

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

**16.99.99.Z0.12 Accounting of Disclosure of Protected Health
Information as required by Law 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

All Protected Health Information (PHI) of the TAMHSC Health Care Component, including any PHI maintained electronically, is confidential, and would not normally be used, disclosed, or released without the patient's written authorization. However, there are times when the TAMHSC Health Care Component is required by law¹ to report or provide PHI to state or federal agencies or authorities, or when it must respond to judicial or administrative requests for PHI. This Policy defines the agencies, authorities, and instances in which the TAMHSC Health Care Component will use, disclose, or release PHI without the patient's authorization in order to comply with its responsibilities under city, state, or federal law.

3. PROCESS

3.1 Responding to Law Enforcement Request.

3.1.1 The TAMHSC Health Care Component will provide PHI to a law enforcement official without first obtaining the patient's written authorization:

3.1.1.1 To assist in the identification or location of a suspect, fugitive, material witness, or missing person;

3.1.1.2 Regarding a patient who is or is suspected to be a victim of a crime;

3.1.1.3 To alert law enforcement of the death of the individual;

- 3.1.1.4 If the TAMHSC Health care Component believes the PHI requested constitutes evidence of criminal conduct that occurred on the premises of TAMHSC; and
- 3.1.1.5 In emergency situations, to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.
- 3.1.2 If the law enforcement official requests PHI via a court order, subpoena, warrant, summons, or other similar document, the TAMHSC Health Care Component will provide the requested PHI if:
 - 3.1.2.1 The PHI sought is relevant and material to the law enforcement inquiry;
 - 3.1.2.2 The request is specific and limited in scope to the extent reasonably practicable;
 - 3.1.2.3 De-identified PHI could not be used; and
 - 3.1.2.4 The court order, subpoena, warrant, summons, or other similar document complies with Texas law which in some cases requires patient authorization to release.
- 3.1.3 If a TAMHSC Health care Component employee is presented with a court order, subpoena, warrant, summons, or other similar document:
 - 1.3.3.1 The employee should immediately notify his/her department Administrator of the document; and
 - 1.3.3.2 The employee who received the initial document or the department Administrator should immediately contact the HIPAA Privacy Officer to discuss and evaluate the document and determine whether and how the disclosure will be made
- 3.1.4 PHI should be disclosed in response to a court order, subpoena, warrant, summons, or other similar document prior to discussing the document with the TAMHSC HIPPA Privacy Officer, System Internal Audit and the A&M System General Counsel's Office
- 3.1.5 The person providing PHI in response to a court order, subpoena, warrant, summons, or other similar document is responsible for documenting the name, title, and contact information of the individual to whom the PHI was provided, the agency name and address (if known), the date the PHI was provided, and a brief summary of the PHI provided (e.g.,

demographic information about the patient, copy of face sheet showing diagnosis, etc.) for each patient whose PHI is reported or released.

- 3.1.6 Documentation of releases and disclosures that are made in response to a court order, subpoena, warrant, summons, or other similar document may be maintained in each individual patient's file (for easy retrieval if the patient requests an Accounting of Disclosures) or on a log in the Department. If documentation is included in the patient's file, the entry will not be considered part of the patient's designated record set.

3.2 Responding to Inquiries from National Security, Intelligence, and Protective Services Officials.

- 3.2.1 The TAMHSC Health care Component will provide PHI to authorized federal officials for intelligence, counter-intelligence, and other national security activities without first obtaining the patient's written authorization.
- 3.2.2 The TAMHSC Health Care Component will also provide PHI to authorized federal officials so they may conduct special investigations and provide protection to the President, other authorized persons, and foreign heads of state without first obtaining the patient's written authorization.
- 3.2.3 The person providing PHI to authorized federal officials for national security and intelligence activities and protective services is responsible for documenting the name, title, and contact information of the individual to whom the PHI was provided, the agency name and address, the date the PHI was provided, and a brief summary of the PHI provided (e.g., demographic information about the patient, copy of face sheet showing diagnosis, etc.) for each patient whose PHI is reported or released.
- 3.2.4 Documentation of releases and disclosures that are made to authorized federal officials for national security and intelligence activities and protective services may be maintained in each individual patient's file (for easy retrieval if the patient requests an Accounting of Disclosures) or on a log in the Department. If documentation is included in the patient's file, the entry will not be considered part of the patient's designated record set.

3.3 Specially Protected Personal Health Information.

- 3.3.1 An employee who receives a request from a federal, state, local, national security, or law enforcement official for PHI that includes HIV/AIDS information, mental health information, or substance abuse and treatment records must immediately contact his/her supervisor and the HIPAA Privacy Officer.

- 3.3.2 Under no circumstances should PHI that includes HIV/AIDS information, mental health information, or substance abuse and treatment records be released to the requesting official unless the disclosure is approved by the TAMHSC HIPAA Privacy Officer.

3.4 Document Retention.

- 3.4.1 All documentation relating to requests for a patient's PHI will be maintained for a minimum of six (6) years.

3.5 Definitions

- 3.5.1 *Protected Health Information (PHI)* means information that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual and identifies or could reasonably be used to identify the individual.

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: §164.526(a)