

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

29.01.03.Z1.14 Privacy

April 20, 2011

Supplements System Policy 29.01.03

1. GENERAL

1.1 Introduction

Privacy policies are mechanisms used to establish the responsibilities and limits for the Texas A&M Health Science Center [HSC] system officials, administrators and users in assuring and providing privacy in HSC information resources and/or sources. The HSC has the right to examine electronic information on information resources which are under the control or custody of the HSC. The general right to privacy afforded under federal and state laws is extended to the electronic environment at Texas A&M Health Science Center, including its schools, programs, centers and departments. However, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.

1.2 Audience

The Texas A&M Health Science Center Privacy Policy applies equally to all individuals who use any HSC information resource.

1.3 Definitions

- **Information Resources (IR):** any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, and software that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

- **Confidential Information:** Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act, FERPA, HIPAA, and other constitutional, statutory, judicial, and legal agreements).
- **Office of Information Technology (OIT):** The name of the institution department responsible for computers, networking and data management.
- **Webserver:** A computer that delivers (*serves up*) web pages.
- **Web page:** A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).
- **World Wide Web (Web):** A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contain links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape Navigator, and Microsoft Internet Explorer.
- **Website:** A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.

2. PRIVACY POLICY

- 2.1 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 appropriate personnel only under specific procedures defined by each component of the HSC and in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards.
- 2.2 In the normal course of their duties, system administrators may examine user activities, files, electronic mail, backups, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware. Individuals who have special access to information because of their position have the absolute responsibility not to take advantage of that access and it shall be done only as minimally necessary and in accordance with federal and state privacy laws. Where resources permit, segregation of duties is to be used per industry standards for both IT and healthcare operations.
- 2.3 Files owned by individual users are to be considered as private to the degree noted herein, whether or not they are accessible by other users. The ability to read a file does not imply authorization to read the file exclusive of the procedures set for the in this policy. Under no circumstances may a user alter a file that does not belong to him or her without prior consent of the file's owners. The ability to alter a file does not imply consent to alter that file.
- 2.4 If access to information is desired without the consent and/or knowledge of the file owner

or if inappropriate use of TAMHSC information resources is suspected, files may be reviewed without the consent and/or knowledge of the file owner if that review is part of the HSC procedure – Complaint Procedures for Electronic Information.

- 2.5 A wide variety of third parties have entrusted their information to HSC for business purposes, and all workers at HSC must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.
- 2.6 If criminal activity is suspected or reported, the appropriate law enforcement agency must be notified. All further access to information on university information resources must be in accordance with directives from law enforcement agencies.
- 2.7 Information resource owners or custodians will provide access to information requested by auditors in the performance of their jobs. Notification to file owners will be as directed by the auditors.
- 2.8 Other than exceptions in 2.2, 2.3, 2.4, 2.5, 2.6, and 2.7, access to information by someone other than the file owner requires the owner's explicit, advance consent.
- 2.9 Users must report any weaknesses in HSC computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- 2.10 Users must not attempt to access any data or programs contained on HSC systems for which they do not have authorization or explicit consent.

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

Executive Director for Information Technology and Chief Information Officer