

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

16.99.99.Z0.27

Data Use Agreement 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/PROCESS

The TAMHSC Health Care Component must ensure that data is appropriately safeguarded in accordance with HIPAA Regulations whereas the Data¹ User performs certain activities (as hereinafter defined):

- 2.1 TAMHSC Health Care Component wishes to disclose a Limited Data Set (as hereinafter defined) to Data User for use by Data User in performance of the Activities Additional information, if necessary.
- 2.2 The TAMHSC Health Care Component wishes to ensure that Data User will appropriately safeguard the Limited Data Set in accordance with HIPAA and the HIPAA Regulations.
- 2.3 Data User agrees to protect the privacy of the Limited Data Set in accordance with the terms and conditions of this Agreement, HIPAA and the HIPAA Regulations.

3. PROCESS

All Data Use Agreements shall be coordinated and approved by TAMHSC Contract Administration in Accordance with A&M System Regulation 25.07.01 Contract Administration, Procedures & Delegations. In addition, any request that TAMHSC Health Care Components sign a Data Use Agreement should be directed to TAMHSC Privacy Officer.

- 3.1 All Data Use Agreement forms must be approved by TAMHSC Contracts Administration.

3.2 Consultation shall be provided by the TAMUS Office of General Counsel and the TAMHSC Privacy Officer as needed.

3.3 Users are responsible for:

- 3.3.1 Knowing the scope of data for which each is responsible;
- 3.3.2 Reviewing and complying with the security policies, procedures, and controls for Electronic Protected Health Information;
- 3.3.3 Using TAMHSC data processing resources for intended purposes;
- 3.3.4 Complying with all appropriate TAMHSC policies, procedures and standards;
- 3.3.5 Promptly reporting security violations or misuse of data;
- 3.3.6 Not providing access to TAMHSC information systems containing EPHI unless authorization has been granted;
- 3.3.7 Assisting with investigations; and
- 3.3.8 Maintaining confidentiality of all data processed or handled.

4. VIOLATIONS

The TAMHSC Privacy/Security 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 TAMHSC Privacy/Security 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 164.514(e)