be disabled or blocked at appropriate network locations. Information technology will use a risk management approach to determine which applications may cause a risk to the university's infrastructure or will allow for secure transfer of information.
- (c) Packets that traverse any university network segment may or may not be actively monitored or reviewed by information technology, but depending on severity, segments or the entire network may be analyzed or monitored periodically to enforce this policy. Only information technology is authorized to perform this activity.

(2) Enforcement

The failure of any institutional member to perform any obligation required of this policy or applicable local, state and federal laws or regulations will be subject to established university disciplinary actions.

(3) Exceptions

- (a) Requests for exceptions to this policy must be submitted to information technology security and compliance.
- (i) Each request for exception will be handled on a case-by-case basis;
 - (ii) Each exception approval will be documented by information technology security and compliance.

(4) Definitions

- (a) Institutional Members: Anyone who participates in University activities, or has an affiliation with The University of Toledo. Includes, but is not limited to general staff, managers, medical staff, contractors, vendors, students, alumni and others involved in treatment, payment, or other normal operations of the University, whether or not they are paid by the University.
- (b) PHI: Acronym for Protected Health Information, which is any information that can possibly be used to identify a patient.
- (c) Transmission: The dispatching of a signal, message, or other form of intelligence, by wire, radio, telegraphy, telephone, facsimile or other means.

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>January 10, 2008</u> Date</p> <p><i>Review/Revision Completed by: Vice President, Administration; HIPAA Leadership Committee; JCAHO IM Chapter Committee; IT Leadership; IT Administration</i></p>	<p>Policies superseded by this policy:</p> <p>None</p> <p>Initial effective date: 10/11/2007 Review/Revision Date: Next review date: 10/11/2010</p>
--	---