

**Travis County Emergency Services District No. 9**  
**Westlake Fire Department**  
**Standard Operating Guideline**

**Subject:** Health Insurance Portability and Accountability Act Compliance

**Effective Date:** March 7, 2003

**Authorized By:** Chief Paul Barker

---

**I. History**

The privacy provisions of the federal law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), apply to health information created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses. The Department of Health and Human Services (HHS) has issued the regulation, "Standards for Privacy of Individually Identifiable Health Information," applicable to entities covered by HIPAA. Under the Privacy Rule, health plans, health care, clearinghouses, and certain health care providers must guard against misuse of individuals' identifiable health information and limit the sharing of such information, and consumers are afforded significant new rights to understand and control how their health information is used and disclosed.

**II Purpose**

To outline levels of access to Protected Health Information (PHI) of employees and patients of WFD and to provide a policy and procedure on limiting access to and disclosure and use of PHI.

**II. Policies**

1. Access to PHI will be limited to those who need access to carry out their duties.
2. PHI information will not be released, unless an official request is made by the patient, the employee, or their designee (by Power of Attorney).
3. PHI may be released without patient consent only for treatment or billing purposes.
4. PHI will be kept separate from employee personnel files. All PHI information will be kept in a locked storage container.
5. Chief Officers are the designated HIPAA contact and must approve any release of PHI for any other purpose.
6. A Patient Disclosure Notice will be given to each patient by the Department or A/TC EMS after / during transport.

### III Procedure

1. Request for PHI
  - a. Requests for PHI must be in writing by the patient, employee or their designee (by Power of Attorney).
  - b. Verification will be made for any request of PHI.
  - c. Information will be processed as soon as possible by the administrative office.
2. Verbal Security
  - a. All personnel will be sensitive of verbally disclosing information in public areas such as garages, waiting rooms, and away from work. Discussions of patient information will be spoken in normal speaking tones when relaying information between HIPPA Compliant entities.
3. Physical Security
  - a. Patient care forms, worksheets, and other records used to gather patient information shall be stored in secured areas such as filing cabinets, desk drawers or envelopes until the patient record is completed. When the patient record is completed, these worksheets or unused forms will be destroyed. At no time shall any worksheet or form be left unattended in a way the general public could read or see them. This includes leaving worksheets or forms exposed in the cabs of apparatus.
4. Photographs, Videotapes, Digital or Other Images
  - a. Images that identify the patient through licenses plates, markings on bodies such as tattoos, or facial photos / images shall not be used for training or publication without the written consent of the patient or their legal representative.
5. Computers and Entry Devices
  - a. Computer access terminals and other remote entry devices such as PDAs and laptops should be kept secure. Access to any computer device should be by password only. Personnel should be sensitive to who may be within viewing range of monitor screens and take simple steps to shield viewing by unauthorized personnel. All remote devices should remain in the physical possession of the individual it is assigned to at all times.