Policy#	Name
04.301	Acceptable Electronic Communications Use Policy
04.302	Server Management and Security Policy
04.304	Data Integrity and Classification Policy
04.305	Web Policy
04.306	Cellular Phone Use and Allowance Policy
04.307	PHI Electronic Communications
04.308	Transmission of Health Information via PDA
04.310	Records Management Program Policy
04.311	Records Retention Policy
04.312	Records Disposition
04.313	Records Authorization Policy
04.314	RM Exit Procedures for Employees Policy
04.315	Legal Hold Policy
04.316	Archives Program Policy

Policies of the University of North Texas Health Science Center	Chapter 04 – Administration
04.301 Acceptable Electronic Communications Use Policy	

Policy Statement.

The University of North Texas Health Science Center (UNTHSC) provides various electronic communication resources for the purpose of conducting business in support of UNTHSC's organizational mission. UNTHSC is the legal owner and operator of all electronic communication resources purchased or leased with UNTHSC funds. All electronic records are the property of UNTHSC, not of the individuals creating, maintaining, sending or receiving such data or information. Each person granted access to UNTHSC electronic communication resources and electronic records is responsible for appropriate use as stated within this policy as well as adherence to all applicable federal, state and local laws. UNTHSC reserves the right at any time to limit, restrict or deny access to its electronic communication resources and records, as well as to take disciplinary and/or legal action against anyone who is in violation of this policy or applicable laws.

Application of Policy.

This document establishes organizational policies and procedures regarding the use of electronic communications. This policy applies to:

(1) All electronic communication resources owned, leased, provided and/or managed by UNTHSC;

(2) All users and types of use of UNTHSC electronic communication resources;

(3) All electronic records generated or maintained in the transaction of UNTHSC business or stored within a UNTHSC electronic communication resource.

Definitions.

Electronic Communication Resources: Telecommunications equipment, electronic audio/video devices, encoding/decoding devices, computers, servers, data processing or storage systems, mobile communication devices, networks, input/output and connecting devices and related programs, software and documentation that support electronic communications. UNTHSC electronic communication resources include institutional and departmental information systems, faculty research systems, desktop computers, UNTHSC campus networks and general access computer systems.

Electronic Record: A record created, generated, sent, communicated, received, or stored by electronic means.

Users: All faculty, staff, students, contractors, volunteers and individuals that maintain a business relationship with UNTHSC that make use of UNTHSC electronic communication resources and/or electronic records.

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. **Authorized Usage**. UNTHSC electronic communication resources and records must primarily be used for business purposes. Personal use is permissible as long as it does not (a) generate a direct cost to UNTHSC, (b) interfere with the user's productivity (c) preempt any business activity and (d) violate the law or UNTHSC policy. Users are forbidden from using UNTHSC electronic communication resources for charitable endeavors not specifically sanctioned by UNTHSC, political or religious activities, commercial or private business activities, solicitations, advertisements, and for creating, storing or maintaining inappropriate content for amusement/entertainment purposes. The use of UNTHSC electronic communication resources should never create the appearance of inappropriate use. Disciplinary action, up to and including termination may result from unauthorized use.	Employees, faculty, contractors or volunteers
Students, shall be allowed to use UNTHSC computer resources for school-related and personal purposes, subject to this policy and other applicable UNTHSC policies, state and federal law and as long as personal use does not result in any additional incremental costs to UNTHSC or cause disruption to the campus. Disciplinary action, up to and including expulsion may result from unauthorized use.	Students
2. **Privacy.** Users of UNTHSC's computer systems should be aware that computer use may be subject to review or disclosure in accordance with the Texas Public Information Act and other laws; administrative review of computer use for security purposes or in regard to a policy or legal compliance concern; computer system maintenance; audits and as otherwise required to protect the reasonable interests of the organization and other users of the computer system. Anyone using the UNTHSC computer systems expressly consents to monitoring on the part of UNTHSC for these purposes and is advised that if such monitoring reveals evidence of possible criminal activity, campus administration may provide that evidence to law enforcement officials.	All Users

3.	**Copyright Law.** U.S. copyright law grants authors certain exclusive rights of reproduction, adaptation, distribution, performance, display, attribution and integrity to their creations, including works of literature, photographs, music, software, film and video. Violations of copyright laws include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recordings) and distributing copyrighted materials over computer networks. Users should assume that works communicated through the computer network are subject to copyright laws, unless specifically stated otherwise.	All Users
4.	**Valuable Assets.** Electronic communication resources and records are considered valuable assets that belong to UNTHSC. Further, computer software purchased or leased by UNTHSC is the property of UNTHSC or the company from whom it is leased. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these assets may constitute a computer-related crime, punishable under Texas statutes and federal laws. UNTHSC computer resources must not be transported without appropriate authorization.	All Users
5.	**Records Retention.** State law defines a state government record as "any written, photographic, machine-readable, or other recorded information regardless of medium created or received by or on behalf of a state agency or an elected state official that documents activities in the conduct of state business or use of public resources. UNTHSC holds ownership and title to all records and information created, received, acquired, or maintained in the normal course of business by any employee or organizational component. These records are the property of UNTHSC. All e-mail sent or received by UNTHSC is considered a state record. Therefore, all e-mail messages must be retained or disposed of according to UNTHSC's Records Retention Schedule. The following Records and Information Management policies provide further direction for the life cycle management of records: 04.310 Records Management Program Policy 04.311 Records Retention Policy 04.312 Records Disposition Policy UNTHSC Records Retention Schedule - http://www.hsc.unt.edu/policies/rcmgmt/schedule.pdf A state record may not be destroyed if any litigation, claim, negotiation, audit, open records request, administrative review, or other action	All Users

involving the record is initiated before the expiration of a retention period for the record set by the commission or in the approved records retention schedule of the agency until the completion of the action and the resolution of all issues that arise from it, or until the expiration of the retention period, whichever is later.

6. **Use of E-mail**. E-mail messages are official records and are subject to state and UNTHSC rules and policies for retention and deletion. All Users

Incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—can be used to attend to personal matters via e-mail.

All e-mail sent or received by UNTHSC is considered a state record. Therefore, all e-mail messages must be retained or disposed of according to the campus retention schedule.

Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.

Individuals must not send, forward or receive confidential or sensitive UNTHSC information through non-UNTHSC e-mail accounts (e.g., Yahoo!, AOL, or any other e-mail service belonging to an Internet service provider).

Departments and individuals should be judicious in sending e-mail to all faculty, staff and/or students. E-mail addressed to faculty/staff and/or students is only allowed by authorized users when the nature of the message is of sufficient general value and length that it would justify being sent as a memorandum, but requires the immediacy of e-mail. Only select UNTHSC users, approved by a Dean, Department Head, Vice President or higher level management official, will be granted the ability to send e-mail to the all-staff and/or student e-mail distributions.

Campus-wide electronic mail distribution is not to be used for personal announcements including lost items, items for sale, or other similar uses. UNTHSC administration has authorized certain types of such advertisements to be posted on Treasure Chest and campus Daily News applications. This exclusion applies ONLY to the Daily News and Treasure Chest. Contact the EBAC for further information on policies, procedures and use of Treasure Chest.

In order to take advantage of the efficiency with which official messages can be transmitted via e-mail, UNTHSC has implemented the electronic student/ faculty/ staff newsletter called The Daily News. The Daily News provides the vehicle for individuals to communicate notice of daily

events in the once-a-day newsletter format.

7.	**Use of Campus Daily News Announcements.** All UNTHSC employees, staff and students are allowed to submit to the HSC "Daily News" e-newsletter in accordance with the Campus Communications policy. The "submitter" must log in with their network user ID and password and are personally responsible for their submissions.	All Users
8.	**Use of the Internet**. Employee personal Internet use on UNTHSC systems is a privilege, not a right. As such, use should be limited (e.g., personal use could be allowed on a limited basis during lunch or other breaks and during limited periods before and after the employee's regularly scheduled working hours). The privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action. Supervisors have the right to monitor employee internet access as well as to restrictions on employee internet use. All users of UNTHSC electronic communication resources must use the Internet facilities in ways that do not disable, impair, or overload performance of any other campus computer system or network, or circumvent any system intended to protect the privacy or security of another user. Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited for all users.	All Users
9.	**Instant Messaging (IM).** Employees must only download, install and/or use Instant Messaging (IM) software approved by the Information Resources & Technology department. IM must only be used for legitimate UNTHSC business purposes and for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action. Do not use IM to conduct any state business that would require the content to be saved as a state record. IM may not be used to document a statutory obligation or agency decision, and IM should not be used when the resulting record would normally be retained for recordkeeping purposes. Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material via IM is strictly prohibited.	Employees & Faculty
10.	**User of Peer-to-Peer Software.** Use of peer-to-peer (P2P) software on UNTHSC computers, networks, mobile computing devices and any other electronic communication devices is strictly prohibited. P2P	All Users

applications and protocols that are not allowed include, but are not limited to: Ares, BitComet, BitTorrent, Direct Connect, Fasttrack, eDonkey, Gnutella, KaZaa, Limewire, uTorrent, and WinMX.

Personal devices with active P2P software must not be used to connect to the UNTHSC network. This includes connections to the campus wired & wireless networks as well as remote access (VPN) connections. Any exceptions must be approved in advance in writing by the Vice President for Information Resources and Technology.

11. **User Responsibility and Accountability.** A user accepts full responsibility for his/her own actions that result in violations defined in this document including but not limited to the following situations: — All Users
    a. A user must operate UNTHSC electronic communication resources responsibly, respecting the needs of other computer users.
    b. Users are responsible for reporting observations of illegal activity and policy violations to their respective dean, department head, supervisor or to the office of the Vice President for Information Resources and Technology.
    c. Users are responsible for proactively protecting assigned account information and associated passwords. Individual account passwords must never be shared or revealed to other users (including supervisors).
    d. When communicating with others via UNTHSC electronic communication resources, a user's communications should reflect high ethical standards, mutual respect and civility.

12. **Management Responsibility.** Responsibilities of deans, department heads and supervisors: — All Users
    a. Promptly inform Human Resources when employees have been terminated so that the terminated employee's access to UNTHSC electronic communication resources can be disabled in a timely manner. In addition, for non-routine terminations including terminations that involve disciplinary action, the IRT accounts administrator must be notified in advance or as soon as the personnel action takes place.
    b. Promptly report ongoing or serious problems regarding electronic communication use to the office of the Vice President for Information Resources and Technology.

13. **Actions that constitute misuse of UNTHSC electronic communication resources and records, and are thus strictly prohibited, include but are not limited to:** — All Users
    a. Criminal and illegal acts. UNTHSC electronic communication resources must not be used for or in support of illegal activities. Any such use will be reported and dealt with by the appropriate UNTHSC

authorities and/or law enforcement agencies. Criminal and illegal use may involve, but is not limited to, unauthorized access, intentional corruption or misuse of electronic communication resources or records, theft, obscenity, and child pornography.

b. Failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of UNTHSC's electronic communication resources or records.

c. Abuse of electronic communication resources or records including, but not limited to, any act which endangers or damages specific computer software, hardware, program, network or the system as a whole, whether located on campus or elsewhere on the global Internet; creating or purposefully allowing a computer malfunction or interruption of operation; injection of a computer virus on to the computer system; sending a message with the intent to disrupt UNTHSC operations or the operations of outside entities.

d. Use of UNTHSC electronic communication resources or records for personal financial gain or personal commercial purposes.

e. Failure to protect a password or account from unauthorized use. This extends to family and other household members when work is performed at home.

f. Permitting someone to use another's computer account, or using someone else's computer account.

g. Unauthorized use, access or reading of electronic communication resources or records.

h. Unauthorized use, access, duplication, disclosure, alteration, damage, or destruction of data contained on any electronic file, program, network, or UNTHSC hardware or software.

i. Unauthorized duplication or distribution of commercial software. All commercial software is covered by a copyright of some form. Unauthorized duplication or distribution of software covered by such copyrights is a violation of the copyright law and this policy.

j. Attempting to circumvent, assisting someone else or requesting that someone else circumvent any security measure or administrative access control that pertains to UNTHSC electronic communication resources and records.

k. Use of the UNTHSC electronic communication resources in a manner that violates other UNTHSC policies such as racial, ethnic, religious, sexual or other forms of harassment.

l. Misrepresenting, obscuring, suppressing, masking, or replacing a sender or recipient's identity on an electronic communication for inappropriate use.

m. The use of UNTHSC electronic communication resources for the improper transmission of information, access to which is restricted by laws or regulations (examples: FERPA, HIPAA, PHI)

n. Use of electronic mail to send information or messages that are not appropriate for public inspection.

o. Installation and/or operation of peer-to-peer software on UNTHSC computers, networks or any other electronic communication resources without having specific written approval from the Vice President for Information Resources for Technology.

References and Cross-references.
04.310 Records Management Program Policy
04.311 Records Retention Policy
04.312 Records Disposition Policy

UNTHSC Records Retention Schedule -
http://www.hsc.unt.edu/policies/rcmgmt/schedule.pdf

Approved: 05/03/2010
Effective: 05/03/2010
Revised:

Policies of the University of North Texas Health Science Center	Chapter 04 - Administration
04.302 Server Management & Security Policy	

Policy Statement.

The purpose of this policy is to state clearly the responsibilities and requirements for managing and securing a data processing server.

All servers in the institution that contain institutional data or are connected to the UNTHSC-FW network must be under the logical and physical control of the Information Technology Services Department unless the Director of Information Technology Services approves that the placement and/or control of a server should reside elsewhere. Logical control over a server is vested in the person who has administrative rights to the server.

Application of Policy.

This policy applies to all servers that belong to the UNTHSC-FW or any server connected to the UNTHSC-FW network.

Definitions.

None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. Server managers and administrators must adhere to the following: a. Responsibilities for server management must be included in a person's job description. b. Server manager is defined as a security-sensitive position (institutional requirements apply to all such positions). c. Server managers will adhere to all institution policies relating to network and data security. d. Complete the institutional security training once per year.	Server managers and administrators
2. Departments housing servers are expected to provide the proper environmental and physical security for the server in accordance with institutional policy.	Server managers and administrators
3. Server managers must maintain current documentation about the server covering the following: a. Server operating systems, directory structures and network connectivity b. License for any software running on the server c. Applications running on the server d. Client list e. Emergency procedures f. Contact list g. Data backup and recovery plan for the server h. A disaster recovery plan for the server	Server managers and administrators

4.	Backup information must be stored off-site using the Record Management Office for storage and retrieval.	Server managers and administrators
5.	Server Managers must classify and protect all data on the server in accordance with the Data Integrity and Classification Policy.	Server managers and administrators

References and Cross-references.
None

Forms and Tools. (optional)

Approved: 3/18/2004
Effective: 3/18/2004
Revised: 6/1/2004

Policies of the University of North Texas Health Science Center	Chapter 04 - Administration
04.304 Data Integrity and Classification	

Policy Statement.
The purpose of this policy is to provide a standardized classification system for data owners and managers to classify data in a consistent way so as to maintain data integrity and appropriate security levels of the University's data resources in the central computing facility.

Application of Policy.
Deans, Department Heads, and Supervisors

Definitions.
None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. Classification: Data should be classified into the following categories. Most data will fall into more than one category, but should be managed in accordance with its most restrictive classification.	Director of Infrastructure and Security

Availability: Data should be analyzed for operational dependency. How long can you operate without the data? Then use the table below to classify its criticality.

Class	A	B	C	D	E
Maximum allowed Server downtime, per event	> 1 Week	1 Week	1 Day	1 Hour	1 Hour
On which Days?	Any	Mon-Fri	Mon-Fri	Mon-Fri	7 Days
During what hours?				07:00-18:00	24h
Expected availability percentage	70%	80%	95%	99.5%	99.9%
==> expected max. downtime	= 1 week/ month	= 1 day/week	= 2 hours/ Week	= 20min./ Week	= 12min./ month

2. Sensitivity

Director of Infrastructure and Security

A classification system is proposed which classes information / processes into three levels. The lowest 1 is the least sensitive and the highest 3 is for the most important information / processes. The following concepts are needed:

- All data has an owner.
- The data or process owner must classify the information into one of the security levels- depending on legal obligations, costs, corporate into policy and business needs.
- If the owner is not sure at what level data should be classified, use level 3.
- The owner must declare who is allowed access to the data.
- The owner is responsible for this data and must secure it or have it secured (e.g. via a security administrator) according to its classification.
- All documents should be classified and the classification level should be written on at least the title page.

Once the data on a system have been classified to one of the following levels, then that system should be installed to conform to all directives for that class and classes below.

If a system contains data of more than one sensitivity class, it must be classified at the most confidential level for data on the system. The data names listed in each class below are not intended to be exhaustive but are only examples. There are many other data at the UNTHSC-FW that need to classified as well.

Class 1: Public / non classified information
This data could be made public without any implications for the UNTHSC-FW (i.e. the data is not confidential). Data integrity is not vital. Loss of service due to malicious attacks is an acceptable danger.

Examples: Test services without confidential data, certain public information services, news releases, news letters, items classified as public by State law, and data already available in the public domain, etc.

Class 2: Internal information
External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g. the UNTHSC-FW may be publicly embarrassed). Internal access is

selective. Data integrity is important but not vital.
Examples of this type of data are found in development groups (where no live data are present), certain production public services, certain Customer Data, "normal" working documents and project/meeting protocols, Telephone books, budgets, purchasing information, and fund raising information, etc.

3. Confidential information — Director of Infrastructure and Security

Data in this class are confidential within the UNTHSC-FW and protected from external access. If such data were to be accessed by unauthorized persons, it could influence the institution's operational effectiveness, cause an important financial loss, or unauthorized access would prove to be a violation of the law. Data integrity is vital.

Examples: Data centers normally maintain this level of security. Such data are personnel data, Accounting data, passwords, data protected by law, patient health information, student records, intellectual property, and data that will cause damage to the institution, etc.

References and Cross-references.
None

Forms and Tools. (optional)

Approved: 5/1/2004
Effective: 5/1/2004
Revised: 4/24/2009

Policies of the University of North Texas Health Science Center	Chapter 04 - Administration
04.305 Web Policy	

Policy Statement.
World Wide Web services at the University of North Texas Health Science Center provide information to and enable the exchange of data with members of the Health Science Center community, prospective students, and the general public. As such, the services represent the Health Science Center. Individuals, corporations, and government agencies can benefit by accessing information resources provided by the University of North Texas Health Science Center via the Web. It is of paramount importance to the Health Science Center community that information be organized and presented in a user-friendly manner on Health Science Center websites because the Web plays a vital role in helping the Health Science Center fulfill its mission.

Types of Information
Each constituency within the Health Science Center -- faculty, students, staff, and administrators -- creates and utilizes information of various types. For example, official information refers to the governing or authoritative documents of the Health Science Center. On the other hand, scholarly information, which is produced by our faculty and other experts, is related to the mission of UNTHSC, but does not necessarily impact the governance of the Health Science Center. Generally, types of information include but are not limited to:

a. Official Information
- Academic Calendar
- Academic Degrees
- Admissions
- Catalogs
- Course materials
- Demographics
- Financial Aid and Scholarships
- Recruitment Materials
- Schedule of Classes
- University Events
- University Policies, Procedures, and Practices
- University Structure

b. General Information
- Advancement and Alumni
- Community Information
- Personal Information
- Scholarly Information (e.g. faculty publications, bibliographies, databases of research results)
- Sponsored Projects
- Health Science Center Organizations

Structure of the Health Science Center Web
The UNTHSC Information Resources Working Group (IRWG) will establish standards for the structure and operation of UNTHSC's Web services as well as develop policies and procedures needed to maintain Web sites that serve the mission of the University in an effective manner.

Responsibility for Official Information
Because official information represents the Health Science Center to a worldwide community, it must be timely and accurate. Furthermore, the presentation of official UNTHSC information via the Web must adhere as closely as possible to UNTHSC's editorial and graphic standards, just as printed publications are subject to these same standards. In addition, all Health Science Center websites must adhere to state and federal regulations that assure accessibility of Health Science Center information to handicapped individuals. Web Publishing Guidelines, approved by the IRSC, assist Web authors in preparing materials that meet those standards.

Each Vice President, or the President in the case of those areas that do not report to a Vice President, is the "owner" of the official information that is created or maintained by his/her area of responsibility. An owner is defined as "the manager or agent responsible for the function which is supported by the resource." Texas Department of Information Resources. Information Resources Security and Risk Management Policy, Standards, and Guidelines. Austin, Texas: March 1993, p. 94. The owner of an official Web document is the person responsible for overseeing the management of that official information. Each Vice President may delegate the management of this official information to department heads, deans, or directors, as appropriate. Only the owners of information, or their designated information managers, may change the content of the information that they manage. Owners must routinely review the official information placed on the Web by their staff to ensure its timeliness and accuracy. In addition, Web-based programs involving financial transactions and records covered under the Family Educational Right to Privacy Act must be approved by the Health Science Center's internal auditors prior to being released to the public.

Any UNTHSC Web document may provide access to any official UNTHSC information that is on the Web, but this should be accomplished by a link to the information, rather than a duplicate copy of that information. In other words, managers of Web documents should not duplicate information that they do not manage, but instead should refer the reader to the original copy.

Application of Policy.
Students, faculty, and staff.

Definitions.
None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. **Maintenance of Official Information** Owners of official information will identify the information managers who will implement information services within the UNTHSC Web services, determining how their information maintenance needs can best be met within existing resources. These individuals must follow the standards and procedures developed by the IRWG for the Health Science Center's Web implementation. They will be assisted in this effort by the University's Team Web, who will develop the necessary models, operational guidelines, and procedures for creating and maintaining effective Web sites.	Data Owners
2. **General Information** Whoever creates information other than official UNTHSC information is the owner of that information and is solely responsible for its content. A Web document, such as a 'personal home page,' which is made available from any UNTHSC computer system, may provide any unofficial information relating to the mission and goals of the University, as long as it complies with UNTHSC policies, as well as federal and state laws. UNTHSC can accept no responsibility for the content of these documents; in fact, UNTHSC will not undertake to edit or pre-approve these documents. However, any of these documents discovered that are in violation of these policies and laws shall be subject to immediate removal from UNTHSC computer systems. Persons responsible for Web development are expected to adhere to all applicable state and federal regulations and internal policies and guidelines associated with security, risk measures, and copyright compliance. Permission must be obtained in advance before publishing copyrighted material (text, graphics, etc.) on UNTHSC Web sites and notification of copyright should be shown on pages containing those materials.	Data Owners

References and Cross-references.
None

Forms and Tools. (optional)
None

Approved: 3/14/2002
Effective: 3/14/2002
Revised: 6/1/2004

Policies of the University of North Texas Health Science Center	Chapter 04 - Administration
04.306 Cellular Phone Use and Allowance	

Policy Statement

To establish UNTHSC policy regarding payments of allowances for the use of personal cellular phones in conducting UNTHSC business and, under limited and exceptional conditions, for the provision of UNTHSC-provided cellular phones to employees. This policy is intended to provide an alternative to the need for many faculty and staff to carry two cellular phones (for UNTHSC and personal use), to simplify payments and associate record keeping, and to eliminate potential problems over personal use of UNTHSC provided cellular phones.

The UNTHSC will cease providing organization-owned cellular phones to faculty and staff, except as prescribed below, as soon as practicable after the adoption of this policy. It will, however, continue to provide an allowance for charges incurred as the result of a faculty or staff member's use of a personal cell phone for official business when the faculty or staff member has an official state business need for the phone.

Cell Phone Allowance

a. The UNTHSC will provide an allowance to regular retirement-eligible faculty and staff members for the use of a personal cell phone for official business purposes. Examples of official state business reasons why a faculty or staff member may need a cell phone include but are not limited to: the employee travels frequently, the employee is frequently out of the office on official business, the employee uses the phone on job sites where wired phones are not available, or the employee is a member of key personnel who are needed in the event of an emergency.

b. The employee's chair/department head must approve the request for the allowance and provide the funding. A HRM6 must be completed in order for the allowance to be paid.

c. The employee is responsible for contracting with a cell phone service provider, for paying any initial plan charges, for the purchase of the cell phone itself and for paying the plan's monthly bills. UNTHSC will pay an initial allowance for the purchase of the telephone instrument (if it has not already been purchased by the UNTHSC) equal to 50% of the purchase price of the instrument, but not to exceed $150 for PDA's (personal Digital assistants) and $50 for non-PDA instruments. A purchase receipt or invoice itemizing the purchase price of the instrument must be submitted on a HRM6 for reimbursement. An employee is eligible to receive this allowance every 36 months if they choose to upgrade their telephone instrument.

d. The UNTHSC will provide a flat-rate monthly allowance, independent of the cell phone provider selected by the employee, of $10 for text messaging (to replace a pager service), either $20, $30 or $40 per month for employees using only basic voice services, and an additional $40 per month for employees using advanced data services (email and web

services), for an approved request.

e. Employees requesting allowances or purchase allowances for advanced voice and data services must justify their request and show why their position at UNTHSC requires advanced services.

f. The allowance amounts shown above will be reviewed annually by Telecommunications. Recommendations for changes may be made if warranted.

g. Each chair/department head is required to annually review eligibility and basic cell phone allowances of employees in their department and verify the employees' eligibility for reimbursement by having the employees demonstrate that they are still utilizing the cell phone service for business purposes and the reimbursement level is correct. It is the responsibility of the employee to inform the department head of any changes in his/her status or need for the use of the phone.

h. All monthly allowances on instrument purchase allowances will be paid as miscellaneous additions to the employee's regular paycheck and are subject to FICA and tax withholding. Employees may choose to detail their cell phone expenses as a business expense when filing income tax forms.

i. The cellular phone acquired by the employee is considered to be the personal property of the employee and accordingly shall be used in any way the employee deems appropriate. Any service contract the employee might enter into regarding the acquisition or operation of the cell phone is personal to the employee. The UNTHSC shall have no obligation or make any guarantees with respect to such contract to the employee or to the service provider.

Support

a. Support for UNTHSC owned devices and plans will be provided by Telecommunications on an as needed basis, and may be subject to service fees.

b. Support for over-the-air email and calendaring, Skyscape, etc on personal devices will be provided by the Help Desk with a per hour charge.

c. All plan and service support for personal devices will provided by the service provider.

Special circumstances of an employee's job responsibilities at the UNTHSC may justify exceptions to the standard policy above.

a. Any exception to the policy must be documented and approved by the chair/department head.

b. HSC may issue HSC owed cell phones to employees whose job duties warrant. Request for a HSC owned cell phone must be submitted to the Telecommunications department on the appropriate form and are subject to the following:

   - HSC owned cell phones will be use for HSC business only. No provision for personnel calls is made.

- Telecommunications will select the vendor, plan and equipment to full fill the request.
- The cell phones will be the property of the HSC and will be listed in the inventory. A property custody receipt will be required.
- The using department will be charged for all costs associated with the phone service plus an administration fee.
- The request must be approved by the Executive Vice President of Finance and Administration.

Application of Policy.
Faculty and staff.

Definitions.
None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
See policy statement above.	

References and Cross-references.
None

Forms and Tools. (optional)
None

Approved: 9/1/2000
Effective: 9/1/2000
Revised: 9/1/2007

Policies of the University of North Texas Health Science Center	Chapter 04 - Administration
04.307 Protected Health Information Electronic Communications	

Policy Statement.
The UNT Health Science Center complies with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards regarding use and disclosure of Protected Health Information through electronic communications.

Application of Policy. This policy applies equally to all individuals granted access privileges to any University of North Texas Health Science Center at Fort Worth (UNTHSC) information resource with the capacity to send, receive, or store electronic communications.

Definitions.

1. **Electronic Communications –** Any form of email or facsimile communication as defined herein.
2. **Electronic Mail System –** Any computer software application that allows electronic mail to be communicated from one computing system to another.
3. **Electronic Mail (email) –** Any message, image form, attachment, data, or other communication sent, received, or stored within an electronic email system.
4. **External EMail –** Email communications sent outside the UNTHSC network (i.e. email communications to an address other than one with hsc.unt.edu).
5. **Internal EMail –** Email communications exchanged within the UNTHSC network (i.e. email communication to an address with hsc.unt.edu).
6. **Facsimile (Fax) –** An image or document that is transmitted in digitized electronic form over telephone/computer lines and reproduced in its original form on the receiving end.
7. **Protected Health Information (PHI) –** Individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic. Individually identifiable health information relates to an individual's health status or condition, furnishing health services to an individual or paying or administering health care benefits to an individual that is created or received by the health care provider. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual.
8. **Treatment –** The provision, coordination, or management of health care 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 for the referral of a patient for health care from one health care provider to another.

9. **Health Care Operations –** Refers to the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates in conducting quality assessment and improvement activities, review of competence or qualifications of health care professionals, legal services, business planning, business management, customer service, and resolution of internal grievances.
10. **Payment –** The activities undertaken by a health care provider to obtain reimbursement, billing, claims management, collection activities, review of health care services with respect to medical necessity, disclosure to consumer reporting agencies, and utilization review activities.
11. **Provider –** For purposes of this policy, the provider is the health care provider allowed by this policy to exchange PHI via electronic mail within the parameters of this policy.

Procedures and Responsibilities.

Responsibility. All supervisors, faculty, staff and students are responsible for complying with this policy. All supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

1. All electronic communications containing PHI must be in accordance with this policy.

2. Electronic communications containing PHI must be treated with the same degree of privacy and confidentiality as the patient's medical record.

3. Both the patient and the provider MUST agree to communicate via electronic communications on non-emergent and non-urgent matters. The patient or authorized representative should complete the University of North Texas Health Science Center at Fort Worth Patient Electronic Communications Authorization Agreement before corresponding by electronic communication. If the University of North Texas Health Science Center at Fort Worth Patient Electronic Communications Authorization Agreement has not been signed allowing correspondence via electronic communication, UNTHSC personnel should have the patient sign an agreement before any electronic communication is initiated. A copy of the signed University of North Texas Health Science Center at Fort Worth Patient Electronic Communications Authorization Agreement should be given to the patient and the original should be forwarded to the appropriate medical records custodian for filing in the patient's medical record. The staff member witnessing the patient's signed authorization should verify the patient's correct e-mail address as it is written on the release by verbally repeating it back to the patient.

4. All electronic communication between a provider or other UNTHSC personnel and a patient should be in accordance with the University of North Texas Health Science Center at Fort Worth Patient Electronic Communications Authorization Agreement and the other

requirements of this policy. It is the responsibility of each UNTHSC faculty or staff member to make sure the patient has signed the University of North Texas Health Science Center at Fort Worth Patient Electronic Communications Authorization Agreement before corresponding with the patient by electronic communications.

5. External electronic communication messages containing PHI are only permitted to be sent to third parties when specifically authorized by the patient and if the electronic communication meets the other requirements of this policy.

6. Patient authorization is not required to exchange internal electronic communication that contains PHI as long as the internal electronic communication is for treatment, payment, or health care operations and complies with the other requirements of this policy.

7. The authority to send external electronic communication which contains PHI to patients or outside health care providers is limited to credentialed providers, such as faculty members, nurse practitioners, physician assistants, etc. The credentialed provider may appropriately delegate electronically communicated PHI to clinic or office staff, such as emailing or faxing a clinical report to an outside physician or an office appointment to a patient if other requirements of this policy are met. Other staff, such as billing staff, are allowed to email or fax PHI if authorized by the department administrator or chairman and if the other requirements of this policy are met.

8. Students are not allowed to send external electronic communications containing PHI to patients or outside health care providers under any circumstances. Students are allowed to send internal electronic communications containing PHI under the direction of the supervising faculty member and if the other requirements of this policy are met.

9. Electronic communications should be considered the same as a formal letter to the patient. In accordance with TSBME Rule 174.4(2) physicians who use the Internet must ensure prior to providing treatment, including the issuing of prescriptions, that a proper physician-patient relationship is established that at a minimum includes the following:
    a) establishing that the person requesting the treatment is in fact who the person claims to be;
    b) establishing a diagnosis through the use of acceptable medical practices such as patient history, mental status examination, physical examination, and appropriate diagnostic and laboratory testing to establish diagnoses and identify underlying conditions and/or contraindications to treatment recommended/provided;
    c) discussing with the patient the diagnosis and the evidence for it, the risks and benefits of various treatment options; and
    d) ensuring the availability of the physician or coverage of the patient for appropriate follow-up care.

10. In general, electronic communications should be used to address administrative issues, relay follow-up information, and answer questions following a face-to-face evaluation and

consultation. Initial evaluation, diagnosis and matters of a sensitive nature are not appropriate topics to be communicated through electronic communications. The health care provider should use discretion in corresponding with the patient through electronic communication for treatment.

11. The following are examples of topics which are appropriate for electronic communication: Prescriptions/refills, general medical advice after an initial face-to-face visit, follow-up on patient status after an office visit and lab test results.

12. Examples of inappropriate topics include:
    - Discussion of HIV status
    - Mental Health problems
    - Substance Abuse (Drug and Alcohol)
    - Sexually-transmitted diseases
    - Any topic that contains "sensitive information"

    Urgent and Emergent issues are not appropriate for electronic communication.

13. All PHI exchanged via electronic communication should be maintained in a private and confidential manner. When using any PHI in electronic communication UNTHSC personnel and students shall limit the information exchanged to the minimum necessary to meet the requestor's needs and use de-identified health information whenever possible.

14. All physicians that use telemedicine medical services in their practices shall adopt protocols to prevent fraud and abuse through the use of telemedicine medical services. These standards must be consistent with those established by the Health and Human Services Commission pursuant to §531.02161 of the Government Code and UNTHSC Computer Resources Security Policy.

15. Patients are free to e-mail their health care provider at any time. The health care provider or UNTHSC personnel should respond to a patient's electronic communication within two to three business days, unless the individual is on leave and not in the office or in the clinic, in which case an automated "out of office" response should be placed on providers email box and a designated clinic staff member should respond to faxes, as appropriate.

16. If an action is taken based upon an electronic communication from a patient, the health care provider or UNTHSC personnel should respond to the patient's electronic communication notifying them of the action taken.

17. Providers should ensure that language used in electronic communications with patients is clear, concise and professional. The following are guidelines for electronic communications:
    a. Include a clear and specific subject line starting with "CONFIDENTIAL" Example: "CONFIDENTIAL – prescription refill"
    b. Edit any quoted text down to the minimum needed

c. Review the final draft before sending
d. Evaluate how the recipient might react to the message
e. Check spelling and grammar
f. Refrain from using ALL CAPS in electronic communication as it is normally perceived as direction, stern emphasis, or dictatorial
g. Use caution in the amount and type of information written in an electronic communication
h. Assume the electronic communication is not secure, and information in electronic communication is always at risk
i. When in doubt about the content of the electronic communication or the possible reaction of the recipient, call the patient rather than communicating by electronic communication.

18. A header should be attached on every electronic communication exchanged stating the following: *"TO MY PATIENTS: You must provide me with written authorization before I can communicate with you be electronic communication (e-mail or fax). If you have not signed an authorization form, please contact my office, and we will send you the form. Please note UNTHSC cannot and does not guarantee the privacy or security of any message being sent over the internet. Electronic communication is not necessarily confidential and should be used for routine matters only.* ***If you have an Urgent or Emergent issue, please go to your nearest emergency department for evaluation or call 911. Electronic communication may not be read in a timely manner if I am out of the office."***

19. In addition, a standard confidentiality statement must be included as a footer on all outgoing electronic Patient Health Information (PHI) communication, "**The information in this electronic communication (email and/or fax) may be confidential. This electronic communication is intended to be reviewed only be the individual or organization named above. If you are not the intended recipient or an authorized representative of the intended recipient, you are hereby notified that any review, dissemination, or copying of this electronic communication and its attachments, if any, or the information contained herein is prohibited. If you have received this electronic communication in error, please immediately notify the sender by telephone or other appropriate means. If sent via computer, delete the communication from your system. Thank you."**

20. All UNTHSC originated facsimile transmissions MUST have a cover sheet that includes the confidentiality statement.

21. Texas State Board of Medical Examiners Rules Chapter 174.4(e) provides that
    a. Medical records must include copies of all patient-related electronic communications, including patient-physician e-mail, prescriptions, laboratory and test results, evaluations and consultations, records of past care and instructions.
    b. Notice of privacy practices related to the use of e-mail must be filed in the medical records.

22. A provider who sends or receives electronic communication messages, concerning the treatment of or health education for a patient, is responsible for printing a copy of the electronic communication message and forwarding same to the medical record custodian to file in the patient's medical record.

23. If UNTHSC personnel receives unwanted electronic communication from a patient or a prospective patient and either does not have a UNTHSC Electronic Communications Authorization Agreement in place or does not wish to communicate with the patient by electronic communication, the individual should respond to the individual with the following statement as appropriate: ***"As a result of my concern for your well being, please contact my office to schedule an appointment to discuss any and all issues regarding the state of your health. Either I do not respond to electronic communications (email and/or fax) at this time or I believe an office visit is the appropriate method to address your concerns. You may reach my office at XXX-XXX-XXXX."***

24. All external disclosures of PHI should be in compliance with the UNTHSC privacy practices and policies addressing use and disclosure of PHI, including accounting for disclosures. When disclosing PHI through electronic communication to a third party, the release must be documented and accounted for as outlined in UNTHSC privacy practices and policies.

25. UNTHSC personnel shall not compile patient email addresses for marketing or fundraising purposes or supply patient email addresses to any third party for advertising, solicitations, or any other use.

References and Cross-references.
None

Forms and Tools. (optional)

The University of North Texas Health Science Center at Fort Worth
Patient Electronic Communication Authorization Agreement
The University of North Texas Health Science Center at Fort Worth (UNTHSC) offers patients the ability to communicate with its health care providers via electronic communication (email and/or fax) for **NON-URGENT** matters. Both you, the patient, and your provider have to agree to this arrangement. **No information is ever sent electronically to you without the permission of you or your legally authorized representative.**

If you have an email address or fax number and would like to take advantage of this service, please discuss your wishes with your health care provider first. Some providers do not communicate with their patients electronically. Others may ask an associate such as a nurse or billing person to contact you, based on your electronic communication.

Electronic communication may be used to request information and ask non-urgent questions. It should NOT be used in emergencies. If you are experiencing a sudden or severe change in your health, or otherwise need an immediate response, please go to your nearest emergency department for evaluation.

Electronic communication may be appropriately used to send protected personal health information to: (1) You, for your personal use, (2) consulting physicians involved in your care, (3) assisted living centers, home health agencies, or nursing homes involved in your care, (4) pharmacies to refill prescriptions, (5) hospitals providing you care and services, (6) physical therapists and other allied health personnel involved in your care, or (7) family members involved in your care and approved by you to receive this information.

UNTHSC may forward electronic communication as appropriate for diagnosis, treatment, and other related reasons. As such, UNTHSC staff, other than your provider, may have access to electronic communication you send. Such access will only be permitted in order to provide service to you. Otherwise UNTHSC will not forward electronic communication to any independent third parties without your prior written authorization, except as authorized or required by law. Electronic communication will be documented in your medical record by filing a paper copy in your medical record.

If a provider agrees to exchange electronic communication with you, please observe the following:

A. When sending electronic communication to your provider please be sure to include your full name and your date of birth in every electronic communication message that you send to your provider. The subject line should include the purpose of the electronic communication, for example: "***CONFIDENTIAL - Prescription Refill Request***."

B. When you receive a message from your provider containing medical advice, please acknowledge the message by sending a brief reply to the provider. If an email message is returned because of a "bad address" please make sure that you entered the complete address as it was given to you. If you are sure that you entered the address the provider gave you, please call the provider's office and make sure you have the correct email address and the computer system is functioning properly. If a health care provider does not answer your electronic communication within two-to-three business days, contact the office by telephone.

C. Do not use electronic communication to send or request very sensitive information. This includes personal information you do not want other people to know about.

D. <u>UNTHSC cannot and does not guarantee the privacy or security of any messages being sent over the Internet</u>.

Any email messages sent between UNTHSC and anyone outside is exchanged over the Internet. There is potential that email sent over the Internet can be intercepted, and read by others. If this is of concern to you, you should **not** communicate with your health care provider by email.

E. UNTHSC may choose to stop electronic communication at any time

Authorization to use Electronic Communication:

1. **I have been informed of and understand the risks, benefits, and procedures involved with using electronic communication (email and/or fax) to communicate with my provider.**
2. **I agree to the terms listed on this form and hereby voluntarily request, consent to, and authorize the use of electronic communication (email and/or fax) as one form of communication with my physician and his/her associates.**
3. **I also agree that the UNTHSC and its faculty and staff shall not be liable for any type of damage or liability arising from or associated with the loss of confidentiality due to electronic communication (email and/or fax).**
4. **I understand that UNTHSC cannot and does not guarantee the use of this means of communication will be free from technological difficulties including, but not limited to, loss of messages.**

Patient/Representative Signature: **Date:**
Print Name/Relationship:
Witness: Date:
Provider email address: **Office Number: ( )**
Print Patient email address:

You will be given a copy of this signed form to keep for your records.

Approved: 8/1/2005
Effective: 8/1/2005
Revised:

Policies of the University of North Texas Health Science Center	Chapter 04 – Administration
04.308 Transmission of Health Information via PDA	

Policy Statement.
The Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards establish mandatory guidelines for protecting a patient's Protected Health Information. This policy sets the rules and procedures for the use of Personal Digital Assistants where Protected Health Information is stored and used.

The use of PDA's to transmit or store PHI should be limited to those individuals whose employment or educational responsibilities require them to have access to such information at sites outside of the UNTHSC campus.

PDA's containing PHI must be treated with the same degree of privacy and confidentiality as the patient's medical record.

Prerequisites for use of PDAs – No user may, for any business purpose, download, maintain, or transmit, confidential patient or other information on a PDA without properly securing the PHI. PDAs pose a significant risk with respect to security issues because they may contain confidential patient information and are portable. As a result, PDA's are at risk for loss, theft, or other unauthorized access.

The best practice is to keep PHI information off PDAs entirely. If that is not possible, users must use complex password protection to limit access to PHI stored on their PDA. This will require passwords to be alphanumeric. Passwords must have a minimum of seven 7 characters with at least four (4) of the characters being one of the following: uppercase letters, lowercase letters, numbers, or special characters. Users must secure their PDAs at all times. If the PDA has advanced password protection and encryption capabilities, these applications should be used to store or transmit PHI.

Removable media such as memory cards must not be used to store confidential PHI.

If the PDA has Bluetooth capabilities and is used to store PHI, the device should be kept in nondiscovery mode at all times.

Users shall not share their password nor permit anyone else to use the PDA for any purpose, including, but not limited to, the user's family and/or associates, patients, patient families, or unauthorized employees or agents of UNTHSC.

If users choose to download any information from a PDA to a personal computer outside of the UNTHSC system, a password security device must be used and the computer must have antiviral

software. If PHI is being transmitted wirelessly, it must be encrypted unless accessing a secured network like the one currently available at UNTHSC by using encrypted VPN.

At the termination of employment or educational training at UNTHSC all PHI contained in a PDA and/or downloaded to a personal computer must be immediately and permanently destroyed.

If the PDA is lost or stolen, the user of that PDA is responsible for notifying his or her department and the UNTHSC Institutional Privacy Officer, in addition to any other reports required to be made under UNTHSC fiscal policies for lost or stolen property.

Application of Policy.
This policy applies equally to all individuals, including students, at the University of North Texas Health Science Center (UNTHSC) granted access to Protected Health Information.

Definitions.

1. Protected Health Information (PHI) – Individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic. Individually identifiable health information relates to an individual's health status or condition, furnishing health services to an individual or paying or administering health care benefits to an individual that is created or received by the health care provider. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual.

2. Personal Digital Assistant (PDA) – Any electronic device that stores or transmits data, including PHI, that is not stationary, like a desktop computer, but instead is mobile. PDAs include but are not limited to beepers or pagers, cellular phones (or any other wireless communication device), notebook or laptop computers, or any other portable electronic device.

3. Treatment – The provision, coordination, or management of health care 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 for the referral of a patient for health care from one health care provider to another.

4. Health Care Operations – Refers to the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates in conducting quality assessment and improvement activities, review of competence or qualifications of health care professionals, legal services, business planning, business management, customer service, and resolution of internal grievances.

5. Payment – The activities undertaken by a health care provider to obtain reimbursement, billing, claims management, collection activities, review of health care services with respect to medical necessity, disclosure to consumer reporting agencies, and utilization review activities.

6. Provider – For purposes of this policy, the provider is the health care provider allowed by this policy to contain and operate PHI in a personal digital assistant within the parameters of this policy.

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. Responsibility. All individuals who choose to store PHI on a wireless device become custodians of that data with all of its attendant responsibilities, including adherence to the procedures contained in this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.	Individuals who choose to store PHI on a wireless device

References and Cross-references.
None

Forms and Tools. (optional)

Approved: 8/1/2005
Effective: 8/1/2005
Revised:

Policies of the University of North Texas Health Science Center	Chapter 04 – Administration
04.310 Records and Information Management Program	

Policy Statement.

The University of North Texas Health Science Center recognizes, as described in the Texas State Records Management Manual, that "the records of Texas state government are an important resource for citizens as well as public officials." State records may provide proof of a particular action, contain evidence to protect the rights of individuals or the government, and provide decision support or other information valuable to the progress of state business.

Records and information management is a science that provides reasonable assurance that the business and technology environments are aware that it is necessary to manage the University's "recorded information" as an asset to support effective decision-making and in order to meet operational, legal, contractual, fiscal, regulatory, research, and historical requirements. Records, regardless of medium, are the memory of the University of North Texas Health Science Center at Fort Worth. Records are created to document specific business activities so that those actions and activities can be substantiated and evaluated at a later point in time. Records must be systematically controlled and managed from the time of creation/receipt to the time of destruction.

All records must be recorded in the regular course of business, at or near the time that events took place, by someone who had knowledge of the events, and the record of those events must have been maintained in manner to demonstrate authenticity of the record.

Ownership

The University of North Texas Health Science Center holds ownership and title to all records and information created, received, acquired, or maintained in the normal course of business by any employee or organizational component. These records are the property of The University of North Texas Health Science Center.

Records and Information Management Program

The Records and Information Management program includes, but is not limited to, records management and storage, imaging services, historical archives, retention scheduling, and records disposition. In addition, issues such as forms management, identification of vital records, and disaster recovery for vital records are also addressed.

Creation and Retrieval

Each health science center division is responsible for maintaining an accurate, timely record of business transactions and events as normally maintained in the regular course of business. Specifically, it is the responsibility of each department to ensure that records are indexed in a manner as to be identified and retrieved in a timely manner per regulatory, contractual, and business requirements.

Archival

All records are to be archived in accordance with the Records Management Archives Policy. Each business operation, in partnership with Records and Information Management, is responsible for maintaining archived records in a manner as to be identified and retrieved in a timely manner pre regulatory, contractual, and business requirements. Each business operation is required to maintain an accurate inventory of records archived.

Disposition

All records are to be destroyed in accordance with the Records Management Disposition Policy. Records that have been identified as candidates for destruction will undergo a review by the Records Manager and the manager of the appropriate business operation prior to destruction. Records series that require additional review will be submitted to the Audit Department and General Counsel.

Application of Policy.

This policy applies to anyone who creates or maintains business records that are either required or would be normally maintained in the regular course of business.

Definitions.

None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
Responsibilities of Agency Heads in the State of Texas regarding records management programs, according to Texas Government Code, Chapter 441.183 are described as follows:	Agency head of each state agency

The agency head of each state agency shall:

(1) establish and maintain a records management program on a continuing and active basis;

(2) create and maintain records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency designed to furnish information to protect the financial and legal rights of the state and any person affected by the activities of the agency;

(3) make certain that all records of the agency are passed to the agency head's successor in the position of agency head;

(4) identify and take adequate steps to protect confidential and vital state records;

(5) cooperate with the commission in the conduct of state agency records management surveys; and

(6) cooperate with the commission, the director and librarian, and any other authorized designee of the director and librarian in fulfilling their duties under this subchapter.

Source: Added by Acts 1997, 75th Leg., ch. 873, sec. 1, eff. Sept. 1, 1997.

Responsibilities of the Records Management Officer, according to Texas Government Code, Chapter 441.184, are as follows:

Records Management Officer

(a) Each state agency head shall act as or appoint a records management officer for the state agency to administer the agency's records management program. An employee of an agency is eligible to be appointed as the agency's records management officer only if the employee holds a position in which the employee reports directly to the agency head or to a person with a title functionally equivalent to deputy executive director.

(b) The records management officer for each state agency shall:

(1) administer the records management program established under Section 441.183;

(2) assist the agency head in fulfilling all of the agency head's duties under this subchapter and rules adopted under this subchapter;

(3) disseminate to employees of the agency information concerning state laws, administrative rules, and agency policies and procedures relating to the management of state records; and

(4) fulfill all duties required of records management officers under this subchapter and rules adopted under this subchapter.

Source: Added by Acts 1997, 75th Leg., ch. 873, sec. 1, eff. Sept. 1, 1997. Amended by Acts 1999, 76th Leg., ch. 321, sec. 1, eff. Sept. 1, 1999.

The Director of Records and Information Management is designated as the Institutions Records Management Officer.

COMMUNICATION

Director of Records and Information Management

Updates

Records and Information Management will form a key network within the University that is concerned about records and information management activities. Members of the network will serve as intermediaries between business operations and the records and information management program to ensure compliance.

Records and Information will work with business departments, technology services, risk management, and internal audit functions to address records and information management deficiencies as applicable.

MEASUREMENT & MONITORING

Tracking & Oversight

The Records and Information Management program is subject to audit by Internal Audit and all parties authorized due to regulatory, contractual, or business requirements.

References and Cross-references.

Statutory Requirements

The Texas Government Code, Chapter 441, Subchapter L, establish the responsibilities of State Agencies and Universities, the State and Local Records Management Division of the Texas State Library, and the State Archives in managing the state's records. Each State Agency and University or University System has a Records Management Officer, who acts as a liaison for records and information management functions between the two agencies.

Acts 1997, 75th Leg., ch. 873, sec. 1, eff. Sept. 1, 1997.

Acts 1997, 75th Leg., ch. 873, sec. 1, eff. Sept. 1, 1997. Amended by Acts 1999, 76th Leg., ch. 321, sec. 1, eff. Sept. 1, 1999.

Forms and Tools.

SUPPORTING DOCUMENTS

Texas State Library and Archives Commission Records Management Manual

RELATED DOCUMENTS

Records Management Manual
* Records Management Policies
* Records Management Procedures
* UNT Health Science Center Records Retention Schedule

Records Management Division Procedures Manual

Approved: **8-16-2006**
Effective: **8-16-2006**
Revised: **4-17-2007**

Policies of the University of North Texas Health Science Center	Chapter 04 – Administration
04.311 Records Retention	

Policy Statement.

The University of North Texas Health Science Center recognizes, as described in the Texas State Records Management Manual, that the records of Texas state government are an important resource for citizens as well as public officials. State Records may provide proof of a particular action, contain evidence to protect the rights of the individuals or the government, and provide decision support or other information valuable to the progress of state business.

The purpose of this records retention schedule is to identify the length of time a records series must be retained in active or inactive status before its final disposition.

Application of Policy.

This policy applies to anyone who creates or maintains business records that are either required or would be normally maintained in the regular course of business.

Definitions.

1. **CFR - Code of Federal Regulations**
   Regulations of federal agencies adopted under authority of laws enacted by the U.S. Congress.

2. A **"state record", "public record", "official record"**
   Is defined as a document, book, paper, photograph, sound recording, or other material, regardless of physical form or characteristics, made or received according to law or ordinance or in connection with the transaction of official business.

3. A **"records series"**
   Is defined as a group of identical or related records that are normally used and filed as a unit.

4. **"Final disposition"**
   Is defined as the terminal treatment of the records series, either by destruction or permanent storage.

5. A **"state publication"**
   Is defined as information in any format that is produced by the authority of or at the total or partial expense of a state agency or is required to be distributed under law by the agency, and is publicly distributed. The term does not include information the distribution of which is solely limited to contractors with or grantees of the agency, staff persons within the agency or within other government agencies, or member of the public under a request

made under the open records law, Government Code, Chapter 552. The term includes but is not limited to: a publication distributed in print, on microform, as audiovisual material, as interactive media or on electronic external storage device; an on-line publication which is an index to other on-line publications, one or more text, graphic, or other digital files, or a user interface to a computer database.

6. **TAC - Texas Administrative Code**.
   Regulations of state agencies adopted under authority of laws enacted by the Texas Legislature.

Procedures and Responsibilities.

The University of North Texas Health Science Center Records Retention Schedule was prepared in response to the requirements of Chapter 441, Subchapter C, of the Texas Government Code. This University of North Texas Health Science Center Records Retention Schedule has been approved by the Texas State Auditor's Office and the State Library and Archives Commission.

Records series titles were based on an audit conducted by the health science center. Retention periods were assigned to record series based on their administrative, legal, fiscal, and historical values.

Questions concerning titles and final disposition of records series should be referred to the Records Manager, who is the health science center's designated records management officer. Questions concerning legal requirements for the retention and disposition of health science center records series should be referred to the General Counsel.

Procedure / Duty	Responsible Party
1. Each Health Science Center office is responsible for the review of, and compliance with, the University of North Texas Health Science Center Records Retention Schedule. The final disposition of records must be documented. Please refer to the Records Management Disposition Policy. Offices should contact the Records Manager concerning the destruction of all state records and, records not listed in the retention schedule. All confidential records series must remain inaccessible to unauthorized personnel.	Department head
2. Each office must ensure that the accuracy, completeness, and accessibility of information are not lost prior to its authorized destruction date because of changing technology or media deterioration, by converting electronic storage media and taking other action as required to provide compatibility with current hardware and software.	Department head

References and Cross-references.
Records Management Manual
* Records Management Policies
* Records Management Procedures
* UNT Health Science Center Records Retention Schedule
Records Management Division Procedures Manual

Forms and Tools. (optional)

Approved: 9-3-2002
Effective: 9-3-2002
Revised: 4-27-2007

Policies of the University of North Texas Health Science Center	Chapter 04 – Administration
04.312 Records Disposition	

Policy Statement.

Purpose
The University of North Texas Health Science Center recognizes, as described in the Texas State Records Management Manual, the statutory responsibility for the legal disposition of state records as outlined in the Texas Government Code, Chapter 441.

State Requirements
All state agencies are required to request authority before destroying state records. The process for the legal destruction of state records is outlined in the Texas Government Code, Chapter 441.

The perpetual destruction of records is based on an agency's approved "Records Retention Schedule" (Form SLR 105) accompanied by a signed "Certificate and Approval" (Form SLR 105C), or submission and approval of a "Request for Authority to Dispose of State Records" (Form RMD 102) each time unscheduled records become eligible for final destruction.

The final disposition of records must be documented. There is no standard state form for this but it is recommended that a disposal log or file be maintained at the agency level that includes at least the following:
(a) Records series title
(b) Retention period
(c) Volume of records eligible for final disposition
(d) Type of final disposition (if destruction, method used)
(e) Disposal date
(f) Signature(s) of agency personnel approving final disposition.

Maintaining documentation of records disposal complies with administrative rules for state recordkeeping (Records Retention Rules, 13 TAC §6.8).

Texas State Records Management Manual 5.98, Final Disposition.

Texas Health and Safety Code, Chapter 181 Medical Records Privacy

Government Code, Chapter 441, Texas Penal Code, Subchapter L, Section 37.10. Tampering With Governmental Records.

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

Texas Business and Commerce Code, Section 35.48 An Act relating to the disposal of certain business records that contain personal identifying information; providing civil penalty.

Application of Policy.
This policy applies to anyone who creates or maintains business records that are either required or would be normally maintained in the regular course of business.

Definitions.

1. **Records destruction** - The objective of records destruction is to remove the record from possible use after it has become obsolete and to ensure that sensitive or confidential information does not become public. Because destroyed records cannot be recalled, extra care should be taken before records destruction. All state, local, and federal statutory regulations must be satisfied.

2. A **convenience copy** - is defined as extra copies in addition to "official" records contained elsewhere.

3. A **records series** is defined as a group of identical or related records that are normally used and filed as a unit.

4. **Final disposition** is defined as the terminal treatment of the records series, either by destruction or permanent storage.

5. A **state record**, **public record, official record** is defined as a document, book, paper, photograph, sound recording, or other material, regardless of physical form or characteristics, made or received according to law or ordinance or in connection with the transaction of official business.

6. **In-Active Record** is defined as a series of records with a reference rate of less than one search per file drawer per month.

7. **Vital records** are those records essential to the resumption of business or operations, recreation of an agency's financial or legal position, and the protection of employee and citizen rights.

8. **General Disposal** is defined as disposing of intact records by general trash collection or bulk recycling.

9. A **state publication** is defined as information in any format that is produced by the authority of or at the total or partial expense of a state agency or is required to be

distributed under law by the agency, and is publicly distributed. The term does not include information the distribution of which is solely limited to contractors with or grantees of the agency, staff persons within the agency or within other government agencies, or member of the public under a request made under the open records law, Government Code, Chapter 552. The term includes but is not limited to: a publication distributed in print, on microform, as audiovisual material, as interactive media or on electronic external storage device; an on-line publication which is an index to other on-line publications, one or more text, graphic, or other digital files, or a user interface to a computer database.

Procedures and Responsibilities.

Questions concerning titles and final disposition of records series should be referred to the Records Manager, who is the health science center's designated records management officer. Questions concerning legal requirements for the retention and disposition of health science center records series should be referred to the General Counsel.

Procedure / Duty	Responsible Party
1. A state record may be destroyed by a state agency if: A. the record appears on the records retention schedule approved under Section 441.185 and the record's retention period has expired; B. a Records Disposal and Disposal Inventory form must be completed and signed by the manager of the appropriate business operation. It is the manager's responsibility to review all records for compliance with the retention schedule before certifying by signature. This person must have signature authority for the department. The records disposal form and inventory must be sent to the Records Manager who will review for approval. Record series that require additional review will undergo a review by the Audit Department and General Council prior to destruction. C. Records Management must submit a RMD 102 to the state records administrator and approved by the director and librarian, or the designee of the director of the librarian, for a state record that does not appear on the approved records retention schedule. D. a state record may not be destroyed if any litigation, claim, negotiation, audit, open records request, administrative review, or other actions involving the record is initiated before the expiration of the retention record set by the commission or in the approved records	Department head

retention schedule of the agency until the completion of the action and the resolution of all issues that arise from the action, or until the expiration of the retention period, whichever is later.

2. Records containing sensitive or confidential information must be disposed of in a manner that ensures protection (13 TAC §6.8). These records must also be stored in a secured location until final disposition. All records containing confidential information must be shredded or sent to Records Management for proper destruction. The recycle bins and trash bins are not to be used for this type of information. Failure to comply is a violation of this policy, state regulations, and federal regulations. Records that are classified as a "state record" must be destroyed in accordance with the retention schedule. These records should be sent to Records Management for disposition. A "Records Disposal Form" and "Records Disposition Inventory" must be completed and submitted to Records Management before the "official record" is destroyed. Upon approval, the records will be destroyed and a copy of the certificate of destruction with the Records Disposal Form and Records Disposition Inventory will be sent to the originating office. Maintaining documentation of records disposal complies with administrative rules for state record keeping (13 TAC §6.8). — Department head

3. "Convenience copies" are extra copies of records in addition to the 'official" records contained elsewhere. Convenience copies of records maintained as reading, convenience, tickler, and identical copies maintained with the "official" record are non records if they are maintained only for reference and convenience, and do not contain additional information. General disposal methods may be used for disposing of records of convenience copies not containing confidential or sensitive information. Convenience copies containing confidential or sensitive information must be disposed of in a manner that ensures protection. The convenience copies must also be stored in a secured location until final disposition. Convenience copies must be shredded or sent to Records Management for proper destruction. All convenience copies must be destroyed before, or at the time the official record is destroyed. These copies may not be kept after the "official" record is destroyed according to the retention schedule. — Department head

4.	"In-Active records" should be transferred to Records Management for off-site storage to live out their retention life reducing unnecessary costs. Records must be separated and boxed by department personnel according to record series title and like retention period. A Records Transmittal and Records Transmittal Inventory Form must be completed and sent to Records Management for approval. Upon approval, the records will be barcoded at box and/or file level and entered into the Records Management software for managing records.	Department head
5.	For some records, destruction is not appropriate because there is an ongoing need for the information as historic documentation. The ultimate disposition for these records is archival preservation as identified in the records retention schedule. Records identified as "archival" will be reviewed by the Library. "Vital records" are those records essential to the resumption of business or operations, recreation of an agency's financial or legal position, and the protection of employee and citizen rights. Vital records have been marked with an (X) in the retention schedule. Texas Government Code §441.183 requires each agency head to identify and take adequate steps to protect confidential and vital state records as part of its records management program. It is the responsibility of the department directors, chairs, or other upper management official with vital records to assure that these records are protected through some type of records protection program. Records Management must be contacted to assist management in developing a protection program.	Department head
6.	A "state publication" is defined as information in any format that is produced by the authority of or at the total or partial expense of a state agency or is required to be distributed under law by the agency, and is publicly distributed. These records should be sent to the health science center contact for the Depository Program who is responsible for ensuring that the Texas State Library receives all qualified HSC publications. State publications not specifically exempt from the program must be deposited with the State Library in the following number of copies based upon the number of copies produced or the medium in which it is made available:	Department head

Format	Number of copies produced	Number of copies deposited
Print	300 or more	55
Print	Fewer than 300	4

Electronic format only, must be provided on electronic external storage devices, such but not by the Internet, as diskettes or CD-ROMS.

Electronic format only, must meet state requirements for Internet availability and by Internet connection accessibility by the State Library.
*Special requirements for print publications (13 TAC 3.4):

References and Cross-references.
Federal Requirements
Gramm-Leach-Bliley Act (A "Non-Bank" Application Of The GLBA – Universities)

Health Insurance Portability Accountability Act – HIPAA

Standard: Sarbanes Oxley, Section 802 Criminal Penalties for Altering Documents, Section 1102 Tampering with a Record or Otherwise Impeding an Official Proceeding

Forms and Tools. (optional)
Related Documents

Records Management Manual
* Records Management Policies
* Records Management Procedures
* UNT Health Science Center Records Retention Schedule
Records Management Division Procedures Manual

Approved: 9/3/2002
Effective: 9/3/2002
Revised: 6/25/2007

Policies of the University of North Texas Health Science Center	Chapter 04 – Administration
04.313 Records Authorization	

Policy Statement.
The University of North Texas Health Science Center recognizes, as described in the Texas State Records Management Manual, the statutory responsibility to identify and take adequate steps to protect confidential and vital state records according to Texas Government Code 441.

Application of Policy.
This policy applies to anyone who creates or maintains business records that are either required or would be normally maintained in the regular course of business.

Definitions.
None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. Records and Information Management requires that a Records Management Authorization Form must be completed, signed by a department supervisor, and submitted to Records Management to request records from storage. Without this approval, records will not be released. Records will only be released to the person authorized to request records for that department. The person(s) authorized to receive records are responsible for the return of these records to Records and Information Management.	Department Supervisor
2. An inventory will be sent by Records and Information Management to department managers and supervisors identifying personnel and records checked out to that department by requestor. Any personnel authorized to request records must return all records checked out under their name to Records Management upon leaving that department or the health science center. These records will be checked in by RIM and the records request account will be closed. Please review Records and Information Management Policy and Employee Records Exit Procedures.	Department Supervisor

References and Cross-references.

Statutory Requirements

To the extent applicable reference is made to the following statutes:

Texas Health and Safety Code, Chapter 181 Medical Records Privacy
Gramm-Leach-Bliley Act
Health Insurance Portability Accountability Act – HIPAA
Government Code Chapter 552. Public Information
Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records.
Standard: Sarbanes Oxley, Section 802 Criminal Penalties for Altering Documents, Section 1102 Tampering with a Record or Otherwise Impeding an Official Proceeding

Forms and Tools.

Records Management Manual
* Records Management Policies
* Records Management Procedures
* UNT Health Science Center Records Retention Schedule
Records Management Division Procedures Manual

Approved: 9-3-2002
Effective: 9-3-2002
Revised: 6-25-2007

Policies of the University of North Texas Health Science Center	Chapter 04 – Administration
04.314 Records Management Exit Procedures for Employees	

Policy Statement.
State records may not be removed from government custody and records must be destroyed according to the records retention schedule and records management disposition policy. Employees leaving the health science center must work with their supervisors to identify and reassign before exiting.

Application of Policy.
This policy applies to anyone who creates or maintains business records that are either required or would be normally maintained in the regular course of business.

Definitions.
None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. Records and Information Management Employee Exit Procedures: Prior to an employee leaving the health science center an employee and supervisor should: 1) Identify all state records in that employee's possession. 2) Reassign records to another employee or records management custodian. 3) Return all records requested from Records Management and/or the Records Center. 4) Transfer or backup all state records before wiping the workstation hard drive. A certification should be made that all state records have been identified and transferred to Records Management or reassigned to another employee.	Department supervisor
2. State records may not be removed from government custody and records must be destroyed according to the records retention schedule and records management disposition policy.	Department supervisor

3.	The University of North Texas Health Science Center holds ownership and title to all records and information created, received, acquired, or maintained in the normal course of business by any employee or organizational component. These records are the property of The University of North Texas Health Science Center.	State agency

References and Cross-references.

Statutory Requirements

The University of North Texas Health Science Center recognizes, as described in the Texas State Records Management Manual, the statutory responsibility to identify and take adequate steps to protect confidential and vital state records according to Texas Government Code 441.

Government Code, Chapter 441, Subchapter L, Section 37.10. Tampering With Governmental Record.

Forms and Tools.

Records Management Manual
* Records Management Policies
* Records Management Procedures
* UNT Health Science Center Records Retention Schedule

Records Management Division Procedures Manual

Approved: 8-16-2006
Effective: 8-16-2006
Revised: 4-24-2007

Policies of the University of North Texas Health Science Center	Chapter 04 - Administration
04.315 Legal Holds and Termination of Legal Holds	

Policy Statement.
Information related to a lawsuit, investigation, or audit record preservation is the responsibility of every employee and department. Notification in writing of legal hold and termination of legal holds must be reported to Records and Information Management department.

Application of Policy.
This policy applies to anyone who creates or maintains business records that are either required or would be normally maintained in the regular course of business.

Definitions.
None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. This policy requires Legal Affairs, Internal Audit, Human Resource, Risk Management, Compliance, or any other entity to notify Records and Information Management of the need to preserve information related to a lawsuit, investigation, or audit. The notification must be in writing and signed by the appropriate officer. The Legal Hold should be specific about what records that need to be preserved – records, documents, and drafts (paper or electronic) created in a specific time period that are about a specific business function. Upon receipt of this notice, Records and Information Management will review its record holdings and place a Legal Hold on all records identified.	Legal Affairs, Internal Audit, Human Resource, Risk Management, Compliance, or any other entity
2. This policy requires Legal Affairs, Internal Audit, Human Resource, Risk Management, Compliance, or any other entity to notify Records and Information in writing once the matter is concluded. A Notice of Termination of the Legal Hold must be sent to Records and Information Management indicating that regular keeping rules once again apply.	Legal Affairs, Internal Audit, Human Resource, Risk Management, Compliance, or any other entity

References and Cross-references.
Statutory Requirements

A state record may not be destroyed if any litigation, claim, negotiation, audit, open records request, administrative review, or other action involving the record is initiated *before* the expiration of a retention period for the record set by the commission or in the approved records retention schedule of the agency until the completion of the action and the resolution of all issues that arise from it, or until the expiration of the retention period, whichever is later.

Section 441.187(b), Government Code

Texas Penal Code Section 37.10 TAMPERING WITH GOVERNMENTAL RECORD

Forms and Tools.
Records Management Manual
* Records Management Policies
* Records Management Procedures
* UNT Health Science Center Records Retention Schedule
Records Management Division Procedures Manual

Approved: 8-16-2006
Effective: 8-16-2006
Revised: 4-17-2007

Policies of the University of North Texas Health Science Center	Chapter 04 – Administration
04.316 Archives Program	

Policy Statement.
The University of North Texas Health Science Center recognizes, as described in the Texas State Records Management Manual, the statutory responsibility to identify and accession historical records/materials to an archive.

Application of Policy.
This policy applies to anyone who creates or maintains business records that are either required or would be normally maintained in the regular course of business.

Definitions.
None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. Each business operation, in partnership with Records and Information Management, is responsible for maintaining archived records in a manner as to be identified and retrieved in a timely manner per regulatory, contractual, and business requirements. Each business operation is required to maintain an accurate inventory of records archived. Records are considered archival for two reasons: (1) They provide evidence of agency functions, and/or (2) They contain information that is of enduring value. The records retention schedule identifies records series eligible for review.	Department head

References and Cross-references.
Statutory Requirements

All branches of government at all levels must create certain records to serve as historical documentation of their activities. To identify and maintain these records as part of the archives of the state is the statutory duty of the Texas State Library, Texas Government Code, §441.181.

Section 441.186. Archival State Records are as follows:
(a) The state archivist, through review of state records retention schedules submitted to the state records administrator under Section 441.185 and other means available under this

section, shall identify and designate which state records are archival state records or which state records of potential archival value shall be subject to the review of the state archivist prior to their destruction.

(b) Records management officers shall submit to the state archivist any information concerning a state record that the state archivist considers necessary to determine the archival value of a record.

(c) The state archivist may inspect any state record to determine if the record is an archival state record and the inspection is not a release of a record to a member of the public under Chapter 552.

(d) Archival state records shall be transferred to the custody of the commission when they are no longer needed for the administration of the state agency unless state law requires that the records remain in the custody of the agency.

(e) If the commission cannot accept immediate custody of an archival state record, the record shall remain in the custody of the state agency and shall be preserved in accordance with this subchapter, rules adopted under this subchapter, and other terms on which the director and librarian and the agency head may agree.

(f) Instead of transferring archival state records under this section, the components of university systems and other institutions of higher education may retain and preserve the archival state records of the component or institution in accordance with this subchapter and rules adopted under this subchapter if the records are preserved in an archives established in a library or research center directly controlled by the university.

(g) Except when permitted under state law, an archival state record may not be transferred from one state agency to another without the consent of the director and librarian.

(h) With the approval of the director and librarian, the state archivist may remove the designation of a state record as an archival state record and permit destruction of the record under this subchapter and rules adopted under this subchapter.

(i) In the event of a disagreement between the commission and a state agency over the custody of an archival record, the attorney general shall decide the issue of custody.

(j) In the event of a disagreement between the commission and the attorney general over custody of an archival state record in the possession of the office of the attorney general, the commission may petition a district court in Travis County to decide the issue of custody. On request, the attorney general shall provide the commission with legal counsel to represent the commission in the matter.

Source: Added by Acts 1997, 75th Leg., ch. 873, sec. 1, eff. Sept. 1, 1997.

Forms and Tools.

Related Documents

Records Management Manual

* Records Management Policies
* Records Management Procedures
* UNT Health Science Center Records Retention Schedule

Records Management Division Procedures Manual

Approved: 8-16-2006
Effective: 8-16-2006
Revised: 4-17-2007