



THE UNIVERSITY OF TEXAS AT DALLAS

SECURITY OF ELECTRONIC HEALTH CARE INFORMATION

Section 2: Introduction With Glossary of Terms	Page: 1 of 5
Effective Date: March 21, 2005	

UTD respects the privacy and confidentiality of its patients' medical information and is committed to safeguarding this valuable information. Protection of patient's privacy is a core value of UTD.

This *Policy and Procedure Manual for the Security of Electronic Health Care Information* ("Manual") addresses policies and procedures for safeguarding health information in electronic form of UTD's patients, consistent with the requirements of the HIPAA Security Standards and any applicable state law. Members of UTD's workforce, including volunteers, trainees, and the medical staff shall be familiar with and comply with this Manual.

An overview of HIPAA and the Security Standards is included in the appendix (*see Appendix: A.1.1 of the Privacy Manual*).

Glossary of Terms

Administrative Simplification – The *Administrative Simplification* provisions are set forth in Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Administrative Simplification provisions give the U.S. Department of Health and Human Services the authority to establish standards and requirements for the electronic transfer of health care information, and for the privacy and security of PHI.

Business Associate – A *business associate* is a person or organization who performs a function or activity on behalf of a covered entity or who performs a specified service regardless of whether it involves performing a service on behalf of a covered entity. The specified services where disclosure of personally identifiable health information is considered routine include: legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, and financial services. When a covered entity discloses PHI to a business associate, a business associate agreement between the covered entity and the person or organization performing functions on behalf of the covered entity or specified services is required to protect the use and disclosure of PHI. (*See Section 3.11 of this Manual.*)

Director-on-call – *Director-on-call* means the manager directly responsible for the servers and software applications in which electronic health care information is stored or processed. The

Director-on-call will be on call in case of an emergency affecting UTD's health care operations-related information systems and will serve as the manager in charge of emergency access procedures and operations.

Disclosure – *Disclosure* means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. *See also Use.*

Electronic Protected Health Information - *Electronic protected health information* means the subset of protected health information (as defined below) that is transmitted by, or maintained in, electronic media.

End User or User – *End User* or *User* means either an UTD workforce member, contractor, volunteer or any person or entity granted access to UTD's health care operations-related information systems or workstations.

Facility – *Facility* means the physical premises and the interior and exterior of a building(s).

Facilities Manager – *Facilities Manager* means the UTD workforce member who oversees and manages the organizational, administrative, and support activities at a particular UTD location involved in health care operations.

Health Care Operations – *Health care operations* activities include, but are not limited to, any of the following activities to the extent these activities are related to the covered entity's functions as a health care provider: (i) conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (ii) reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (iii) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (iv) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the covered entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (v) business management and general administrative activities of the covered entity, including, but not limited to: (A) management activities relating to implementation of and compliance with the requirements of the covered entity's policies and procedures and the HIPAA Privacy Standards; (B) customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; (C) resolution of internal grievances; (D) the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that

following such activity will become a covered entity and due diligence related to such activity; and (E) consistent with the applicable requirements of 45 C.F.R. § 164.514 of the Privacy Manual (*see* Section 5.1 of the Privacy Manual (relating to de-identified information); *see* Section 5.2 of the Privacy Manual (relating to limited data sets); and *see* Section 9 of the Privacy Manual (relating to fundraising)), creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. (*See also* Appendix: A.6.2.1 of the Privacy Manual.)

Health Oversight Agency – A *health oversight agency* is an agency or a person or entity acting under a grant of authority from or contract with such public agency, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Human Resources – *Human Resources* means the department responsible for personnel management and recruitment.

Information System – *Information System* means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.

Management – *Management* means those persons within UTD who possess supervisory authority over other workforce members and the ability to hire and fire workforce members.

Manual – *Manual* refers to this *Policy and Procedure Manual for the Security of Health Care Information*.

Minimum Necessary Standard – The *minimum necessary standard* is a limitation placed on uses, disclosures, and requests for PHI. It applies when using or disclosing PHI or when requesting PHI from another covered entity. A covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary standard does not apply to certain disclosures or requests.

Mitigation – *Mitigation* is the reasonable action taken by a covered entity to lessen the damage of a known security incident or disclosure of PHI in violation of the covered entity's policies and procedures or the requirements of the Security Standards. (*See* Section 3.8 of this Manual.)

Payment Activities – *Payment activities* are the activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of plan benefits, as well as those activities undertaken by a covered provider to obtain or to provide reimbursement for the provision of health care. Such activities include, but are not limited to, determinations of eligibility or coverage, risk adjusting amounts due based on enrollee health status and demographic characteristics, billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing, review of health care services, utilization review activities, and disclosure to consumer reporting agencies of any of the following PHI: name and address; date of birth; Social Security number;

payment history; account number; and name and address of the health care provider and/or health plan. (*See also* Appendix: A.6.2.1 of the Privacy Manual.)

Privacy Manual – *UTD HIPAA Privacy Manual*.

Privacy Officer – *Privacy Officer* is as defined in the Privacy Manual.

Privacy Standards or Privacy Rule – *Privacy Standards or Privacy Rule* refer to the final rule “Standards for Privacy of Individually Identifiable Health Information,” which the Department of Health and Human Services published at 65 Fed. Reg. 82462 *et seq.* (Dec. 28, 2000), and modified at 67 Fed. Reg. 53182 *et seq.* (Aug. 14, 2002).

Protected Health Information (“PHI”) – *PHI or protected health information* is individually identifiable health information that is transmitted or maintained in any medium or form. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended; in records described at 20 U.S.C. § 1232g(a)(4)(B)(iv) (student treatment records excepted from FERPA); and in employment records held by a covered entity in its role as an employer.

Public Health Authority – *Public health authority* means an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with a public agency, including the employees or agents of the public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. A public health authority can create health information as well as receive it.

Sanctions – *Sanctions* are administrative actions by a covered entity taken against members of its workforce who fail to comply with the entity’s policies and procedures or with the requirements of the Security Standards. A covered entity must have and apply appropriate sanctions and must document the sanctions that are applied. (*See* Section 3.2 of this Manual.)

Security Officer – *Security Officer* is as defined in Section 3.3 of this Manual.

Security Rule – *Security Rule* refers to the final rule adopting standards for the security of electronic protected health information as required by the Administrative Simplification title of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). *See* 45 C.F.R. Parts 160, 162, and 164; 68 Fed. Reg. 8334 *et seq.* (Feb. 20, 2003).

System Administrator – *System Administrator* means the UTD workforce member(s) who oversee(s) all information technology and technical support activities related to information systems supporting health care operations. Activities performed by a System Administrator include monitoring security configuration, managing allocation of user names and passwords, monitoring disk space and other resource use, performing backups, and setting up new hardware and software.

Treatment – *Treatment* means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management

of health care by a health care provider with a third party, consultation between health care providers relating to a patient, or the referral of a patient for health care from one health care provider to another. (See also Appendix: A.6.2.1 of the Privacy Manual.)

Use – *Use* means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains the information.

Workstation – *Workstation* means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Date Approved: _____	Date Revised/Reviewed: _____
Approved By: _____	_____
Title: _____	_____
Signature: _____	_____