Purpose: All UT Health Science Center employees, volunteers, contractors and any other person given access to UTHSC information systems and/or protected health information must comply with all security and privacy policies. This policy defines security violations and addresses a formal process to be followed in the event a security violation has been identified. This policy is in compliance with HIPAA – Sec. 164.530 (e)(1-2).

Scope: This policy applies to paper and electronic documents and systems and verbal communication. UTHSC's policies established to promote proper privacy and security measures should be followed. Any violations of those policies will be handled following the steps outlined in this policy. All confidential patient and business information must remain confidential and private.

Policy: Staff, students, faculty, volunteers, contractors and any other person given access to UT Health Science Center's information systems and/or protected health information will be held responsible for any transaction(s) associated with their access and will be held accountable for any security or privacy violation. Any staff, faculty, volunteer, vendor, student or business associate who breaches confidentiality is subject to disciplinary action up to and including immediate termination.

A. Information Systems Auditing. Information Systems Department will conduct internal audits of system activity maintained by UTHSC. System activity may include file login access by patient or by employee, security incidents or investigations. Any findings from audits will be reported to the employees' supervisor on the attached Security Violation Response Form. It will be the supervisor's responsibility to follow up on the potential incidents.

B. Reporting Security and Privacy Access Violations. UTHSC's Privacy Officer should be notified of suspected security and privacy violations. Staff, students, faculty and patients may report the issue informally by contacting the privacy officer. The privacy officer will work thru the incident and verify the extent of the violation according to UTHSC Compliance Program guidelines.

C. Security Violation Levels. Security violations have been categorized in severity levels for use as a guideline to supervisors. They are defined below as follows:

Security Violation Level I **-** Represents a minor violation that is accidental, non malicious in nature, and/or due to lack of proper training.

Level I violation may include, but are not limited to:

1. Code (Password) Sharing

    a. Giving his/her access code (password) to another person.
    b. Signing on and allowing another person to use his/her code.
    c. Failing to sign off a given computer terminal.

2. Accessing his or her own record without following the proper process for completing an authorization.

3. Requesting another co-worker to access his or her own record without following the proper process for completing an authorization.

Security Violation Level II **-** Represents a moderate violation in which the intent of the violation is unclear and the evidence cannot be clearly substantiated as to malicious intent.

Level II violation may include, but are not limited to:

1. Accessing a record of a patient without a legitimate reason. This includes accessing a co-worker, friend, spouse, child of legal age, neighbor, etc.

2. Using another co-worker's access code without the co-worker's authorization.

3. Releasing patient data inappropriately.

Security Violation Level III **-** Represents a severe violation in which the employee purposefully breaks the terms of the Acknowledgement of Information Systems Usage Form and/or UT Health Science Center policies, in which evidence clearly establishes malicious intent and/or which there have been an unacceptable number of previous violations.

Level III violation may include, but are not limited to:

1. Releasing data for personal gain.

2. Destroying or falsely altering data intentionally.

3. Releasing data with the intent to harm an individual or the organization.

D. Corrective Action

1. Any employee found by UTHSC to have violated the policy will be subject to appropriate disciplinary actions, up to and including immediate termination.

2. It is the responsibility of the employee's direct supervisor in conjunction with Human Resources to take corrective action for each security violation. The violation and the action(s) taken by the supervisor or department head must be communicated back to UT Health Science Center Privacy Officer within five working days after identification of the security violation. The form "Security Violation Response", Attachment A, will be used as communication tools for follow up of potential security violations.

Security / Privacy Violation Response
UT Health Science Center

Type: (Circle one) Audit Other_____

Patient medical record and account number:_____

Employee involved: _____

Department:_____

Incident description:_____

_____

_____

_____

_____

Reason for access of record:_____

_____

_____

_____

_____

_____

_____

Action taken:

? **Disciplinary Action Taken**
? **No Action Taken (Explain briefly below.)**
? **Security / Privacy Violation could not be validated.**

Explain:

_____

Supervisor's signature:_____**Date:**_____

******Please route this form to the Privacy Officer**

Attachment A