

**THE TEXAS A&M UNIVERSITY SYSTEM
HEALTH SCIENCE CENTER INTERNAL POLICIES**

**16.99.99.Z0.28 Email Use and Disclosure of Protected Health
Information Internal Policy**

Approved January 26, 2011

1. GENERAL/OVERVIEW

This policy applies to TAMHSC health care providers, its participating physicians and clinicians, employees and business units who provide management, administrative, financial, legal, and operational support to or on behalf of the health care provider and has been designated as a member of the TAMHSC Health Care Component. This policy pertains to protected health information covered by the TAMHSC Health Care Component's Notice of Privacy Practices.

2. INTERNAL POLICY/RESPONSIBILITIES

TAMHSC health care providers are committed to safeguarding patient information in order to fulfill its mission to patients, and to operate in a manner that is consistent with applicable federal and State laws and regulations. This policy defines the guidelines and procedures that must be followed when transmitting or receiving e-mail¹ that contain a patient's protected health information.

3. PROCESS

TAMHSC encourages the business use of e-mail to increase productivity. The e-mail system and all messages generated by e-mail, including backup copies, are part of the business infrastructure of TAMHSC, and must comply with TAMHSC policies.

- 3.1 Patient information should be hand delivered or mailed whenever possible. However, emailing of patient information internally to authorized personnel within the TAMHSC Health Care Component is allowable to facilitate treatment, payment and health care operations, provided the guidelines outlined in this policy are adhered to.
- 3.2 Information transmitted must be limited to the minimum necessary to meet the requester's needs.
- 3.3 TAMHSC Health Care Provider personnel may e-mail PHI to other TAMHSC Health Care Component personnel only. These e-mails can only be sent from and to secure e-mail addresses within the TAMHSC Health Care Component network.

The TAMHSC Health Care Component defines a secure e-mail address established and approved by TAMHSC Office of Information Technology. E-mails of PHI cannot be sent unless the recipient address can be verified as being secure.

3.4 All persons who send PHI via email should be aware of the following points:

- 3.4.1 E-mails containing PHI must be treated with the same degree of privacy and confidentiality as the patient's medical/dental record.
- 3.4.2 Confirm that the receiver has a need to know the information and is authorized to receive it.
- 3.4.3 Send only the minimum necessary PHI to meet the intent of the request.
- 3.4.4 Double check all recipient names/addresses to verify the correct person(s) will receive the email. (Be particularly sensitive to persons with the same last names/similar addresses.)
- 3.4.5 In the event of a misdirected e-mail, the sender should direct the recipient to immediately delete the e-mail by: holding down the Shift key and clicking Delete on the closed message; this bypasses sending message to deleted items folder.

3.5 If an e-mail that contains PHI is received in error, the recipient should notify the sender and immediately delete the e-mail by hitting alt-delete.

3.6 All provisions of the TAMHSC Information Technology Computer Use and Security Policy must be observed with regard to:

- 3.6.1 Access;
- 3.6.2 Use;
- 3.6.3 Modification;
- 3.6.4 Creation;
- 3.6.5 Disclosure;
- 3.6.6 Storage;
- 3.6.7 Copying;
- 3.6.8 Transmission; and

3.3.9 Destruction of information in any way related to online patient communications or interactions.

4. VIOLATIONS

The Privacy Officer has general responsibility for implementation of this policy. Employees who violate this policy will be subject to disciplinary action up to and including termination of employment. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the Privacy Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, every effort will be made to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment.

OFFICE OF RESPONSIBILITY

Vice President of Finance and Administration

ⁱ HIPAA Code: 45 CFR 164.312