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: