

<p style="text-align: center;"><b>The University of Texas SOUTHWESTERN MEDICAL CENTER At Dallas</b></p>	<p style="text-align: center;"><b>Privacy Compliance Program Privacy Manual</b></p> <p style="text-align: center;">Section 6: Uses, Disclosures and Requests of PHI</p> <p>Policy No: 6.2 Last Revised: March 20, 2003 Effective Date: April 14, 2003</p>
<p><b>Access and Use of Protected Health Information</b></p>	

**POLICY:**

UT Southwestern Workforce may access and use PHI consistent with their job functions, in circumstances permitted by this Manual and the Privacy Laws. Where required by the minimum necessary rule, UT Southwestern will make reasonable efforts to limit Workforce access and use of PHI to the minimum use necessary to achieve the purpose of the use.

**PROCEDURE:**

1. What is a Use?
  - a. Definition. For purposes of this Policy, “use” of PHI is the sharing, employment, application, utilization, examination, or analysis of PHI by and among UT Southwestern Workforce. See also Section 1.2 of this Manual, which sets forth the Definitions.
  - b. Use versus Disclosure. This policy does not apply to the “disclosure” of PHI to persons outside UT Southwestern. See Section 6.3 of this Manual for the policy and procedure on Disclosures of Protected Health Information.
  
2. Compliance With The Minimum Necessary Rule
  - a. Generally. UT Southwestern will comply with the minimum necessary rule for uses of PHI in circumstances where the rule is applicable. For situations where the minimum necessary rule is not applicable, see Section 6.1 of this Manual, which sets forth the policy and procedure on the Minimum Necessary Rule.
  - b. Entire Medical Record. If the minimum necessary rule applies to the use, UT Southwestern Workforce will not use the entire medical record unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the disclosure. To determine whether the minimum necessary rule applies, see Section 6.1 of this Manual for the policy and procedure on the Minimum Necessary Rule.

3. Categories of Workforce Who Need PHI Access
  - a. The Department Manager, or designee, shall identify the members of UT Southwestern's Workforce that need access to PHI to carry out their job functions.
  - b. Access to Electronic Systems.
    - i. When possible, access to electronic PHI is authorized based upon the users role and responsibilities at UT Southwestern (role-based access). Each user is assigned to one or more predefined access profiles, each of which has been assigned various levels of privileges needed to perform the duties assigned.
    - ii. When role-based access is not applicable, the Department Manager will authorize and submit an Inter-institutional Access Request (IAR) to the System Account Management (SAM) group for the creation of a user account.
    - iii. The SAM group will obtain an Inter-Institutional Security Agreement (ISA) from the requesting individual.
    - iv. The SAM group is responsible for maintaining user account and access authorization documentation for all electronic systems containing PHI. For more information see Policy 200-4 of the Information Security Program Security Manual which sets forth the policy and procedure on Information Access Management. <insert link>
  - c. Access to Paper-based Medical Records.
    - i. Access to the Ambulatory Services Medical Record will be accomplished through the Chart Tracking System. Users of the Chart Tracking System will only be granted access in accordance section 3b of this policy.
    - ii. Access to other paper-based medical records not using the Chart Tracking System will be subject to approval by the HIM Director, HIM Manager or designee. The HIM Director, HIM Manager or designee, will be responsible for maintaining documentation of access.
  - d. All employees will complete the appropriate Privacy and/or Security training prior to obtaining access to electronic or paper PHI.
  - e. Access may be granted to Workforce members and independent contractors with an on-site workstation designated as Workforce by UT Southwestern.
4. Categories of PHI To Which Workforce Need Access
  - a. Identification. The Department Manager, or designee, shall identify the categories or types of PHI to which each person or group of persons needs access consistent with their job responsibilities ("Access Rights").
  - b. When possible, Access Rights are authorized based upon the user's job responsibilities. Users are assigned one or more pre-defined access profiles for that job type. Individual-based Access Rights will be used when role-based profiles are not applicable or possible.
  - c. Scope of Access. In establishing Access Rights, the Department Manager, or designee will establish any conditions appropriate to the Access Rights and make reasonable efforts to limit access by Workforce to the amount of PHI necessary to perform their job functions.

- d. The Department Manager, or designee, will establish reasonable safeguards to limit access to areas containing PHI.
5. Ongoing Review. Privacy and Security compliance activities shall include periodic review of the categories of Workforce who are granted access to PHI, and the categories of PHI to which the Workforce need access.
7. Access Controls
- a. Controlling What PHI is Accessed. Department Managers, or designee, will make reasonable efforts to limit the access to PHI by Workforce members under their control in accordance with the established Access Rights for such persons. Workforce will report any identified violations of Access Rights immediately to the Security and/or Privacy Officer. Access Controls will address both physical and electronic access.
  - b. Emergency Overrides. There shall be at least one person on-site or on-call to UT Southwestern at all times with the capability to override any barriers (electronic or physical) to accessing PHI in emergency situations.
    - i. Whenever possible, such access should be accomplished by Information Security personnel and the relevant information forwarded to the requestor.
    - ii. In certain circumstances, emergency access may be granted directly to the requestor for a limited time. In all cases, emergency access will be authorized by the Information Security Officer, or designee.
    - iii. The Information Security Officer, or designee, will be responsible for maintaining documentation of all emergency access.
    - iv. Emergency access to the Medical Record is available by contacting the HIM personnel on call. For more information regarding emergency access to Ambulatory Services Medical Records, see Ambulatory Services Policy 7-01 which sets forth the policy and procedure for After-Hours Availability of Medical Records. <insert link>

---

**LEGAL REFERENCES:**

45 C.F.R. §§ 160.103, 164.502, 164.514(d)(2) (2001)  
65 Fed. Reg. 82462, 82480, 82544-45, 82570, 82575, 82579, 82630, 82712-16, 82746 (Dec. 28, 2000); 67 Fed. Reg. 53182, 53195-99, 53205 (Aug.14, 2002)