

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

29.01.03.Z1.05 Data Classification

Approved September 1, 2010

Supplements System Regulation 29.01.03

1. GENERAL

1.1 Introduction

Data classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All Texas A&M University System Health Science Center (HSC) data, whether electronic or printed, should be classified. The data owner, who is responsible for data classification, should consult with legal counsel on the classification of data as confidential, institution-sensitive, or public. Consistent use of data classification reinforces with users the expected level of protection of HSC data assets in accordance with HSC security policies.

1.2 Audience

The HSC Data Classification Policy applies equally to all individuals who use or handle any HSC information resource.

1.3 Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of the HSC are the property of the HSC.

1.4 Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the HSC are not private and may be accessed by HSC information system employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards

2. DATA CLASSIFICATION POLICY

Data shall be classified as follows:

- 2.1 Confidential: Sensitive data that must be protected from unauthorized disclosure or public release based on federal or state law, (e.g. the Texas Public Information Act) and other constitutional, statutory, judicial, and legal agreements.

Examples of “Confidential” data may include but are not limited to:

- Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: Copyrights, Patents and Trade Secrets
- Medical Records

- 2.2 Institution-Sensitive: Sensitive data that may be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection.

Examples of “Institution-Sensitive” data may include but are not limited to:

- HSC operational information
- HSC personnel records
- HSC information security procedures
- HSC research
- HSC internal communications

- 2.3 Public: Information intended or required for public release as described in the Texas Public Information Act.

3. DISCIPLINARY ACTIONS

Violations of this policy may result in disciplinary action which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY

Vice President for Information Technology and Chief Information Officer