

	UT Health Science Center		
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 1 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

**UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER
(UTHSC) HIPAA PRIVACY AND SECURITY COMBINED
POLICIES**

Table of Contents

- ❖ [PREAMBLE](#)
- ❖ [PURPOSE](#)
- ❖ **GENERAL POLICIES APPLICABLE TO BOTH PRIVACY AND SECURITY**
 - [Applicability](#)
 - [Individuals' Basic HIPAA Rights](#)
 - [Business Associates](#)
 - [Education and Training of Workforce](#)
 - [HIPAA Privacy and Security Officers](#)
 - [Access to Policies and Procedures](#)
 - [Policy and Procedure Documentation Requirements](#)
 - [Complaints and Reports of Potential Privacy and/or Security Violations](#)
 - [Response to Complaints and Reports of Potential Privacy and/or Security Violations](#)

	UT Health Science Center		
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 2 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

- [Security Incident Procedures](#)
- [Risk Assessments to Determine the Existence of a Breach; Breach Notification Procedures](#)
- [Sanctions](#)

❖ **SPECIFIC PRIVACY POLICIES**

- [Access to Protected Health Information – Patient’s Rights](#)
- [Access to Protected Health Information – UTHSC Employees](#)
- [Compliance with HIPAA’s “Minimum Necessary” Rule](#)
- [Patient Requests for Amendments of Their Own PHI](#)
- [Authorization for Access, Disclosure and Release of PHI](#)
- [Communication with Family, Friends and Relatives of patients](#)
- [Removal of Written Records from the UTHSC Premises](#)

❖ **SPECIFIC SECURITY POLICIES**

- [Security Rule Compliance Personnel](#)
- ❖ [Administrative Policies](#)
 - [Security Management](#)
 - [Security and Information Access Management](#)
 - [Contingency Plans](#)
- ❖ [Physical Safeguard Policies](#)
 - [Facility Access Controls](#)
 - [Workstation Use](#)
 - [Workstation Security](#)

	UT Health Science Center		
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 3 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

- ❖ [Device and Media Controls](#)
 - [Hardware and Media inside a Facility](#)
 - [Surplus Equipment](#)
- ❖ [Technical Safeguard Policies](#)
 - [Access Control](#)
 - [Audit Controls](#)
 - [Data Integrity](#)
 - [Authentication](#)
 - [Transmission Security](#)

	UT Health Science Center			
<p style="text-align: center;">HIPAA Privacy and Security</p> <p style="text-align: center;">Combined Policies</p> 	Doc. Version:	1.0	Page 4 of 30	
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date:	9/23/13
	Effective Date:	9/23/13		
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations		

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 5 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

PREAMBLE

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations adopted by the United States Department of Health and Human Services (DHHS) pursuant thereto provide, among other things, standards for the privacy and security of individuals' health care information. See, 42 U.S.C. §§1320d et seq.; 45 C.F.R. Parts 160 and 164.

HIPAA provides a national standard for the privacy and security of health information, and it provides individuals with certain rights with regard to the use and disclosure of their health information. HIPAA provides a floor rather than a ceiling for the protection of health information. It does not override state laws that are more restrictive or more protective of individuals' health information. HIPAA also was intended to improve efficiency in the health care industry by creating national standards for electronic health care transactions.

Health information protected by HIPAA is known as Protected Health Information, or PHI. In general, PHI means any information, including demographic information collected from an individual, whether oral or recorded in any form or medium, which is created or received by a Covered Entity or Business Associate, and which: (a) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (b) either actually identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and (c) is transmitted or maintained in electronic media or any other form or medium.

HIPAA regulations apply both to Covered Entities and to Business Associates of Covered Entities. A Covered Entity is a health care plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. A Business Associate of a Covered Entity is a person, who is not a member of the workforce of the Covered Entity, but who, on behalf of the Covered Entity: (a) creates, receives, maintains or transmits PHI in the performance of a function or activity regulated by HIPAA, including but not limited to claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management and practice management; or (b) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, where the provision of the service involves the disclosure of PHI from such

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 6 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

Covered Entity (or from another Business Associate of such Covered Entity) to the person. A Business Associate also includes, but is not limited to a subcontractor that creates, receives, maintains, or transmits PHI on behalf of a Business Associate. A Covered Entity may be a Business Associate of another Covered Entity.

The University of Tennessee Health Science Center (“UTHSC”) campuses and clinics comprise the health care component (Covered Entity) of The University of Tennessee under HIPAA. The UTHSC is considered to be a Covered Entity and governed by HIPAA regulations whenever the UTHSC (through one or more of its health care providers) orders, furnishes, bills for, or receives payment for health care services or supplies, and when the UTHSC transmits or causes to be transmitted PHI related thereto in electronic form. The health care providers and clinics of UTHSC include all clinics located on the UTHSC campus in Memphis, Tennessee; the Graduate Pediatric Dental Clinic in West Memphis, Arkansas; the Graduate School of Medicine Clinics in Knoxville, Tennessee; the Jackson Family Practice Center in Jackson, Tennessee; and the College of Allied Health Audiology/Speech Therapy Clinics in Knoxville, Tennessee. In some instances, the UTHSC may be considered to be a Business Associate of a Covered Entity, if the UTHSC is carrying out some basic function *on behalf of* another Covered Entity. Likewise, whenever the UTHSC engages an outside individual or entity who is not a part of the UTHSC’s workforce to provide some function *on behalf of* the UTHSC when the UTHSC is acting as a Covered Entity, which outside individual or entity may be considered to be a Business Associate of the UTHSC. However, in some instances, for example, when the UTHSC is receiving, generating, maintaining, or transmitting health information in conjunction with purely a research function, and the UTHSC is not ordering, furnishing, billing for, or receiving payment for health care services or supplies related to such research, the UTHSC may not be considered to be acting as a Covered Entity under HIPAA.

While HIPAA’s privacy regulations protect PHI in any medium, the security regulations are not as broad, and those regulations protect PHI only in electronic form. HIPAA privacy regulations limit the manner in which PHI can be used and disclosed by those to whom the regulations apply. HIPAA security regulations expand upon this by requiring all Covered Entities to implement policies and procedures to ensure the security as well as the privacy of PHI. Although the regulations treat the requirements for privacy and security separately, the two are inherently intertwined.

On February 17, 2009, the HIPAA privacy and security regulations were amended by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act as a part of the

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 7 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009) (“ARRA”). See Sections 13001 - 13424 of Division A, Title XIII of ARRA (hereinafter referred to as “the HITECH Act”). Among other things, the HITECH Act expanded the applicability of HIPAA regulations directly to Business Associates, provided for greater enforcement HIPAA’s privacy and security rules, and increased the penalties for unauthorized disclosures of a patient’s PHI. The HITECH Act also required Covered Entities and Business Associates to provide written notice to patients (and in some cases, when large numbers of patients are involved, to the media and the Secretary of the United States Department of Health and Human Services) under certain circumstances and conditions when a patient’s unsecured PHI has been disclosed to an unauthorized individual.

On January 25, 2013, DHHS issued rules and regulations, commonly referred to as the “HIPAA Final Omnibus Rule,” which (a) modified HIPAA’s privacy, security, breach notification, and enforcement rules, (b) implemented certain provisions of the HITECH Act, and (c) strengthened the privacy and security protections for individuals’ protected health information. See, 78 Fed. Reg. 5566-5702, codified at 45 C.F.R. Parts 160 and 164. In addition to modifying certain definitions within HIPAA and making HIPAA directly applicable to Business Associates and subcontractors of Business Associates the same as HIPAA applies to Covered Entities, the HIPAA Final Omnibus Rule, among other things, modified and finalized HIPAA’s breach notification requirements, which were first announced in the HITECH Act. The HIPAA Final Omnibus Rule also required Covered Entities to modify their Notice of Privacy Practices and their Business Associate Agreements to account for the strengthened privacy, security, breach notification, and enforcement provisions set forth in the HIPAA Final Omnibus Rule.

	UT Health Science Center			
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 8 of 30	
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date:	9/23/13
	Effective Date:	9/23/13		
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations		

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 		Doc. Version:	1.0 Page 9 of 30
		Revised by:	F. Davison W. Schuler C. Moffitt Revision Date: 9/23/13
		Effective Date:	9/23/13
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

PURPOSE

The purpose of these policies is to establish a plan to ensure the UTHSC's compliance with applicable HIPAA laws and regulations, and to provide for the privacy and security of PHI that is received, generated, maintained, or transmitted by the UTHSC. These policies are designed to replace existing UTHSC policies and procedures pertaining to HIPAA privacy and security and to supplement University of Tennessee policies and other UTHSC policies.

GENERAL POLICIES APPLICABLE TO BOTH PRIVACY AND SECURITY

Applicability

The UTHSC's HIPAA privacy and security policies apply to all UTHSC locations statewide, whenever the UTHSC is acting as a Covered Entity or as a Business Associate under applicable HIPAA regulations.

Individuals' Basic HIPAA Rights

Whenever the UTHSC is acting as a HIPAA Covered Entity, patients have a right to:

- Receive a copy of UTHSC's standard Notice of Privacy Practices, which describes how the patient's PHI may be used and disclosed and how the patient can gain access to this information. (See Items 1, 2, 6, 7 and 8 of HIPAA Policies and Procedures [http://www.uthsc.edu/compliance/hipaa_policies.php] and Notice of Privacy Practices forms [http://www.uthsc.edu/compliance/privacy_practices.php])
- http://www.uthsc.edu/compliance/hipaa_policies.ph
- Request an amendment to their PHI to correct errors, which the UTHSC may either approve or reject with written notice to the patient, advising the patient of the UTHSC's decision. (See Item 9 of HIPAA Policies and Procedures [http://www.uthsc.edu/compliance/hipaa_policies.php])
-

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 10 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

(See HIPAA Policies and Procedures [
http://www.uthsc.edu/compliance/hipaa_policies.php])

- You have the right to request in writing a restriction on the uses and disclosures of your protected health information for treatment, payment and health care operations; however, we are not required to agree to your request. If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment. We may, however, also end the agreement at any time after notifying you in writing of such. (See Item 11 of HIPAA Policies and Procedures [
http://www.uthsc.edu/compliance/hipaa_policies.php])
-
- Inspect and obtain a copy of your health record within sixty days of request. There may be a charge to cover the cost of producing your record in hard copy or electronic form.
- Obtain an accounting of disclosures of your protected health information made after April 14, 2003 for purposes other than treatment, payment, and healthcare operations;
- Request communication of your health information in a certain way or at a certain location. For example, you can ask that we contact you by mail and not by telephone, or that we contact you at a specific telephone number, or that we use an alternative address for billing purposes, or that we not leave messages on certain answering machines. Email communication will be provided only at your written request indicating you understand that email can be an unsecure communication method;
- Revoke your authorization to use or disclose health information except to the extent that action has already been taken; and

Restrict disclosures to a health plan for services when those services have been paid out-of-pocket in full by the patient, a family member, or another individual

- [
http://www.uthsc.edu/compliance/hipaa_policies.php])
- File a complaint with UTHSC in accordance with a complaint process established and maintained by UTHSC, and/or with DHHS. (See Item 10 of HIPAA Policies and Procedures, and Complaint Form link on right side of webpage [
http://www.uthsc.edu/compliance/hipaa_policies.php])

Business Associates

Business Associates of the UTHSC are required to comply with HIPAA. The UTHSC shall identify

		UT Health Science Center		
HIPAA Privacy and Security Combined Policies 		Doc. Version:	1.0	Page 11 of 30
		Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
		Effective Date:	9/23/13	
			Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

all Business Associates through Purchasing, Grants and Contracts, Research Administration, and clinical departments with the assistance and input of UTHSC's HIPAA Privacy Officer. The Contracts Administration Manager shall maintain a current list of Business Associates. A Business Associate Agreement in a form approved by legal counsel shall be prepared by the department requesting the arrangement. (See Item 14 of HIPAA Policies and Procedures [http://www.uthsc.edu/compliance/hipaa_policies.php] and updated Business Associate Agreement [<http://www.uthsc.edu/hipaa/hipaaforms.php>])

Education and Training of Workforce

The development and implementation of HIPAA-related education and training seminars for employees is an integral part of the UTHSC's HIPAA compliance program. Compliance program education contains an introduction to HIPAA applicable to all employees and specialized training where needed.

All staff, faculty, and students regardless of job title or responsibility, must complete on-line HIPAA training; Additional training may be required to address amendments to the HIPAA law, or as a refresher. (See Items 3, 4, and 5 of Compliance Training [<http://www.uthsc.edu/compliance/training.php>])

Comprehensive education materials shall be developed to facilitate the HIPAA training sessions and ensure that a consistent message is delivered to all employees. Generally, subjects to be presented shall include:

- Patient Rights
- Patient Privacy Notices
- Access to Protected Health Information
- Request for Amendments to Health Information
- Accounting of Disclosures
- Complaints
- Disclosures

		UT Health Science Center		
HIPAA Privacy and Security Combined Policies 		Doc. Version:	1.0	Page 12 of 30
		Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
		Effective Date:	9/23/13	
			Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

- Authorizations
- Security

The Dean of each College and the Vice Chancellors, or their designees, is responsible for ensuring that employees and students have completed HIPAA training. The privacy officer and the security officer shall monitor training progress and advise the Dean or Vice Chancellor of any deficiencies. No UTHSC employee shall be exposed to PHI until appropriate HIPAA training has been provided to the employee.

In the event that a new UTHSC employee is unable to obtain a UTHSC personnel number, which would enable the new employee to complete UTHSC's web-based HIPAA training, prior to the need to disclose PHI to the new employee, the Dean or Vice Chancellor, or their designee, should contact the UTHSC HIPAA Privacy Officer to obtain appropriate printed materials to allow for completion of appropriate HIPAA training prior to the disclosure of PHI to the new employee. Documentation of such training is to be maintained in the new employee's departmental personnel file. In any event, the UTHSC's web-based HIPAA training is to be completed by all new UTHSC employees prior to the expiration of thirty (30) days after the new employee obtains his or her personnel number, or prior to the new employee being exposed to any PHI, whichever event first occurs.

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 13 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

HIPAA Privacy and Security Officers

HIPAA requires Covered Entities to name a Privacy Officer and a Security Officer to oversee HIPAA privacy and security requirements. (See UTHSC HIPAA Announcement [http://www.uthsc.edu/hipaa/UTHSC_HIPAA_Announcement.pdf]; HIPAA Information [<http://www.uthsc.edu/hipaa/>]; Item 4 of HIPAA Policies and Procedures [http://www.uthsc.edu/compliance/hipaa_policies.php]) The Privacy Officer and the Security Officer are responsible for:

Ensuring the confidentiality of all PHI through development and implementation of policies, procedures, and training programs affecting privacy and security of PHI.

- Coordinating HIPAA training of the workforce.
- Providing information about matters covered by the Notice of Privacy Practices.
- Auditing sites where protected health information is maintained to ensure compliance with HIPAA regulations.
- Documenting, investigating and responding to all patient complaints regarding improper disclosure or use of PHI.
- Reviewing audit logs to verify workforce activities.
- Investigating, reporting and mitigating effects of all disclosures that are not HIPAA compliant.
- Advising members of the workforce on privacy and security matters.

	UT Health Science Center		
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 14 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

Access to Policies and Procedures

HIPAA policies and procedures are available to all faculty, staff and students on the UTHSC website at [<http://www.uthsc.edu/hipaa>].

Policy and Procedure Documentation Requirements

Form: All HIPAA policies and procedures must be in a written form (which may be electronic). Also, actions, activities or assessments undertaken as a part of HIPAA compliance must be in a written form.

Document Retention: The Security Officer shall maintain a copy of all HIPAA policies and procedures, and revisions thereto. These documents shall be retained for a period of at least six (6) years after they were last in effect.

All documents related to investigations, complaints, and disclosures shall be maintained for at least six (6) years. All documentation related to training shall be maintained in electronic form for at least six (6) years after employment cessation. Documentation relating to privacy investigations, complaints and disclosures shall be maintained by the Privacy Officer. Documentation relating to security investigations, complaints and incidents shall be maintained by the Security Officer.

Reviews and Updates: UTHSC shall undertake a review and update of its HIPAA policies and procedures at least every three (3) years, or as otherwise required by law.

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 15 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

Complaints and Reports of Potential Privacy and/or Security Violations

Complaints and other reports of potential privacy or security violations, and the response to such complaints and reports, shall be kept on file by the Security and/or Privacy Officer. Patients shall be informed in the Notice of Privacy Practices of his/her right to file a complaint without fear of reprisal or other adverse treatment.

All complaints and reports of potential HIPAA violations shall be investigated and resolved as quickly as possible by the appropriate administrative/ management staff and the Privacy and/or Security Officers.

- Complaints and other reports of potential HIPAA violations may be directed either in person or via telephone to the Privacy Officer at 901- 448-1700 or 1-888-455-158 or the Security Officer at 901-448-5841 or 1-800-786-1991. Complaints and other reports may be made anonymously. (See generally HIPAA Policies and Procedures [http://www.uthsc.edu/compliance/hipaa_policies.php])
- All complaints and other reports shall be documented.
- The Privacy and/or Security Officer, as appropriate, shall investigate the complaints and reports.
- The Privacy and Security Officer shall make every effort to resolve the complaint or report within a reasonable time according to the HIPAA policies and procedures.

Response to Complaints and Reports of Potential Privacy and/or Security Violations

Violations of privacy, security, or UTHSC policies and procedures may occur despite privacy and security protections. Early detection and response to such violations are critical to correct the violation, mitigate any harm that results from such violation, and prevent the violation from recurring.

- All UTHSC employees must cooperate with any investigation. Failure to cooperate, failure to furnish requested information, or furnishing false information may result in employee

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 16 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

discipline up to and including termination. Department managers shall ensure that the investigating officer is provided appropriate access to employees and information needed to conduct a thorough investigation.

- UTHSC students must cooperate with any investigation. Failure to cooperate, failure to furnish requested information, or furnishing false information is a violation of the Honor Code (<http://www.uthsc.edu/centerscope/>) and may result in discipline up to and including dismissal from the UTHSC.
- Documentation detailing the investigation of complaints and other reports of potential HIPAA violations shall be prepared and maintained by the Privacy Officer and the Security Officer.
- The fact that the UTHSC’s investigation has concluded, and/or the findings of such investigation shall be reported to the complainant or other individual reporting the potential HIPAA violation when appropriate or as required by law.

Security Incident Procedures

A security incident, defined as “the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system,” (see 45 CFR § 164.304) must be reported immediately upon discovery to the Security Officer. Procedures for reporting these matters are posted on the UTHSC web site at [<http://www.uthsc.edu/hipaa>].

- All faculty, staff and students must assist in UTHSC’s compliance with the privacy and security provisions of HIPAA, as amended by the HITECH Act, regarding security breach notice requirements.

Risk Assessments to Determine the Existence of a Breach; Breach Notification Procedures

In the event of a potential Breach of Unsecured Protected Health Information or a potential unauthorized use or disclosure of unsecured PHI, the Privacy Officer and the Security Officer shall be notified immediately. Under HIPAA, the term “Breach” means the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI. The term “Breach” does not include;

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 17 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

(i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA;

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the PHI received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA; or

(iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such PHI.

IMPORTANT: Any acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA is *presumed to be a "Breach"* unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the PHI or to whom the disclosure was made;

(iii) Whether the PHI was actually acquired or viewed; and

(iv) The extent to which the risk to the PHI has been mitigated.

ONLY UTHSC'S PRIVACY AND SECURITY OFFICERS, AFTER CONSULTATION WITH UTHSC ADMINISTRATION AND WITH UT'S OFFICE OF GENERAL COUNSEL (AS NEEDED) MAY DETERMINE THAT A PARTICULAR ACQUISITION, ACCESS, USE, OR DISCLOSURE OF PHI IN A MANNER NOT PERMITTED UNDER HIPAA DOES NOT CONSTITUTE A BREACH. ALL POTENTIAL BREACHES MUST BE REPORTED TO UTHSC'S PRIVACY AND SECURITY OFFICERS. UTHSC'S PRIVACY AND SECURITY

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 18 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

OFFICERS WILL CREATE AND MAINTAIN DETAILED DOCUMENTATION OF THE REASONING FOR ANY DETERMINATION THAT A PARTICULAR ACQUISITION, ACCESS, USE, OR DISCLOSURE OF PHI IN A MANNER NOT PERMITTED UNDER HIPAA DOES NOT CONSTITUTE A BREACH.

The term “Unsecured Protected Health Information” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in the HITECH Act.

All notifications required by HIPAA to individuals, the media, and the Secretary of DHHS (and to other Covered Entities or Business Associates when UTHSC is acting a Business Associate or as a subcontractor of a Business Associate) of any Breach of Unsecured Protected Health Information discovered by UTHSC shall be carried out by UTHSC within the time frames and in the manner required by 45 C.F.R. §§ 164.402, 164.404, 164.406, 164.408, 164.410, and 164.412. All Breaches of Unsecured Protected Health Information shall be treated as “discovered by UTHSC” as of the first day on which such Breach is known to UTHSC, or by exercising reasonable diligence, would have been known to UTHSC.

For Breaches of Unsecured Protected Health Information involving less than five hundred (500) individuals, in addition to providing any other timely notification required by HIPAA, UTHSC’s Privacy and Security Officers shall maintain a log or other documentation of such Breaches and, not later than sixty (60) days after the end of each calendar year, provide the notification required by 45 C.F.R. §§ 164.408(a) to the Secretary of DHHS for Breaches discovered by UTHSC during the preceding calendar in the manner specified on DHHS’s website.

(See Items 21 and 22 of HIPAA Policies and Procedures [http://www.uthsc.edu/compliance/hipaa_policies.php])

- All faculty, staff and students must assist in UTHSC’s compliance with the risk assessment and breach notification provisions of HIPAA.

Sanctions; Disciplinary Policy

Failure of employees to comply with HIPAA and/or UTHSC policies and procedures implementing HIPAA, is a violation of the Code of Conduct, HR 580 [https://my.tennessee.edu/portal/page?_pageid=34,140536&_dad=portal&_schema=PORTAL&p_policy=HR0580] and may subject the employee to discipline, up to and including termination. Failure of

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 19 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

students to comply with HIPAA and /or UTHSC policies and procedures implementing HIPAA, is a violation of the Standards of Student Conduct Rule 1720-3-3-.02 [<http://www.uthsc.edu/centerscope/>] and may result in discipline up to and including dismissal from The University.

HIPAA requires all Covered Entities to maintain a written disciplinary policy and to consistently administer disciplinary action whenever appropriate to address violations of HIPAA privacy and security regulations. (See HIPAA Sanctions Addendum [http://www.uthsc.edu/policies/w932_document_show.php?p=527].

Whenever a UTHSC employee is found to have violated UTHSC’s HIPAA Privacy and Security policies and/or procedures, it is the responsibility of the employee’s direct supervisor in conjunction with Human Resources to take corrective action for each such violation, or to document the reason(s) for not taking any such action, as may be appropriate in any given circumstance.

SPECIFIC PRIVACY POLICIES

Access to Protected Health Information – Patient’s Rights

The Privacy Act of 1974, T.C.A. §§ 63-2-101 et seq., and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§1320d et seq., limit access to medical records.

Requests by patients to review their own PHI should be scheduled in advance, if possible, during normal business hours. The physician of record should be notified of the request. A UTHSC representative must supervise all record reviews by patients. The patient should be provided a private place to review the records. No records may be removed by the patient.

Release of Medical Records. T.C.A. §63-2-101(a)(1) requires the production of medical records to a patient or his/her representative: “Notwithstanding any other provision of law to the contrary, a health care provider shall furnish to a patient or a patient’s authorized representative a copy or summary of such patient’s medical records, at the option of the health care provider, within ten (10) working days upon request in writing by the patient or such representative. The party requesting the patient’s records is responsible for the costs of copying and mailing the records, as set forth in T.C.A. §63-2-102.

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 20 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

Access to Protected Health Information – UTHSC Employees

Access to PHI is governed by 45 C.F.R. §164.506, which provide in part: “(a) Standard: Permitted uses and disclosures. Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.”

Paragraph (c) states:

(c) Implementation specifications: Treatment, payment, or health care operations.

- (1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.
- (2) A covered entity may disclose protected health information for treatment activities of a health care provider.
- (3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.
- (4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:
 - (i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or
 - (ii) For the purpose of health care fraud and abuse detection or compliance.
- (5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 21 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

operations activities of the organized health care arrangement.

Compliance with HIPAA’s “Minimum Necessary” Rule

When using or disclosing PHI, or when requesting PHI from another Covered Entity, UTHSC shall make reasonable efforts to limit the amount of PHI used, disclosed or requested to the minimum necessary amount of PHI to accomplish the intended purpose of the use, disclosure or request.

For the purpose of this policy, protected health information means any individually identifiable health information collected or stored by the University. Individually identifiable health information includes demographic information and any information which relates to the past, present or future physical or mental condition of an individual.

- a. Individuals acting on behalf of UTHSC must always use the minimum amount of information necessary to accomplish the intended purpose of the use, access or disclosure.
- b. With respect to system access, patient privacy shall be supported through authorization, access and audit controls and should be implemented for all systems that contain identifying patient information. Within the permitted access, an individual system user is only to access what he or she needs to perform his or her job.
- c. Consistent with the Privacy Policy, the Privacy Officer and the Security Officer shall facilitate compliance with these principles in conjunction with the UTHSC Compliance Committee.

		UT Health Science Center		
HIPAA Privacy and Security Combined Policies 		Doc. Version:	1.0	Page 22 of 30
		Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
		Effective Date:	9/23/13	
			Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

Patient Requests for Amendments of Their Own PHI

A patient has a right to request an amendment to patient records in accordance with HIPAA, to amend the record unless it is proven that an error does not exist in the patient medical file. Within sixty (60) days of receipt of a request for amendment, UTHSC must accept the amendment, deny the amendment, or notify the individual in writing that a delay has prevented UTHSC from acting on the request for an amendment.

Authorization for Access, Disclosure and Release of PHI

T.C.A. §68-11-304 allows patients access to their own medical records. Upon presentation of valid identification and completion of an authorization form, patients may review their medical records in the appropriate clinical area. As a courtesy, the provider should be notified of the review. In psychiatric or other mental health cases, the practitioner shall be notified prior to allowing examination of the record by the patient.

Likewise, prior practitioner notification shall be given in cases felt to be potentially harmful to the patient.

Patient authorization is required to release information from the medical or dental record unless disclosure is permitted by HIPAA for disclosure of PHI for public health activities.

1. Information released to authorized individuals/agencies shall be strictly limited to that information required to fulfill the purpose stated on the authorization. Authorizations specifying “any and all information” or other such broadly inclusive statements shall not be honored. Release of information that is not essential to the stated purpose of the request is specifically prohibited.
2. Patient authorization is **not** required to release information from one provider to another for treatment purposes. However, it is recommended that all UTHSC providers involved receive notification when records are released and/or transferred within UTHSC.

Patient authorization is **not** required when the record is needed for administrative or financial purposes.

		UT Health Science Center		
HIPAA Privacy and Security Combined Policies 		Doc. Version:	1.0	Page 23 of 30
		Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
		Effective Date:	9/23/13	
			Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

Following authorized release of patient information, the signed authorization must be retained with the medical or dental record with notation of the specific information released, the date of release and the signature of the individual who released the information. These forms do not become part of the record and should not be released when the record or information is released. The Federal Privacy Act requires that a record of disclosures of information be maintained. This applies only to federal facilities but many other health care organizations have adopted this practice. The original patient authorization must be filed in the designated location in the medical or dental record.

Communication with family, friends and relatives of patients

We may give to a family member, or other relative, close personal friend or any other person you identify, certain parts of your health information that are directly relevant to that person's involvement in your care or payment related to your care.

Your health information will only be shared if you agree, or are silent when given the opportunity to disagree, or we believe, based on the circumstances and our professional judgment that you do not object.

If you are incapacitated or in an emergency circumstance, we may provide to a family member, or other relative, close personal friend, or any other person accompanying you, certain parts of your health information that is directly relevant to that person's involvement in your care or payment related to your care.

With written request, we will provide you with a copy of your electronic health record in electronic form and we will transmit the copy directly to another person designated by you. An electronic copy may be attached to an email that does not require encryption as long as you have been advised of the risk of transmission of an unencrypted document.

Removal of Written Records from the UTHSC Premises

Written records shall not be removed from any UTHSC practice site without written consent of the business or clinic manager. Original written medical records may be removed only by court order or subpoena. In such cases, a complete copy of the record must be made prior to removal. Upon return, the original must be compared to the copy prior to storage. Any alterations to the original must be noted and brought to the attention of the UT Office of General Counsel.

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 24 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

SPECIFIC SECURITY POLICIES

Security Rule Compliance Personnel

Policies or procedures noted as being the responsibility of the UTHSC shall be maintained at a campus level under the direction of the UTHSC Chief Information Officer (CIO). Unless otherwise specified, the Security Officer shall provide guidance the custodians and others and oversight for the UTHSC. Because the UTHSC is the owner of all information and systems, custodians are designated to act on behalf of the UTHSC. An Information Custodian acts on behalf of the UTHSC and is responsible for a particular set of information and associated computer systems. See the University of Tennessee System IT Policy IT0115 regarding Information Custodians.

[\[https://my.tennessee.edu/portal/page?_pageid=34,140536&_dad=portal&_schema=PORTAL&p_policy=IT0115\]](https://my.tennessee.edu/portal/page?_pageid=34,140536&_dad=portal&_schema=PORTAL&p_policy=IT0115)

If more than one person performs the role, only one person shall be designated as the Custodian, the others shall be associates. No group may be designated a Custodian. All networking functions, networking equipment and security functions are under the direction of the CIO.

Administrative Policies

Security Management:

Risk Analysis: UTHSC’s Security Officer shall conduct an accurate and thorough assessment of potential risks and vulnerabilities to ePHI every three (3) years. The Security Officer shall also maintain procedures for the performance of risk analyses at UTHSC, including in those procedures the addition of new systems, environmental changes, handling of “addressable” implementation specifications and mitigation of risks.

Risk Management: UTHSC’s Custodians, with the guidance of the Security Officer, shall maintain security measures to reduce risks and vulnerabilities for all systems when technically possible and consistent with regulatory guidance. Those measures shall include:

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 25 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

- Installation of “Warning Banners”
- Use of anti-virus and/or anti-malware software with current signatures
- Updating the operating system and software when patches are released by the vendor, subject to evaluation of suitability.

Information System Activity Reviews: UTHSC’s Custodians, with the guidance of the Security Officer, shall maintain procedures to review records at least monthly of information systems, including such items as audit logs, access reports and security incident tracking reports. The procedures shall address:

- Failed login attempts
- System use by unauthorized or unexpected users
- Failures and errors logged by software or processes

Evaluations: UTHSC’s Security Officer shall evaluate annually the extent to which its policies and procedures meet the requirements of the HIPAA security rule.

Security and Information Access Management:

UTHSC’s Custodians, with the guidance of the Security Officer, shall maintain written procedures for authorizing access to ePHI that are consistent with both the Privacy Rule and the Security Rule, and which provide methods for:

- the authorization and supervision of faculty, staff and students who work with ePHI, or in locations where ePHI might be accessed to ensure appropriate access to ePHI and preventing access as appropriate;
- confirmation that the access granted is appropriate;
- granting access to ePHI, through a workstation, transaction, program, process,

	UT Health Science Center		
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 26 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

etc.;

- establishing, documenting, reviewing, and modifying the right of access to a workstation, transaction, program, process, etc.; and
- terminating access to ePHI for such reasons as the end of employment, change of responsibilities, etc.

Contingency Plans:

UTHSC’s Custodians shall maintain written procedures for responding to an emergency or other occurrence that damages systems that contain ePHI. The Custodians for each system containing ePHI or supporting the creation, transmission, or storage of ePHI and/or encryption keys are responsible for maintaining a written plan or plans that must include procedures for annual testing, revision of the plans as needed, and assessment the relative criticality of their specific applications and data. These plans must address these elements:

- A data backup plan that will create and maintain retrievable exact copies of the ePHI.
- A disaster recovery plan that details the procedures to restore any loss of data.
- An emergency mode operations plan to enable the continuation of critical business processes for the security of ePHI while operating in an emergency mode.

Physical Safeguard Policies

Facility Access Controls:

The Custodians, with the guidance of the Security Officer, shall implement written procedures to: limit physical access to electronic information systems, limit access to the facilities in which they are housed, and ensure that properly authorized access is allowed. These procedures shall include:

- Allowing facility access in support of restoration of data under the disaster recovery plan and emergency mode operations plan.

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 27 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

- Safeguarding the facility and equipment therein from unauthorized access, tampering and theft.
- Validating a person's access to the facility based on their role or function including visitor control, and control of access to software programs for testing and revision.
- Documenting repairs and modifications to the physical components of the facility relating to security such as doors, locks, wall, hardware, etc.

Workstation Use:

The Custodians, with the guidance of the Security Officer shall maintain procedures specifying the proper functions to be performed, the manner in which those functions are to be performed and the physical attributes of the surroundings of specific or classes of workstations that address ePHI to:

- Reflect the job responsibilities of the user of the workstation
- Be consistent with the University of Tennessee's acceptable use policies.
[\[https://my.tennessee.edu/portal/page?_pageid=34,140536&_dad=portal&_schema=PORTAL&p_policy=IT0110\]](https://my.tennessee.edu/portal/page?_pageid=34,140536&_dad=portal&_schema=PORTAL&p_policy=IT0110)

Workstation Security:

The Custodians, with the guidance of the Security Officer shall maintain the physical safeguards on all workstations, whether a desktop or laptop configuration, to restrict access to ePHI to authorized users. Those safeguards shall include:

- Use of cable locks for all laptops in unprotected areas
- Positioning displays away from unauthorized users
- Securing unattended workstations in protected areas

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 28 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

- Use of restrictive “hardening” configurations on workstations

Device and Media Controls

Hardware and Media inside a Facility:

The Custodians, with the guidance of the Security Officer, shall maintain written procedures: addressing the final disposition of electronic media on which ePHI is stored; governing the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, the movement of these items within the facility and documenting any person responsible for that hardware and electronic media; the removal of ePHI from electronic media before the media is made available for re-use; and creating an exact copy of ePHI before the movement of equipment.

Surplus Equipment:

UTHSC’s Surplus Property with the guidance of the Security Officer shall maintain written procedures addressing the final disposition of equipment on which ePHI is stored. These procedures shall include:

- Criteria for purging or destruction
- Methods for purging or destruction

Technical Safeguard Policies

Access Control:

UTHSC’s Custodians, with the guidance of the Security Officer, shall maintain technical procedures for:

- systems containing ePHI to require unique individual user identification for each user (group or shared identification is not permitted for users);

		UT Health Science Center	
HIPAA Privacy and Security Combined Policies 	Doc. Version:	1.0	Page 29 of 30
	Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
	Effective Date:	9/23/13	
		Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

- obtaining ePHI during an emergency;
- termination of an electronic session after ten minutes of inactivity or in the event the system is incapable of that termination, run a password protected screen saver after ten minutes of inactivity;
- a mechanism approved by UTHSC to encrypt and decrypt ePHI stored on electronic media, including portable media used in connection with any system storing ePHI or encryption keys. Encryption of ePHI stored on laptops, portable devices and portable media is required using an encryption algorithm validated by the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program for the current FIPS 140 standard. [<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>]

Audit Controls:

The Custodians, with the guidance of the Security Officer, shall maintain hardware, software and /or procedural mechanisms to record and examine activity in information systems that contain or use ePHI. These events shall be audited:

- Failed login attempts
- System use by unauthorized or unexpected users
- Failures and errors logged by software or processes

Data Integrity:

The Custodians, with the guidance of the Security Officer, shall maintain electronic mechanisms to protect ePHI from improper alteration or destruction in an unauthorized manner. Conformance shall be verified by test procedures specified by NIST.

[http://healthcare.nist.gov/docs/170.302.s_Integrity_v1.1.pdf]

Authentication:

		UT Health Science Center		
HIPAA Privacy and Security Combined Policies 		Doc. Version:	1.0	Page 30 of 30
		Revised by:	F. Davison W. Schuler C. Moffitt	Revision Date: 9/23/13
		Effective Date:	9/23/13	
			Anthony A. Ferrara, C.P.A., M.A.S. Vice Chancellor for Finance and Operations	

The Custodians, with the guidance of the Security Officer, shall maintain written procedures to verify that a person or entity seeking access to ePHI is the one claimed including:

- Use of multi-factor authentication as appropriate
- Use of “strong” password construction.

Transmission Security:

The Custodians, with the guidance of the Security Officer, shall maintain technical measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of. UTHSC shall implement a mechanism to encrypt ePHI in transit over open networks. Transmission of ePHI over the Internet (even when sending from one uthsc.edu email address to another uthsc.edu email address) without encryption is prohibited, except that a UTHSC staff member, faculty member or student may communicate with a patient or the patient’s authorized representative via unencrypted email if (1) the UTHSC staff member, faculty member or student has notified the patient or the patient’s authorized representative in writing that there may be some level of risk that the information in the email could be read by a third party, (2) the patient or the patient’s representative responds in writing that the patient still prefers the unencrypted email, and (3) the UTHSC staff member, faculty member or student maintains a copy of these written communications with the patient or the patient’s representative and provides a copy of such communications to the HIPAA Privacy and Security Officers (who shall maintain such communications in UTHSC’s files) prior to transmitting any unencrypted ePHI over the Internet. The encryption algorithms employed shall have been validated by the NIST Cryptographic Module Validation Program for the current FIPS 140 standard. [<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>]

[End of Document]