

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

**16.99.99.Z0.29 Preparation and Maintenance of Designated
Records Sets 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

Under federal health information privacy regulations, patients have the right to inspect, copy, and request amendment of protected health information in "designated record sets" maintained by the TAMHSC Health Care Component. A patient's designated record setⁱ means all records maintained by or for the TAMHSC Health Care Component that are medical records, billing records, or records that are used to make decisions about patients. The privacy rule states that covered entities are required to document "the designated record sets that are subject to access by individuals." This policy identifies which records are part of a designated record set maintained by or for the TAMHSC Health Care Component.

3. PROCESS

- 3.1** The Texas A&M Health Care Component shall maintain "designated record sets" and provide a patient the opportunity to inspect, copy, and request amendment of the data.
- 3.2** A "designated record set" may include records in a variety of formats. The designated record sets maintained by the TAMHSC Health Care Component include:
 - 3.2.1 Medical records maintained by the TAMHSC Health Care Component.
 - 3.2.2 Billing records maintained by the TAMHSC Health Care Component.
 - 3.2.3 Any other group of records maintained by the TAMHSC Health Care

Component to make decisions about individual patients:

3.2.3.1 handwritten notes;

3.2.3.2 x-rays;

3.2.3.3 print-outs or readings from equipment;

3.2.3.4 index or note cards;

3.2.3.5 typed letters or memos;

3.2.3.6 handwritten letters;

3.2.3.7 electronic database documents or spreadsheets;

3.2.3.8 electronic mail; and,

3.2.3.9 information on microfiche, diskette, or compact disc.

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: §164.512(i), §164.514(a)(b)