TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER™

Security Manual for

Protected Health Information

Revised September 2011

Contents

PREFACE 4

TTUHSC Operating Policy Regarding Privacy and Security 5

1. DEFINITIONS: 6

2. ADMINISTRATIVE SAFEGUARDS 45 CFR 164.308 12

2.1 TTUHSC Information Security Officer 45 CFR 164.308(a)(2) 12

2.2 HIPAA Security Compliance Committee 13

2.3 Human Resources Department 13

2.4 Security Management Process 45 CFR 164.308(a)(1)(i)-(ii) 13

2.4.1 Risk Analysis 45 CFR 164.308(a)(1)(ii)(A) 13

2.4.2 Risk Management 45 CFR 164.308(a)(1)(ii)(B) 14

2.4.3 Information System Activity Review 45 CFR 164.308(a)(1)(ii)(D), 45 CFR 164.312(b) 17

2.4.4 System Evaluation 45 CFR 164.308(a)(8) 18

2.5 Workforce Security 45 CFR 164.308(a)(3)(i) 19

2.5.1 Authorization and Supervision 45 CFR 164.308 (a)(3)(ii)(A) 19

2.5.2 Workforce Clearance Procedure 45 CFR 164.308(a)(3)(ii)(B) 20

2.5.3 Workforce Termination Procedure 45 CFR 164.308(a)(3)(ii)(C) 21

2.6 Information Access Management 45 CFR 164.308(a)(4)(i) 22

2.7 Reporting, Disciplinary Action, and Sanction Policy 45 CFR 164.308(a)(1)(ii)(C) 23

2.8 Security Awareness, Training, and Reminders 45 CFR 164.308(a)(5) 24

2.8.1 Training 24

2.8.2 Reminders 45 CFR 164.308(a)(5)(ii)(A) 24

2.8.3 Other Security Awareness 25

2.9 Security Incident Procedures 45 CFR 164.308(a)(6)(i) 25

2.10 Contingency Plans - 45 CFR 164.308(a)(7)(i) 26

2.10.1 Emergency Mode Operations And Access Procedures 45 CFR 164.308(a)(7)(ii)(C), 45 CFR 164.312(a)(2)(ii) 26

2.10.2 Data Backup 45 CFR 164.308(a)(7)(ii)(A) 26

2.10.3 Testing and Revision Procedure 26

2.10.4 Application and Data Criticality Analysis 26

2.11 Business Associate Contracts and Other Arrangements - 45 CFR 164.308(b)(1) 27

2.12 Documentation 45 CFR 164.316(b) 27

3. PHYSICAL SAFEGUARDS 45 CFR 164.310 28
3.1 Facility Access Controls 45 CFR 164.310(a)(1) 28
3.1.1 Facility Security Plan 45 CFR 164.310(a)(2)(ii) 29
3.1.2 Access Control and Validation 45 CFR 164.310(a)(2)(iii) 29
3.2 Workstation Use and Security 45 CFR 164.310(b), 45 CFR 164.310(c) 30
3.3 Device and Media Controls – 45 CFR 164.310(d)(1) 31
4. TECHNICAL SAFEGUARDS 45 CFR 164.312 34
4.1 Access Control 45 CFR 164.312(a)(1) 34
4.1.1 Unique User Identification 45 CFR 164.312(a)(2)(i) 34
4.1.2 Emergency Access Procedure 45 CFR 164.312(a)(2)(ii) 35
4.1.3 Automatic Logoff 45 CFR 164.312(a)(2)(iii) 35
4.1.4 Encryption And Decryption 45 CFR 164.312(a)(2)(iv) 35
4.2 Audit Controls 45 CFR 164.312(b) 36
4.3 Integrity 45 CFR 164.312(c)(1) 36
4.4 Person or Entity Authentication 45 CFR 164.312(d) 36
4.5 Transmission Security 45 CFR 164.312(e)(1) 37
4.51 Data Integrity Controls 45 CFR 164.312(e)(2)(i) 37
4.52 Encryption 45 CFR 164.312(2)(ii) 38

PREFACE

The Health Insurance Portability and Accountability Act of 1996 established national standards for the security and privacy of electronic protected health information. The Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, published in the Federal Register on February 20, 2003 (Volume 68, No. 34, page 8333) specifies a series of administrative, technical, and physical security safeguards and organizational requirements with which certain entities involved in health care must comply to secure the privacy and confidentiality of their electronic protected health information.

The Security Rule requirements are organized into three categories: administrative safeguards, technical safeguards, and physical safeguards. Within these three categories, there are 18 security standards, with implementation specifications identified as either "required" or "addressable."

The Administrative Safeguards category makes up 50% of the Security Rule's standards. These require documented policies and procedures for managing day-to-day operations; the conduct and access of workforce members to electronic protected health information; and the selection, development, and use of security controls.

The Physical Safeguards are a series of requirements meant to protect a covered entity's electronic information systems and electronic protected health information from unauthorized physical access.

Technical Safeguards outline the use of technology to protect electronic protected health information, particularly controlling access to it.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act or "The Act") is part of the American Recovery and Reinvestment Act of 2009 (ARRA). The primary impacts involving HIPAA Security Policies are breach notification procedures and stricter requirements for Business Associates.

Texas Tech University Health Sciences Center (TTUHSC) is committed to compliance with HIPAA and its accompanying regulations, as stated in HSC OP 52.02, Health Insurance Portability and Accountability Act.

TTUHSC Operating Policy Regarding Privacy and Security

The purpose of this Operating Policy and Procedure (HSC OP) is to provide a framework for Texas Tech University Health Sciences Center's (TTUHSC) compliance with the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and state laws and regulations for the privacy and security of health information. Responsibilities of workforce members, institutional officers and the HIPAA Privacy and Security Committee are identified. For more information, see the actual policy.

HSC OP 52.02 Privacy and Security of Health Information

1. DEFINITIONS:

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. 45 CFR 164.304

Administrative Safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of TTUHSC's workforce in relation to the protection of that information. 45 CFR 164.304

Anti-Virus Software means software that detects or prevents malicious software.

Authorize means to give a right or authority to act.

Authentication means the corroboration that a person or entity is the one claimed. 45 CFR 164.304

Availability means the property that data or information is accessible and useable upon demand by an authorized person. 45 CFR 164.304

Backup means creating a retrievable, exact copy of data including electronic protected health information, or a procedure to restore loss of data. 45 CFR 164.308(a)(7)(ii)(A)

Biometric Identification system means a system in which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures.

Business Associate, 45 CFR Part 160.103 (According to Office of Civil Rights (OCR) guidance printed December 3, 2002), means a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, TTUHSC.

- A member of TTUHSC's workforce is not a business associate.
- Business Associate functions include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.
- Business Associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

A non-inclusive list of Business Associates includes lawyers, auditors, consultants, contractors, clearinghouses, third-party administrators, and life insurance issuers.

Checksum means a count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received. This number can be regularly verified to ensure that the data has not been improperly altered.

Chief Information Officer (CIO) means a member of an institution's executive management staff responsible for the overall information technology and computer systems that support enterprise goals.

Code of Federal Regulations (CFR) means the codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government.

Confidentiality, 45 CFR Part 164.304, means the property that data or information is not made available or disclosed to unauthorized persons or processes. In other words, as used herein, confidentiality is when protected health information is not made available or disclosed to those persons or processes unauthorized to receive such information under federal or state law.

Covered Entity, 45 CFR Parts 160.102 and 160.103, means:

- A health plan.
- A health care clearinghouse.
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

Cryptography means encrypting ordinary text into undecipherable text then decrypting the text back into ordinary text.

Cryptographic Key means a variable value that is applied using an algorithm to data to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the data.

Data User - see User.

Digital Signature means a cryptographic code that is attached to a piece of data. This code can be regularly verified to confirm that the data has not been improperly altered.

Disaster means an event that causes harm or damage to TTUHSC information systems. Disasters include but are not limited to: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.

Electronic Communications Network means any series of nodes interconnected by communication paths that is outside the TTUHSC network (e.g., the Internet). Such networks may interconnect with other networks or contain sub networks.

Electronic Media means: 45 CFR 160.103

1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased

lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, voice, and telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic Protected Health Information (EPHI) means individually identifiable health information that is transmitted by electronic media, or maintained in electronic media. 45 CFR 160.103

Emergency means a crisis situation.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. To read encrypted data, a person must have access to a secret key or password that enables them to decrypt (decode) the data. 45 CFR 164.304

Erase Tool means hardware or software that is capable of completely removing all recorded material from electronic media.

Facility means the physical premises and the interior and exterior of a building(s). 45 CFR 164.304

Hash (or Hash Value) means a number generated from a string of text. A sender of data generates a hash of the message, encrypts it, and sends it with the message itself. The recipient of the data then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they are the same, there is a very high probability that the message was transmitted intact.

Health Care Component, 45 CFR Part 164.103, means a component or combination of components of a hybrid entity designated by the hybrid entity.
The component or combination of components includes the following:

- Any component of the covered entity that engages in covered functions;
- Any component that engages in activities that would make such component a business associate of a component that performs covered functions, if the two components were legal entities; or
- Any component that would meet the definition of covered entity if it were a separate legal entity.

Hybrid Entity means a single legal entity that is a covered entity, whose business activities include both covered and non-covered functions, and that designates health care components. 45 CFR 164.103

Individually Identifiable Health Information, 45 CFR Part 160.103, means health information collected from an individual that is created or received by a health care provider, a health plan, a health care clearing house or an employer and that does all of the following:

- Involves the past, present, or future physical or mental health, or condition of an individual; the providing of health care to an individual; or the past, present or future payment for the providing of health care to an individual; and
- Identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

Information Security Officer is the individual designated by the Chief Information Officer to be responsible for the development and implementation of security policies and procedures as required by the HIPAA Security rule as well as for the overall security processes of TTUHSC.

Information System means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. 45 CFR 164.304

Information Systems Owner means TTUHSC and its workforce designee with overall or final responsibility for an information system.

Integrity means the property that data or information has not been altered or destroyed in an unauthorized manner. 45 CFR 164.304

Malicious Code means an executable application (e.g. Java applet or Active X control) designed to damage or disrupt an information system.

Malicious Software means software, for example, a virus, designed to damage or disrupt an information system. 45 CFR 164.304

Message Authentication Code means a one-way hash of a message that is then appended to the message. This is used to verify that the message is not altered between the time the hash is appended and the time it is tested.

Password means confidential authentication information composed of a string of characters. 45 CFR 164.304

Physical Safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. 45 CFR 164.304

Protected Health Information (PHI), (PHI) 45 CFR Part 160.103, means individually identifiable health information maintained or transmitted by TTUHSC or any other covered entity in any form or medium, including information transmitted orally, or in written or electronic form. Except as otherwise permitted or required herein, TTUHSC may not use or disclose PHI without a valid Authorization that meets the elements set forth herein.
Examples of PHI include, but are not limited to, information regarding the name of the attending physician(s) for an individual and the fact that an individual has ever attended a clinic, or is presently attending a clinic.
PHI does NOT include employment records held by TTUHSC in its role as employer or education records covered by the Family Educational Rights and Privacy Act (FERPA).

Restoration means the retrieval of files previously backed up and returning them to the condition they were at the time of backup.

Re-use means the use of electronic media containing EPHI for something other than its original purpose.

Risk means the likelihood that a specific threat will exploit a certain vulnerability, and the resulting impact of that event.

Risk Analysis means a systematic and analytical approach that identifies and assesses risks to the confidentiality, integrity or availability of a covered entity's EPHI. Risk analysis considers all relevant losses that would be expected if specific security measures protecting EPHI are not in place. Relevant losses include losses caused by unauthorized use and disclosure of EPHI and loss of data integrity. 45 CFR 164.308(a)(1)(A)

Security Token System means a system in which a small hardware device along with a secret code (e.g. password or PIN) is used to authorize access to an information system.

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. 45 CFR 164.304

Security or Security Measures encompass all of the administrative, physical, and technical safeguards in an information system. 45 CFR 164.304

Technical Safeguards mean the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45 CFR 164.304

Token means a physical device which, together with something that a user knows, will enable authorized access to an information system.

Trojan Horse means a program in which malicious or harmful code is contained inside apparently harmless programming or data.

User means a person or entity with authorized access to information systems. 45 CFR 164.304

Virus means a piece of code, typically disguised, that causes an unexpected and often undesirable event. Viruses are frequently designed to automatically spread to other computers. They can be transmitted by numerous methods: as e-mail attachments, as downloads, and on floppy disks or CDs.

Workforce, 45 CFR Part 160.103, means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. 45 CFR 164.304

Worm means a piece of code, usually disguised, that spreads itself by attacking and copying itself to other machines. Some worms carry destructive payloads that delete files or distribute files; others alter Web pages or launch denial of service attacks.

Terms used in this Manual, and not otherwise defined in this section, shall have the meaning as those terms are defined by HIPAA, state law, or institutional policy - whichever provides the greater protection for the individual.

2. ADMINISTRATIVE SAFEGUARDS 45 CFR 164.308

2.1 TTUHSC Information Security Officer 45 CFR 164.308(a)(2)

The TTUHSC Chief Information Officer (CIO) shall designate a TTUHSC Information Security Officer (ISO). The TTUHSC Information Security Officer is responsible for protecting the confidentiality, integrity, and availability of TTUHSC information systems and EPHI, as well as promoting TTUHSC information systems compliance with applicable federal and state laws and regulations.

Under the supervision of the CIO, the TTUHSC Information Security Officer is responsible for:

- conducting evaluations to avoid a TTUHSC information system from compromising the confidentiality, integrity, or availability of any other TTUHSC information systems;
- developing, documenting, and disseminating security policies, procedures, and standards for authorized users of TTUHSC information systems and the data contained therein (in conjunction with information system owners);
- coordinating the selection, implementation, and administration of TTUHSC security controls;
- organizing regular TTUHSC security awareness and training; and
- coordinating with TTUHSC's Institutional Privacy Officer and the HIPAA Committee to support compliance with security policies, procedures, and controls found in the HIPAA Privacy Rule.

The TTUHSC Information Security Officer, with input from the Institutional Privacy Officer, is responsible for:

- reviewing the TTUHSC HIPAA Security Policy Manual on an annual basis and, in accordance with Institutional policies, updating the Manual as necessary. The Information Security Officer shall also make these policies and procedures readily available for all workforce members, including business associates and any third party individuals;
- developing and implementing policies and procedures necessary to appropriately protect the confidentiality, integrity, or availability of any other TTUHSC information systems; and
- overseeing that adequate physical security controls exists to protect TTUHSC's EPHI by implementing a risk management process and conducting periodic risk analysis.

2.2 HIPAA Privacy and Security Committee

TTUHSC has created and will maintain a HIPAA Committee, which is responsible for HIPAA Privacy and Security policies and oversight and is chaired by the Institutional Privacy Officer (IPO). These responsibilities are detailed in HSC OP 52.02.

In further support of the regulations issued through the HITECH act, the HIPAA Committee, in conjunction with the Information Security Officer and the Institutional Privacy Officer will develop and maintain a Breach Notification Process to be used in the event of an unauthorized disclosure of EPHI.

2.3 Human Resources Department

The Assistant Vice President for Human Resources is responsible for TTUHSC policies that require appropriate clearance and training before a workforce member is allowed access to TTUHSC information systems containing EPHI. These responsibilities are stated in TTUHSC OP 70.20 - Employment Background Screening Policy.

2.4 Security Management Process 45 CFR 164.308(a)(1)(i)-(ii)

To protect the confidentiality, integrity, and availability of its information systems containing EPHI, TTUHSC shall implement appropriate and reasonable policies, procedures, and controls to prevent, detect, contain, and correct security violations.

TTUHSC's security management process outlines the steps to safeguard the TTUHSC's EPHI and is based on formal and regular risk analysis management.

2.4.1 Risk Analysis 45 CFR 164.308(a)(1)(ii)(A)

TTUHSC shall review, identify, define, and prioritize risks to the confidentiality, integrity, and availability of its information systems containing EPHI on an on-going basis. The risk analysis shall consider the following factors:

- the importance of the applications operating on the information systems;
- the value or sensitivity of the data on the information systems; and
- the extent to which the information systems are connected to other information systems.

The risk assessments are conducted annually on all identified servers and databases that contain PHI. The risk management tool will be reset annually to open the system to all departments to enter new risk assessment data.

- First time users will require additional time to enter their data.
- Returning users will be required to review and update their data.

The risk assessment process is as follows:

a. Information Owner documents current state to assess information security (asset) on an annual basis or as needed. A compliance report is generated at the completion of the assessment and contains detailed information about security risks.

b. The Security and Infrastructure Assurance (SIA) department conducts a validation review of the compliance report. The compiled data will be presented in an annual report and given to Executive Management, which includes Chief Information Officer, PEC, Internal Audit, and General Council. Summary information will also be provided to the HIPAA Committee

c. Risk review is conducted by the information owner and Security and Infrastructure Assurance (SIA) to define the risks and review the overall state of the asset. The information owner needs to either accept the risk and document acceptance of the risk or take corrective actions to mitigate the risk.

d. Acceptable risks are agreed to by the information owner, Executive Management and General Council. Signatures are required on the risk assessment report.

e. Corrective Action begins with analyzing risk factors. This is conducted by the information owner, information custodian, information user, and SIA.

f. A Remediation Plan is developed by the information owner, information custodian, information user, and SIA.

g. The Remediation Plan is implemented the by information owner, information custodian, information user, and SIA.

h. Once the corrective action process is complete, the data is updated in the ISAAC-s and the current state is re-evaluated and the cycle is repeated until the risks are accepted.

2.4.2 Risk Management 45 CFR 164.308(a)(1)(ii)(B)

TTUHSC shall implement security measures that reduce the risks to its information systems containing EPHI. Selection and implementation of security measures shall be based on the on-going risk analysis and monitoring, and the formal annual risk assessment report from the Security and Infrastructure Assurance team. (See Appendix A for a sample risk analysis checklist.)

2.4.2.1 Approved Information Systems and Electronic Media

The Chief Information Officer and the HIPAA Committee are responsible for designating approved information systems and electronic media. TTUHSC workforce members shall use only TTUHSC approved information systems and electronic media to store EPHI.

Transfer or storage of TTUHSC EPHI on personal/home computers or other electronic media is not authorized. Requests for exceptions must be presented in writing to the information systems owner for approval. These exceptions will be considered acceptable risks by the Information Owner or their delegate and must be documented in their annual risk assessment.

Workforce members who move electronic media or information systems containing EPHI must adhere to HSC OP 56.04, Electronic Transmission of Personally Identifiable Information (PII) and Protected Health Information (PHI).

2.4.2.2 Tracking and Logging of EPHI

Each information systems owner is responsible for tracking and logging movement of EPHI through TTUHSC information systems and electronic media in his/her assigned area, into and out of TTUHSC facilities. This responsibility includes tracking and logging both EPHI received by TTUHSC and created within TTUHSC.

Tracking and logging shall include the following information:

- date and time EPHI received;
- brief description of electronic media or information systems containing EPHI;
- name of person(s) receiving EPHI;
- date and time of the previous successful log-in;
- date and time of unsuccessful log-in;
- date and time of revision;
- identification of workforce member logged-in; and
- number of unsuccessful log-in attempts.

Tracking and logging records shall be maintained a minimum of two weeks from the date of creation by the information systems owner or designee.

2.4.2.3 Information Systems Owner

Information systems owners have overall authority for information systems and electronic media in their assigned areas. The security management responsibilities of information systems owners include but are not limited to:

- monitoring appropriate access to the EPHI;
- promoting TTUHSC security training and awareness for workforce members;
- coordinating identification of TTUHSC data processing assets; and
- confirming data backup integrity for TTUHSC information systems containing EPHI.

2.4.2.4 Data User

Users are responsible for creating or using data that is stored in TTUHSC's information systems in their assigned areas. For security management purposes, data users are responsible for maintaining the confidentiality, integrity, and availability of EPHI data as follows:

- knowing the scope of data for which each is responsible;
- reviewing and complying with security policies, procedures, and controls for the EPHI as applicable to the data creation and processing services functions;
- using TTUHSC data processing resources only for intended purposes;
- complying with all appropriate TTUHSC security policies, procedures and standards;
- promptly reporting security violations and/or inappropriate use of data processing resources and risks to the EPHI to the information systems owner and/or the Information Security & Privacy Officer;
- assisting with investigation of violations, as requested;
- maintain confidentiality of all data processed, handled, or seen in the performance of job duties;
- as appropriate, supervising workforce members performing maintenance activities on TTUHSC information systems containing EPHI;
- attending appropriate TTUHSC security training and awareness;
- not attempting to gain access to TTUHSC information systems containing EPHI if proper authorization has not been granted; and
- not providing access to TTUHSC information systems containing EPHI to unauthorized persons.

2.4.3 Information System Activity Review 45 CFR 164.308(a)(1)(ii)(D), 45 CFR 164.312(b)

a. Records of activity created by audit mechanisms implemented on TTUHSC information systems must be reviewed at least monthly by the information systems owner or their delegate. More frequent reviews may be required as determined by TTUHSC's risk analysis. A written report shall be generated and submitted to the Information Security & Privacy Officers by the information systems owner, as requested. Summary information may be provided to the HIPAA Committee as needed. Items to be included in the activity review report are:

   - definition of which activity is significant;
   - definition of which activity records need to be archived and for what period of time;
   - procedures defining how significant activity will be identified and reported; and
   - procedures for preserving records of significant activity.

   Records of activity may include but are not limited to:

   - audit logs;
   - access reports; and
   - security incident tracking reports.

b. Hardware, software, or procedural auditing mechanisms shall be maintained on TTUHSC information systems that contain or use EPHI. Such mechanisms must provide the following information:

   - date and time of activity;
   - origin of activity;
   - identification of user performing activity; and
   - description of attempted or completed activity.

c. The level and type of auditing mechanisms to be implemented on TTUHSC information systems that contain or use EPHI shall be determined by TTUHSC's risk analysis process. Auditable events can include but are not limited to:

   - access of sensitive data;

- use of audit software programs or utilities;
- use of a privileged account;
- information systems start-up or stop;
- failed authentication attempts; and
- security incidents.

TTUHSC workforce members shall not monitor or review activity related to their own user account.

2.4.4 System Evaluation 45 CFR 164.308(a)(8)

The Information Security Officer, or designee, shall oversee a technical and non-technical system evaluation of TTUHSC security controls and processes and in writing document compliance with TTUHSC security policies and the HIPAA Security Rule. The Office of Audit Services may also conduct an evaluation in its sole discretion.

a. Annually. A system security evaluation shall occur at least annually by the Information Security Officer. The annual system security evaluation shall include but is not limited to:

    - detailed review of TTUHSC's security policies, procedures and standards to determine whether they are effective and appropriate.
    - gap analysis of the requirements of TTUHSC's security policies, procedures and standards and actual practices.
    - identification of the risks to TTUHSC information systems.
    - assessment of the appropriateness of TTUHSC security controls compared to the risks to TTUHSC information systems.
    - testing of all significant TTUHSC security controls to ensure that hardware and software controls have been correctly implemented. Such testing must be carried out only by authorized and appropriately trained persons.

b. Environmental or Operational Changes. If an environmental or operational change occurs which significantly impacts the confidentiality, integrity, or availability of TTUHSC EPHI, as determined by the Information Security Officer, the Information Security Officer shall conduct a technical and non-technical evaluation of the affected areas. Such changes include but are not limited to:

    - significant security incidents to TTUHSC information systems;
    - significant new threats or risks to TTUHSC information systems;

- significant changes to the organizational or technical infrastructure of TTUHSC; and
- significant changes to TTUHSC information security requirements or responsibilities.

Evaluations in response to environmental or operational changes must at a minimum include:

- detailed review of TTUHSC's security policies, procedures and standards to determine whether they are still effective and appropriate.
- identification of the risks to TTUHSC information systems after the environmental or operational changes.
- assessment of the appropriateness of TTUHSC security controls compared to the risks to TTUHSC information systems.
- testing of all TTUHSC security controls affected by the changes to ensure that hardware and software controls remain correctly and appropriately implemented.

c. Evaluation criteria and results of all system evaluations shall be documented by the Information Security Officer and presented to the TTUHSC HIPAA Committee and the CIO. This documentation must be maintained by the Information Security Officer in a secure and confidential location.

2.5 Workforce Security 45 CFR 164.308(a)(3)(i)

TTUHSC is committed to protecting the confidentiality, integrity, and availability of its information systems containing EPHI by preventing unauthorized access while providing access to properly authorized and trained workforce members.

Only trained TTUHSC workforce members having a legitimate need for specific information in order to accomplish their assigned job responsibilities shall be granted access to a TTUHSC information system. The supervisor of those individuals who are granted access is responsible for monitoring through tracking and logging that access is appropriately used. See also Section 2.4.2.2. 45 CFR 164.308(3)(ii)(A)

Access to TTUHSC information systems containing EPHI shall only be initiated in accordance with Section 2.6 - Information Access Management.

2.5.1 Authorization and Supervision 45 CFR 164.308 (a)(3)(ii)(A)

TTUHSC workforce members who need direct access to TTUHSC information systems containing EPHI to accomplish his/her legitimate job duties or responsibilities shall obtain access authorization under Section 2.6, Information Access Management before

accessing TTUHSC information systems containing EPHI. TTUHSC workforce, such as maintenance or operational workers, who work in locations where EPHI might be accessed, and who do not need direct access EPHI to accomplish his/her legitimate job duties or responsibilities, shall be supervised by an individual physically present with authority for the area being accessed.

2.5.2 Workforce Clearance Procedure 45 CFR 164.308(a)(3)(ii)(B)

a. Background Checks

All new faculty, staff and volunteer positions at TTUHSC are required to have a employment background check as referenced in HSC OP 70.20.

b. Employment Decisions

In making a final decision about employment of individuals whose duties require access to TTUHSC information systems containing EPHI, the following shall be considered, at a minimum, by the hiring department:

- check prior employment references;
- confirm claimed academic and professional qualifications;
- professional license validation;
- results of criminal background check;
- Criminal registry lists;
- Healthcare sanctions lists – OIG, HHS Medicare/Medicaid Exclusion Lists, other state and federal lists related to healthcare; and
- Government Contractor Debarment list.

c. Position Description

When defining a position, the TTUHSC Human Resources Department and the hiring supervisor shall identify the security responsibilities and supervision required for the position. Security responsibilities include general responsibilities for implementing or maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of TTUHSC information systems or processes.

d. Recruiting Agency

When job candidates are provided via an agency, TTUHSC's contract with the agency must clearly state the agency's responsibilities for reviewing the candidates' backgrounds.

e. Third Party Contracts

Each TTUHSC department that initiates contracts for services of a third party is responsible for verifying that the third party has executed a Business Associate (BA) agreement or otherwise entered into an authorized arrangement before EPHI is accessed. See Section 2.13 regarding Business Associate Agreements and Other Arrangements for more information.

f. Confidentiality Statement

Each TTUHSC workforce member who is authorized to access TTUHSC information systems containing EPHI must sign a confidentiality agreement. The confidentiality statement shall affirmatively set forth the individual's responsibility for protecting confidentiality, integrity, or availability of TTUHSC information systems and processes, and possible sanctions for a violation. Further details and information can be found in HSC OP 52.09

2.5.3 Workforce Termination Procedure 45 CFR 164.308(a)(3)(ii)(C)

a. HSC OP 70.19, Exit Interview and Separation Checkout Procedures, is TTUHSC's policy that specifies the procedures for faculty and staff that must be followed when a termination occurs. The completed Separation Checkout Procedure form (appendix C of OP 70.19) must be returned to the Human Resources Department at the separating employee's location. The checkout document will serve as the receipt during the checkout process and log of action(s) taken, including the following:

- disable and remove the individual's information systems access, both internal and remote. This may include, but is not limited to, access to workstation and server access, data access, network access, email accounts, inclusion on bulk e-mail lists, as well as physical access to areas where EPHI is located;
- deactivate or change all physical security access codes used to protect TTUHSC information systems that are known by a departing workforce member. (For example, the PIN to a keypad lock that restricts entry to a TTUHSC facility containing information systems with EPHI must be changed if a workforce member who knows the PIN departs.); and
- review files on the individual's computer to determine appropriate transfer or disposal of any confidential information.

b. During the process of terminating the employment of a TTUHSC workforce member, the immediate supervisor shall give notice to the relevant information systems

owners and the Information Security Officer, or designee, both of whom are responsible to immediately do or delegate the following:

- The Human Resources Department shall notify the Information Technology Division immediately if an Employee Separation From Employment action is received but the employee failed to complete the checkout process. In which case, the IT Division will immediately disable the former employee's access to any information systems.

- If a departing employee poses a risk to information or systems at TTUHSC as determined by the employee's supervisor and the information systems owner, and/or an individual is to be terminated immediately, the individual's information systems access must be removed or disabled prior to notifying the individual of termination.

- A workforce member who separates from TTUHSC must not retain, give away, or remove from TTUHSC premises any TTUHSC information. Refer to the Board of Regents Rule, Chapter 10, Intellectual Property Rights, for more information. All other TTUHSC information in the possession of the departing workforce member must be provided to the person's immediate supervisor at the time of departure. This does not apply to copies of information provided to the public or copies of correspondence directly related to the terms and conditions of employment.

2.6 Information Access Management 45 CFR 164.308(a)(4)(i)

a. Managing Access. The TTUHSC HIPAA Committee and the information systems owner have final responsibility for defining access standards to TTUHSC information systems containing EPHI in order to protect the confidentiality, integrity, and availability of EPHI. Access to each system shall be monitored by the information systems owner.

   The HIPAA Committee is responsible for all access requests from third parties. See also 2.13 - Business Associate Contracts and Other Arrangements.

b. Request for Access. Management of access authorization begins with a Request for Access to a TTUHSC information system containing EPHI from a department.

   - identify the information systems containing EPHI for which access is requested;

   - name, position, and location of individual for whom access is requested;

   - describe purpose of access and establish level of access needed;

   - preferred start date for access and length of time for which access is requested;

- type of equipment through which access will occur (i.e., computer, smartphone, tablet, etc.);
- state access method (e.g. password or token or other); and
- confirmation of security training.

c. Review of Access. The information systems owner will at least annually review access to TTUHSC information systems containing EPHI and revise authorizations as necessary. Review shall be documented in writing and include:

- creating a time schedule of when access to each TTUHSC information systems containing EPHI will be reviewed;
- document that Requests for Access were properly completed;
- confirm the established level of access for each workforce member given access authorization;
- prompt removal or disabling of access methods for persons and entities that no longer need access to TTUHSC EPHI;
- modifying or retracting access authorization as necessary;
- change an existing access method as may be needed;
- confirm that tracking and logging of activities by authorized workforce members occurs;
- date and time of any changes to access authorization, identification of workforce member or software program whose access is being revised, brief description of revised access right(s); and reason for revision; and
- compliance with termination procedures set forth in section 2.5.3 above.

2.7 Reporting, Disciplinary Action, and Sanction Policy 45 CFR 164.308(a)(1)(ii)(C)

Each workforce member is responsible for reporting security violations in accordance to Section 2.4.2.4 of this Manual (also see HSC OP 52.04 – Reporting Violations; Non-Retaliation Policy). TTUHSC workforce members who fail to comply with TTUHSC security policies and procedures will be subject to disciplinary procedures as defined in TTUHSC operating policies. The appropriate policy is dependent on workforce status (faculty, staff or student). The workforce member may also be subject to applicable state and/or federal laws and regulations.

2.8 Security Awareness, Training, and Reminders 45 CFR 164.308(a)(5)

2.8.1 Training

The TTUHSC Information Security Officer or designee, in collaboration with the HIPAA Privacy Officer, shall coordinate the training of new and current TTUHSC workforce members regarding the TTUHSC HIPAA Privacy and Security requirements and compliance expectations. New TTUHSC workforce members, both remote and onsite, shall receive security training before such members are provided with access or accounts to TTUHSC information systems. Existing or current TTUHSC workforce members, both remote and onsite, shall receive privacy and security training on an annual basis.

Privacy and Security training shall include, but is not limited to, the following topics:

- applicable TTUHSC information security policies, procedures, and standards;
- secure use of TTUHSC information systems (e.g., log-on monitoring, allowed software) (See HSC OP 56.01 - Use of Information Technology Resources and its accompanying IT Policy 1.4 Security Safeguards);
- significant risks to TTUHSC information systems and data;
- TTUHSC's legal and business responsibilities for protecting its information systems and data;
- Protection from malicious software, including, but not limited to, viruses and procedures for detecting and reporting malicious software (See HSC OP 56.01 - Use of Information Technology Resources and its accompanying IT Policy 1.4.22
- Password management (See HSC OP 56.01 - Use of Information Technology Resources and its accompanying IT Policy 1.4.12 Password/Authentication.
- Contingency plans for emergencies and disasters that damage the confidentiality, integrity, or availability of its information systems (see Section 2.10 below); and
- Procedures for reporting a privacy or security violation. (See section 2.9 below)

The online training sessions shall be tracked and logged by the TTUHSC Privacy and Security offices. These records will be available to TTUHSC Human Resources Department as needed.

2.8.2 Reminders 45 CFR 164.308(a)(5)(ii)(A)

The TTUHSC Information Security Officer, or designee, shall provide periodic security reminders through the TTUHSC Announcements webpage and/or by email to applicable TTUHSC workforce members. Security reminders may include, but are not limited to:

- reminders regarding the importance of compliance with the TTUHSC Security Manual and federal and state laws pertaining to information security;
- updates or revisions to TTUHSC information security policies or provisions;
- security best practices;
- TTUHSC's information security legal and business responsibilities;
- newly implemented information security controls or substantial changes made to TTUHSC information security controls; and
- new threats or risks that could affect TTUHSC information systems or data and how to minimize possible security risks.

2.8.3 Other Security Awareness

In addition to security training and security reminders, the TTUHSC Information Security Officer, or designee, may provide other security awareness including, but not limited to:

- posters;
- workforce member meetings or orientations;
- security seminars;
- information systems sign on messages;
- newsletter articles; and

2.9 Security Incident Procedures 45 CFR 164.308(a)(6)(i)

TTUHSC workforce members, including, but not limited to, TTUHSC data users, shall report promptly any suspected or observed violation of this HIPAA Security Manual to the appropriate departmental administrator and to the TTUHSC Information Security Officer or Institutional Privacy Officer, as defined in HSC OP 52.02.

Business associates and other third parties shall report promptly any suspected or observed security incidents that may impact the confidentiality, integrity, and availability of TTUHSC information systems and the EPHI contained therein to the TTUHSC Information Security Officer and/or the Institutional Privacy Officer, as defined in HSC OP 52.13, Business Associate Agreements The information systems owner, in consultation with the Information Security Officer, will mitigate to the extent practicable, harmful effect of the security incidents that are known to TTUHSC.

For additional guidelines, refer to HSC OP 56.01 - Use of Information Technology Resources and its accompanying IT Policy 1.4.7 – Incident Management

2.10 Contingency Plans - 45 CFR 164.308(a)(7)(i)

The TTUHSC Chief Information Officer is responsible for coordinating a response to emergencies and disasters that damage the confidentiality, integrity, or availability of its information systems in accordance with HSC OP 76.01, Emergency Management Plans, and the Information Technology Disaster Recovery Plan in IT Policy 1.3 Disaster Recovery.

The TTUHSC Chief Information Officer shall develop and implement the Information Technology Disaster Recovery Plan. The plan shall be reviewed annually by the Information Security Officer with revisions sent to the Chief Information Officer for final approval. A copy of the IT Disaster Recovery Plan is available to those workforce members with assigned disaster recovery duties under the Disaster Recovery Plan.

The TTUHSC Chief Information Officer is responsible for providing annual training and awareness on TTUHSC's disaster preparation and disaster and emergency response processes to TTUHSC workforce members who are assigned disaster recovery duties. All personnel designated as part of the disaster recovery team shall have a current copy of the IT Disaster Recovery Plan with copies kept off-site at the Technology Operations and Systems Management (TOSM) facility at the Texas Tech University academic campus and at the regional campuses.

2.10.1 Emergency Mode Operations And Access Procedures 45 CFR 164.308(a)(7)(ii)(C), 45 CFR 164.312(a)(2)(ii)

The Chief Information Officer is responsible for protecting TTUHSC's critical information systems during and immediately after a crisis situation, and for emergency access procedure enabling authorized workforce members to obtain required data during an emergency. These emergency operations procedures are addressed in the Disaster Recovery Plan.

2.10.2 Data Backup 45 CFR 164.308(a)(7)(ii)(A)

The TTUHSC CIO is responsible for documenting a backup procedure for TTUHSC information systems and electronic media containing EPHI, including both EPHI received by TTUHSC and created within TTUHSC. The backup process is addressed in the Disaster Recovery Plan.

2.10.3 Testing and Revision Procedure

The TTUHSC CIO is responsible for implementing procedures for periodic testing and revision of the contingency plans for TTUHSC information systems and electronic media containing EPHI, including both EPHI received by TTUHSC and created within TTUHSC. The testing and revision process is addressed in the Disaster Recovery Plan.

2.10.4 Application and Data Criticality Analysis

TTUHSC's CIO is responsible for assessing the criticality of specific applications and data in support of other contingency plan components. The procedure for the analysis is addressed in the Disaster Recovery Plan.

2.11 Business Associate Contracts and Other Arrangements - 45 CFR 164.308(b)(1)

All TTUHSC Business Associates, which have a business relationship with TTUHSC that arises, shall sign a Business Associate Agreement which includes privacy and security provisions. In accordance with the Business Associate Agreement, a Business Associate (BA) is responsible to protect the EPHI that it creates, receives, maintains, or transmits on TTUHSC's behalf. HSC OP 52.13 - HIPAA Business Associate Agreement Policy details how to identify business associates and provides guidelines and a BA agreement template.

2.12 Documentation 45 CFR 164.316(b)

If any action, activity or assessment is required by this Security Manual and/or the HIPAA Security Rule to be documented, TTUHSC shall maintain a written (paper or electronic) record of the action, activity, or assessment. The TTUHSC Information Security Officer, or designee, shall retain such documentation for a minimum of 6 years from its date of creation or the date when it was last in effect, whichever is later, or as required in HSC OP 10.09 – Records Retention.

3. PHYSICAL SAFEGUARDS 45 CFR 164.310

3.1 Facility Access Controls 45 CFR 164.310(a)(1)

a. TTUHSC, through the Information Security Officer, is responsible for protecting the confidentiality, integrity and availability of its information systems, by preventing unauthorized physical access, tampering, and theft to the systems and to the facilities in which these systems are located while allowing properly authorized access to EPHI. TTUHSC information systems containing EPHI shall be physically located in areas where unauthorized access is minimized.

b. The level of protection provided for TTUHSC information systems containing EPHI must be commensurate with that of the identified risks. These information systems and electronic media containing EPHI shall be located and stored in secure environments that are protected by appropriate security barriers and entry controls.

c. The perimeter of a building or site containing TTUHSC information systems with EPHI must be physically sound. The external walls of the building or site solidly constructed, and all external doors must have appropriate protections against unauthorized access. Physical barriers must, if necessary, be extended from actual floor to actual ceiling to prevent unauthorized entry. Doors and windows shall be locked when unattended, and reasonable external protection adapted for windows, particularly those at ground level. These safeguards shall be consistent with determinations under TTUHSC policies relating to TTUHSC Safety and Security Programs as implemented by the Director of Plant Operations (Lubbock) and the Directors of Facilities Operations and Maintenance (regional campuses) and the Police Department. These TTUHSC officials shall be responsible, with consultation as required with the Information Security Officer, to control TTUHSC delivery and loading areas to prevent unauthorized access. Where possible, the following controls shall be used:

   - access to a holding area from outside of the building restricted to identified and authorized persons;
   - the holding area designated or set up so that supplies can be unloaded without delivery staff gaining access to other parts of the building;
   - the external door(s) of a holding area secured when the internal door is opened.

d. The Director of Plant Operations (Lubbock), and the Directors of Facilities Operations and Maintenance (regional campuses) shall document all repairs, modifications, and maintenance done to the physical components of TTUHSC facilities that are related to the security of EPHI. Physical components include, but are not limited to, automated physical access systems, locks, doors, and walls. Repair or modification documentation shall be maintained in a secure manner and shall include:

- date and time of repair or modification;
- reason for repair or modification;
- person (s) performing the repair or modification; and
- outcomes of repair or modification.

e. The Information Security Officer shall require an inventory of all physical access controls used to protect information systems with EPHI at all facilities and maintain the report in a secure manner. The inventory shall specifically identify all areas when information systems containing EPHI are maintained and the level and means of access approved for each area. Access shall be provided only to TTUHSC workforce members having a need for specific access in order to accomplish position responsibilities and must be regularly reviewed by the authorizing department and revised as necessary.

f. Procedures that allow facility access in support of restoration of data are set forth in the TTUHSC Disaster Recovery Plan. For more information, see Section 2.10 of this Manual.

3.1.1 Facility Security Plan 45 CFR 164.310(a)(2)(ii)

Policies and procedures have been established in TTUHSC OPs to protect TTUHSC facilities and the confidentiality, integrity, and availability of its information systems by preventing unauthorized physical access, tampering and theft. Applicable OPs include policies on:

- Facilities Management (HSC OP 61);
- Safety Services (HSC OP 75); and
- Security (HSC OP 76)

A current copy of TTUHSC operating policies is available to all TTUHSC workforce members at http://www.ttuhsc.edu/hsc/op/ For off-site locations without internet access, sufficient copies of current policies shall be kept on file by the administrative staff of every Dean and department heads.

3.1.2 Access Control and Validation 45 CFR 164.310(a)(2)(iii)

a. Approved access shall be limited to workforce members who have a need for specific physical access in order to accomplish a legitimate task.

b. The TTUHSC Information Security Officer, the Institutional Privacy Officer, and the information systems owner have final responsibility for access to TTUHSC information systems containing EPHI. Access shall be granted, terminated, and reviewed in accordance with Sections 2.5.3 and 2.6 of this Manual respectively.

c. In compliance with HSC OP 76.02, Identification Badges, TTUHSC workforce members are required to have in their possession their TTUHSC identification badge while on a TTUHSC campus or facility. Employees must be able to present their badges when requested. Employees are encouraged to report unescorted strangers.

d. Each information systems owner is responsible for providing the manner where sign-in visitors are properly identified prior to admission to TTUHSC areas where information systems containing EPHI are located or stored.

e. Physical access by workforce members and others to areas identified in the annual inventory 3.1(e) shall be tracked and logged by the information systems owner and shall include the following information:

- date and time of access;
- reason for access;
- name or user ID of person gaining access; and
- name of the workforce member who granted access.

This information shall be maintained by the information systems owner and reviewed regularly by the Information Security Officer, or designee.

f. TTUHSC workforce members shall immediately report to the department supervisor, TTUHSC Police Department, and/or the Information Security Officer, the loss or theft of any device (e.g. card or token) that can enable physical access to facilities identified in the inventory.

3.2 Workstation Use and Security 45 CFR 164.310(b), 45 CFR 164.310(c)

a. Workstation In General. TTUHSC workstations shall be used only for authorized purposes: to support the research, education, clinical, administrative, and other functions of TTUHSC. Workforce members shall not use TTUHSC workstations to engage in any activity that is either illegal under applicable local, state, federal, or international law or is in violation of TTUHSC policy. All workforce members who use TTUHSC workstations shall take all reasonable precautions to protect the confidentiality, integrity, and availability of EPHI contained on the workstations. Refer to See HSC OP 56.01 - Use of Information Technology Resources and its accompanying IT Policy 1.4.1 – Acceptable Use Policy and Section 2.4, Security Management Process, in this Manual for more information. http://www.ttuhsc.edu/it/policy/safeguards.aspx

b. Access To Workstations. Access to all TTUHSC workstations containing EPHI shall be controlled with a username and password or an access device such as an authorized card

reader. Access to all TTUHSC workstations with EPHI must be authenticated via a process that includes, but is not limited to:

- unique user IDs that enable users to be identified and tracked;
- secret identifier/password; and
- verification that redundant user IDs is not issued.

All password-based access control systems on TTUHSC workstations shall mask, suppress, or otherwise obscure the passwords so that unauthorized persons are not able to observe them. TTUHSC workforce members shall not share passwords with others. A TTUHSC workforce member who believes that someone else is inappropriately using a user-id or password shall immediately notify the department supervisor, information systems owner or the Information Security Officer.

The initial password (s) issued to a new TTUHSC workforce member must be valid only for the new user's first logon to an account. At initial logon, the user will be required to choose another password. Where possible, this same process must be used when a workforce member's account password is reset. The system shall also require the regular changing of account passwords and, where necessary, only allow the use of unique passwords each time.

TTUHSC workforce members shall not attempt to access, duplicate or transmit electronic media containing EPHI for which they have not been given appropriate authorization.

c. Safeguarding The Workstation. TTUHSC workstations displaying EPHI shall be physically located in such a manner as to minimize the risk that unauthorized individuals can gain access to them. The display screens of all TTUHSC workstations displaying EPHI shall be positioned such that information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in a reception, public, or other related areas. A privacy screen that fits over the workstation monitor may also be used if the workspace does not readily allow for the relocation of the workstation.

   Institutionally approved anti-virus software must be installed on workstations to prevent transmission of malicious software. Refer to HSC OP 56.01 - Use of Information Technology Resources and its accompanying IT Policy 1.4.22 – Viruses and Other Malicious Code.

   TTUHSC workforce members shall lock their workstation when they leave their workstation area unattended and/or log off from or lock their workstation (s) when their shifts are complete. Refer Section 4.1.2 for more information.

3.3 Device and Media Controls – 45 CFR 164.310(d)(1)

a. EPHI located on TTUHSC information systems or electronic media shall be protected against damage, theft, and unauthorized access. This includes both EPHI received by TTUHSC and

created within TTUHSC. EPHI shall be consistently protected and managed through its entire life cycle, from origination to destruction.

See Section 2.4.2.2 for tracking and logging information and Section 2.10 for contingency planning.

b. All TTUHSC hardware and electronic media that contains EPHI must be clearly marked as confidential and should have a tracking number attached to it. Each information systems owner shall conduct an annual inventory to identify information systems and electronic media that contain EPHI. This may be done in conjunction with the annual TTUHSC asset inventory. This inventory shall be maintained by the information systems owner. The information systems owner must also document and maintain a record of all movements of hardware and electronic media containing EPHI.

c. When no longer needed for legitimate use, and to avoid access to EPHI by unauthorized persons, the Information Owner or their designee, is responsible for the direct disposal of TTUHSC information systems and electronic media containing EPHI in accordance with the following process:

    - disposal shall be documented on the inventory list maintained by each information systems owner, and shall include EPHI received by TTUHSC and created within TTUHSC that is maintained on the system or media.

    - each information systems owner is responsible to track and log disposal of all TTUHSC electronic media and information systems containing EPHI, and the following information shall be included:

        i. date and time of disposal;

        ii. who performed the disposal and how; and

        iii. brief description of media or information system that was disposed.

    For obsolete hardware and software, please see HSC OP 63.11- Disposal of Surplus, Obsolete, or Uneconomically Repairable Inventory for guidance.

d. An information system or electronic medium containing EPHI that is to be disposed of permanently shall be physically destroyed and rendered functionally unusable. An industrial data destruction service or facility may be used through a purchase order approved by the Chief Information Officer and the Information Security Officer and executed through the TTUHSC Purchasing Department.

e. If an information system or electronic medium containing EPHI is to be reused within TTUHSC (or for other entities), all data shall be completely removed by using erase tool (s) approved by the Information Security Officer. Each information systems owner, or his

designated representative, is responsible to confirm and document removal of all EPHI on electronic media before the media are re-used.

f. Before EPHI is moved, a backup must be completed in accordance with Section 2.10.2 of this Manual.

4. TECHNICAL SAFEGUARDS 45 CFR 164.312

4.1 Access Control 45 CFR 164.312(a)(1)

a. The Information Security Officer shall approve all TTUHSC information systems for compliance with Section 2.6 of this Manual.

Any current TTUHSC information systems that do not currently comply with TTUHSC's information access management policy shall be subject to restricted access until compliance is approved by the Information Security Officer.

TTUHSC information systems shall support one or more of the following types of access control to protect the confidentiality, integrity, and availability of EPHI contained on TTUHSC information systems:

- user-based;
- role-based; and
- context-based.

4.1.1 Unique User Identification 45 CFR 164.312(a)(2)(i)

Unique identifiers must not give any indication of the user's privilege level and may include:

- biometric identification;
- workforce member names; and
- exclusive numbers (e.g. PIN).

TTUHSC information systems must grant users access via unique identifiers that:

- identify workforce members or users; and
- allow activities performed on information systems to be traced back to a particular individual through tracking of unique identifiers.

Group user identifiers shall not be used to gain access to TTUHSC information systems that contain EPHI. When unique user identifiers are insufficient or inappropriate, group identifiers may be used only to gain access to TTUHSC information systems that do not contain EPHI.

4.1.2 Emergency Access Procedure 45 CFR 164.312(a)(2)(ii)

Procedures to address emergency access to EPHI are addressed in the TTUHSC Disaster Recovery Plan. For more information, see Section 2.10 of this Manual.

4.1.3 Automatic Logoff 45 CFR 164.312(a)(2)(iii)

TTUHSC workforce members must end electronic sessions on information systems that contain or can access EPHI when such sessions are completed, unless the information system is secured by an appropriate locking method, e.g. a password protected screen saver.

Electronic sessions on information systems that contain or can access EPHI and which lack appropriate locking methods must be automatically terminated after 15 minutes of inactivity. Exceptions to TTUHSC's information systems required inactivity timeout must be approved by TTUHSC's Information Security Officer after risk analysis has been conducted.

TTUHSC workforce members must activate their workstation locking software whenever they leave their workstation unattended for 15 minutes or more and log off from or lock their workstation(s) when their shift is complete.

4.1.4 Encryption And Decryption 45 CFR 164.312(a)(2)(iv)

a. When risk analysis indicates it is necessary, appropriate encryption must be used to protect the confidentiality, integrity, and availability of EPHI contained on TTUHSC information systems. All portable devices (e.g., laptops, smartphones, tablets etc.) that contain EPHI must be encrypted.

b. TTUHSC must protect all of its cryptographic keys against modification and destruction; its secret and private keys must be protected against unauthorized disclosure. TTUHSC must have a formal, documented process for managing the cryptographic keys used to encrypt EPHI on TTUHSC information systems. This process must include:

    - a procedure for generating keys for different cryptographic systems;
    - a procedure for distributing keys to intended users and then activating them;
    - a procedure for enabling authorized users to access stored keys;
    - a procedure for changing and updating keys;
    - a procedure for revoking keys;
    - a procedure for recovering keys that are lost or corrupted;
    - a procedure for archiving keys; and

- appropriate logging and auditing of cryptographic key management.

4.2 Audit Controls 45 CFR 164.312(b)

In conjunction with the Information owners, and under the supervision of the CIO, the Information Security Officer shall approve and implement appropriate hardware, software, and/or procedural auditing mechanisms to record and examine activity on TTUHSC information systems that contain or use EPHI. Audit controls shall be implemented in accordance with Section 2.4.3, Information System Activity Review, of this Manual.

4.3 Integrity 45 CFR 164.312(c)(1)

Under the supervision of the CIO and with input from the Institutional Privacy Officer, the Information Security Officer and the information systems owner are jointly responsible for implementing mechanisms to authenticate and corroborate that EPHI has not been altered or destroyed in an unauthorized manner. These procedures shall be implemented based on the risk analysis findings and in accordance with Section 2.4, Security Management Process, of this Manual.

4.4 Person or Entity Authentication 45 CFR 164.312(d)

a. The information systems owner will follow Section 2.6 of this Manual with respect to verifying the identity of the workforce member before granting access to EPHI.

b. TTUHSC will utilize appropriate and reasonable system(s), which meet the requirements, as defined by Institutional policies, to confirm that only properly authenticated persons and entities access its EPHI. Such authentication system(s) will include, but are not limited to:

    - unique user identifiers (user IDs) that enable persons and entities to be uniquely identified. User IDs must not give any indication of the user's privilege level;
    - secret identifier/password;
    - the prompt removal or disabling of authentication methods for persons and entities that no longer need access to TTUHSC EPHI; and
    - verification that redundant user identifiers are not issued.

    As part of the Privacy and Security Awareness training, TTUHSC must provide employees with information about the authentication process.

c. All authentication data, such as passwords and PINs, must be protected with appropriate systems on TTUHSC information systems and must mask, suppress, or otherwise obscure the passwords and PINs so that unauthorized persons are not able to observe them.

    Methods for authentication (e.g. password or PIN) to TTUHSC information systems must not be built into logon scripts. All exceptions must be reviewed and approved by appropriate management.

TTUHSC employees must not share or reveal their authentication methods to others. Sharing an authentication method means the authorized user assumes responsibility for actions that another party takes with the disclosed method. A TTUHSC employee who believes that their authentication method is being inappropriately used must immediately notify his or her manager or the Information Security Officer.

TTUHSC employees must also immediately report the loss or theft of their identification card to appropriate management and/or to the TTUHSC Police Department.

d. To prevent authentication by unauthorized persons, TTUHSC employees must activate their workstation locking software whenever they leave their workstation unattended. Locking or timeout processes must activate on all other TTUHSC information systems after 15 minutes or more of inactivity.

4.5 Transmission Security 45 CFR 164.312(e)(1)

HSC OP 56.04, Electronic Transmission of Personally Identifiable Information (PII) and Protected Health Information (PHI) provide a framework to allow Personally Identifiable Information (PII) and Protected Health Information (PHI) to be securely transmitted over electronic communication networks such as e-mail and the Internet.

4.51 Data Integrity Controls 45 CFR 164.312(e)(2)(i)

a. Integrity controls must always be used when highly sensitive TTUHSC data, such as EPHI and passwords, are transmitted over electronic communications network. TTUHSC's integrity controls must ensure that the value and state of all transmitted data is maintained and the data is protected from unauthorized modification. Such controls may include:

- checksums;
- digital signatures;
- hash values; and
- encryption.

b. When determining whether or not integrity controls must be used when sending specific data over an electronic communication network, the following factors should be taken into account:

- the sensitivity of the data;
- the risks to the data; and
- the expected impact to TTUHSC functionality and work flow if these mechanisms are used to protect the integrity of the EPHI.

4.52 Encryption 45 CFR 164.312(2)(ii)

Unless risk analysis indicates that there is no significant risk when sending TTUHSC data over an electronic communications network, the data must be sent in encrypted form. Encryption and integrity controls must always be used when sending EPHI or other highly sensitive TTUHSC data, such as passwords, over external/non-TTUHSC electronic communication networks.

The Information Security Officer and the Institutional Privacy Officer will jointly review all encryption used to protect the confidentiality, integrity, and availability of EPHI contained on TTUHSC information systems, with final approval by the Chief Information Officer and the HIPAA Committee. The Information Security Officer, or designee, will also maintain documentation with regards to when encryption is utilized. No department will implement encryption of data without the knowledge and approval of the Information Security Officer.