MARSHALL UNIVERSITY INFORMATION TECHNOLOGY COUNCIL

Policy ITP-30

Email and Computer Mediated Communication of PHI

General Information:

1.1 Scope: This policy applies to all workforce members of SOM/UP&S.

1.2 Authority: Marshall University Information Technology Council

1.3 Passage Date: 11/17/2003

1.4 Effective Date: 11/17/2003

1.5 Revision Date:

1.6 Controlling over: Marshall University

Policy Summary

This policy restricts the transmission of electronic protected health information (PHI) and allows for exceptions only in specifically defined and pre-approved circumstances when such transmission is necessary for payment or operations.

Purpose

This policy reflects the commitment of the Marshall University Joan C. Edwards School of Medicine and University Physicians & Surgeons (SOM/UP&S) to ensure that all workforce members exercise appropriate discretion when transmitting PHI through computer mediated means of communication such as electronic mail.

Policy

1. No SOM/UP&S workforce member shall transmit protected health information (PHI) through computer mediated communication.
2. Exceptions to the restrictions contained in this policy may be granted by the SOM/UP&S HIPAA Security Officer provided that:
    - They are granted only when necessary for payment or operations;
    - The computer mediated communication employs robust encryption methods, if possible; and
    - Documentation of these exceptions:
        - Includes the rational for this exception;
        - Specifies the parties covered by the exception, including school of medicine users and external entities;
        - Details the specific computer mediated communication permitted, including the level of encryption used, if any;
        - Is maintained by the SOM/UP&S Security Officer; and
        - Is provided to the HIPAA Security Committee for review.

- View currently approved exceptions.

Regulatory Categories
General Rules
Technical Safeguards

Regulatory Type
ADDRESSABLE implementation specification for transmission security standard.

Regulatory References

1. §164.306(a)(1) "Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits."
2. §164.306(a)(3) "Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part."
3. §164.312(e)(1) "Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

Definitions

Computer mediated communication (CMC)
Forms of communication made possible by the use of computers and incorporating text, embedded or attached files and/or graphic images, such as, but not limited to, electronic mail, World Wide Web pages, instant messaging, short-message service (SMS), text paging, and others.

Workforce
"Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity" (§160.103).

Related Policies
- Marshall University Information Technology Environment Acceptable Use Policy
- Marshall University Email Policy
- Marshall University Information Security Policy

Renewal / Review
This policy shall be reviewed annually to determine if it complies with current HIPAA Security regulations and is appropriate given current technology. In the event that significant related regulatory changes occur, the policy will be reviewed and updated as needed.

Adoption
Adopted by **SOM/UP&S Board of Directors** on **11/17/2003**.