

MAY 17 2012

UNIVERSITY OF HOUSTON SYSTEM
ADMINISTRATIVE MEMORANDUM

UCC Certified

SECTION: General Administration

NUMBER: 01.D.06

AREA: Legal Affairs

SUBJECT: Protection of Confidential Information

RECEIVED MAR 06 2012

1. PURPOSE AND SCOPE

It is the policy of the University of Houston System (the "System") to ensure that there are guidelines, safeguards, and controls in place to effectively manage and protect confidential information in accordance with applicable laws, regulations, and best practices.- Such confidential information includes, but is not limited to, social security numbers, educational records as defined by the [Family Educational Rights and Privacy Act](#) ("FERPA"), health care information as defined by the [Health Insurance Portability and Accountability Act](#) ("HIPAA") and other applicable law, and customer information as defined by the [Gramm-Leach-Bliley Act](#) ("GLB Act").

2. POLICY

~~2.2.1.~~ Each component institution shall appoint its own Privacy Coordinator who will be responsible for the component institution's compliance with the guidelines issued by the General Counsel as described in Sections 2.2 and 2.3. The Privacy Coordinator for each component institution will also provide training, in consultation with the General Counsel, as well as report to the General Counsel any known or suspected instances of non-compliance with the General Counsel's guidelines. At the end of each fiscal year, the Privacy Coordinator for each component institution will submit a report to the General Counsel detailing the training that has been provided to the component institution during the fiscal year, any instances of non-compliance during the fiscal year, and the actions taken in response to any instances of non-compliance. The General Counsel will serve as the Privacy Officer for the System.

2.2. The Privacy Officer's duties include the General Counsel will issuing of guidelines with regard to the use of social security numbers, educational records, health care information, customer information, and other confidential information, as well as appropriate steps to follow in the event of a suspected security incident/breach involving sensitive personal information as required by applicable law. These guidelines will be posted on the web site for the UHS Office of the General Counsel. [Link to <http://www.uh.edu/legal-affairs/general-counsel/resources-and-policies/index.php>] In addition to issuing guidelines, the General Counsel will provide legal advice as requested in relation to the applicable laws and regulations governing the protection of confidential information.

- 2.3. The guidelines will be issued by the ~~Privacy Officer~~General Counsel to help each component institution ensure that:
- a. The release, use, display, transmission, and retention of social security numbers are only allowed if permitted by law.
 - b. Information that is considered an educational record (as defined by FERPA) will only be disclosed to someone other than an “eligible student” or an “eligible parent” with the consent of the student or as otherwise authorized by law.
 - c. The use, receipt, or transmission of an individual’s health care information (as defined by HIPAA and other applicable law) is allowed only as permitted by law.
 - d. Customer information (as defined by the GLB Act), including financial information, which is collected or maintained, will be safeguarded as required by law.
 - e. Appropriate steps are taken by the component institutions consistent with applicable law in the event of a suspected security incident/breach involving sensitive personal information.
 - ef. The use and/or release of any other information determined by the ~~Privacy Officer~~General Counsel to be confidential is allowed only as required by and consistent with applicable law.
- 2.4. No person having access to confidential information shall disclose confidential information in any manner ~~except as established in~~contrary to applicable law and/or the guidelines issued by the ~~Privacy Officer~~General Counsel. Any such disclosure of confidential information, whether intentional or unintentional, could subject the person to disciplinary action, up to and including termination.
- 2.5. It is the responsibility of each component university of the System and its employees to adhere to the guidelines that are issued by the ~~Privacy Officer~~General Counsel.
- 2.6. The ~~Privacy Officer~~General Counsel will revise its guidelines whenever necessary to conform to changes in applicable law or regulations.

3. REVIEW AND RESPONSIBILITIES

Responsible Party: Vice Chancellor for Legal Affairs

Review: Every three years on or before November 30th

4. APPROVAL

Approved: Dona G. Hamilton
Vice Chancellor for Legal Affairs

John M. Rudley
~~Interim~~ Chancellor

Date: October 17, 2007

REVISION LOG

<u>Revision Number</u>	<u>Approval Date</u>	<u>Description of Changes</u>
<u>1</u>	<u>08/31/2007</u>	<u>Initial version</u>
<u>2</u>	<u>TBD</u>	<u>Applied revised SAM template and added new revision log. Replaced "Privacy Officer" with "General Counsel" throughout procedure to reflect current operating practices. Provided web links to FERPA, HIPPA and GLB Act in Section 1.0. Rewrote Section 2.1 to outline duties of the Privacy Coordinator. Added documentation to Section 2.2 on activities and web site for reporting a security incident/breach. Added Section 2.3.e on component university taking appropriate steps during a security incident. Documentation added to Section 2.4 on possible termination for disclosure of confidential information</u>