WEST TENNESSEE HEALTHCARE
MANAGEMENT GUIDEBOOK POLICY

SUBJECT: Patient and System Confidentiality		**POLICY NO.:** 7577
APPLICATION: System-Wide		**PAGE(s):** 1 of 3 +Attachments
DEPT. RESPONSIBLE: Compliance Office		**EFFECTIVE:** 09/27/93
		REVIEWED:
		REVISED: 01/27/09
APPROVED BY:		
	President/CEO	**Date:**

PURPOSE: To establish a policy for creating awareness of the importance of privacy, security, and confidentiality of all medical and system related information, whether oral, visual, electronic or recorded in any form or medium at West Tennessee Healthcare (WTH) in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations, 45 CFR Parts 160, 162, and 164. This policy applies to both WTH workforce members and non-workforce members.

DEFINITIONS:

- WTH's workforce includes employees, volunteers, trainees, and other persons whose conduct in the performance of work is under the direct control of WTH, whether or not they are paid by WTH.
- Non-workforce members include medical staff members and non-employed clinic staff members that access patient protected health information in the course of their job responsibilities using WTH information systems.

POLICY: All members of WTH's workforce will be educated on HIPAA Privacy and Security compliance and acknowledge that they are generally familiar with the regulations regarding the confidentiality of identity and records of patients of WTH. All members of WTH's workforce will understand and agree that in the performance of duties as an employee, student, other, of WTH, they must hold all medical information in the strictest confidence. Workforce members will certify that any such information of which they become aware in the course of employment/association with WTH is confidential, and they will not disclose any such information which can be associated with the identity of WTH, its staff, its patients, and/or its patient records. Workforce members will understand that the disclosure of such information may give rise to irreparable injury to WTH or to the provider of such information and agree that any violation of the confidentiality of medical or hospital information may result in some form of punitive action ranging from written warning to termination - depending on the nature of the offense. (See Attachment 1)

Furthermore, security and confidentiality are matters of concern for all persons who have access to WTH information systems. Each person accessing WTH data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. Therefore, all persons who are

authorized to access data and resources, both through enterprise information systems and through individual department local area networks and databases, must read and comply with WTH policy.

The Compliance Office will participate in WTH new employee and volunteer orientation to discuss privacy and security of protected health information. The WTH Online Education System will be utilized for mandatory employee training on WTH HIPAA policies and procedures. Department directors will be responsible for enforcing policies and procedures created by WTH.

PROCEDURE:

1. New employee and volunteer orientation will cover general HIPAA awareness. All new employees and volunteers will receive a copy of the WTH Notice of Privacy Practices and Management Guidebook Policy No. 7577, Patient and System Confidentiality. Employees will also receive a copy of the Management Guidebook policy, IS Acceptance Use Policy, Policy No. 3046.
2. In orientation, all new employees and volunteers will sign a Confidentiality Acknowledgement form which will be placed in their Human Resources/Volunteer Services personnel file.
3. New employees will follow up orientation with training on WTH HIPAA policies and procedures through the WTH Online Education System within a reasonable period of time after they join the workforce (approximately 60 days from their hire date).
4. Workforce members whose functions are affected by material changes in WTH HIPAA policies and procedures will be trained within a reasonable period of time after such changes take effect.
5. Ongoing security training will be conducted in response to environmental and operational changes affecting security.
6. Mandatory employee training will be documented and tracked in the WTH Online Education System on a yearly basis. Documentation regarding training for the workforce will be retained for a period of at least six years from the date of its creation or the date when it was last in effect, whichever is later.
7. Non-workforce members will receive the Management Guidebook policies, IS Acceptance Use Policy, Policy No. 3046 and Patient and System Confidentiality, Policy No. 7577. They will sign both acknowledgement forms before receiving access to any WTH information system. The Information Systems Department will maintain these acknowledgement forms.

STANDARDS OF BEHAVIOR: Users of patient information available through WTH information systems will abide by the following basic principles:

1. Respect the privacy and rules governing the use and disclosure of protected health information accessible through the WTH computer system or networks necessary for the delivery of care to patients.
2. Access patient records only for the purposes of treatment, payment, and certain health care operations and only if such access has not been restricted by the patient and such restriction agreed to by WTH.
3. Expect for purpose of treatment, agree to limit access to patient information to the minimum necessary to accomplish the intended purpose of the use or disclosure.
4. Do not exhibit or divulge the contents of any patient record or report, except in the course of delivery of care to patients, and then only to those who are authorized to receive it.

5. Follow acceptable use/security policies to ensure that patient information is safeguarded and protected.
6. Do not knowingly include or cause to be included in any patient record or report, a false, inaccurate, or misleading entry.
7. Respect the confidentiality of all patient records or reports that are printed from WTH information systems and handle, store, and dispose of these reports in a manner that protects patient confidentiality.
8. Recognize that the information accessed through all WTH information systems contains patient information that is confidential and, in some instances, may be sensitive and should only be used in the delivery of care to the patient and should never be disclosed to individuals not authorized to receive it.
9. Do not seek personal benefit or permit others in your control such as family members, employees, or agents to benefit personally by the use or disclosure of confidential information.
10. Respect the policies and procedures established by WTH to manage the use of the information systems.
11. Prevent unauthorized use and disclosure of any information in files maintained, stored or processed by WTH.
12. Do not release assigned authentication codes, passwords, or devices to anyone else, or allow anyone else to access or alter information contained on the WTH information system under user's identity.
13. Do not utilize anyone else's authentication code, password, or device in order to access information contained on any WTH system
14. Recognize that all access to information contained on WTH information systems will be monitored by WTH.
15. Report any unauthorized access and/or violation of this policy to the WTH privacy coordinator or information security manager.
16. Understand that obligations to maintain the privacy and security of patient information will continue after termination of employment and/or medical staff membership. Understand that privileges to access and use the WTH information system are subject to periodic review, revision, and if appropriate, relinquishment.

Those who cannot accept these standards of behavior may be denied access to the WTH information systems and networks. Violators also may be subject to penalties, including disciplinary action under policies of WTH, Medical Staff Rule and Regulations and under laws of the State of Tennessee and under federal laws, to the extent applicable.

LEVEL	CAUSE OR MOTIVATION	TYPE OF VIOLATION	SANCTION ACTIVITY	EXAMPLES
Level I	§ Lack of training § Inexperience § Accidental	§ Clerical error § Technical error § Judgment error	§ Training § Counseling § "Three strikes" model	§ PHI left on copier or fax § Unopened mail left unattended § E-mail address error § Protected health information (PHI) sent to similarly named patient § PHI in conversation overheard § Desk or work area left unsecured § Computer files erased § PHI found in trash/document not placed in document destruction bin or shredded § Computer screen left unattended/failure to sign off computer
Level II	§ Curiosity § Concern § Compassion	§ Unauthorized § Not job-related § Disregard of organizational policy § Repeated Level I offense	§ Documentation: – Warning – Counseling § Administrative leave without pay § Probationary period (another violation in a stated time period will result in more severe sanction, such as leave without pay) § Corrective action plan (CAP)	§ Accessing patient information without a legitimate reason § Releasing PHI inappropriately per policy, state, and/or federal law § Copying information as a favor § Installing software § Experimenting with computer § Using someone else's password or sharing personal access codes (providing PHI access to someone else) § Deleting information from network
Level III	§ Malicious intent § Financial gain § Disgruntled	§ Theft § Maliciousness § Repeated Level II offense	§ Termination	§ Selling PHI § E-broadcasting patient info § Intentionally destroying or altering PHI § Intentionally accessing and releasing PHI for own interest or personal gain § Releasing PHI with the intent to harm the individual or the organization § Repeated malicious disregard of organizational policy

SAMPLE COPY (Print from Public Folders, Human Resources folder) Attachment 2

BARCODE

Confidentiality Acknowledgement

Name (Printed) Employee Number (if WTH employee)

West Tennessee Healthcare is dedicated to protecting the confidentiality of its patients and maintaining a high level of security to all who have access to West Tennessee Healthcare information systems. It is your responsibility as an employee, student, volunteer or other position with West Tennessee Healthcare to continue this standard. By signing this form, you acknowledge the following:

* I have received a copy of Policy No. 7577—Patient and System Confidentiality.
* I have read or had the Patient and System Confidentiality policy explained to me.
* I understand and agree to comply with the policy.
* I understand that if I fail to adhere to these policies, I may be subject to disciplinary action, up to and including termination depending upon the nature of the offense, as determined by management.

Signature Department or Facility Name

Position Title Date