

Title: HIPAA Compliance - Administration

**Date Issued: December 6, 2005
Date Last Revised: NEW
Revision Number: NEW
Total Pages: 8**

Purpose: To provide a policy and procedure on limiting access, disclosure, and use of Protected Health Information (PHI); to provide policies outlining patient rights and Winter Park Fire-Rescue Department's (WPFRD) responsibilities in fulfilling patient requests; and to establish an acceptable format and consistent procedure to enable WPFRD to become compliant with *The Health Insurance Portability and Accountability Act of 1996* (HIPAA). Security of PHI is everyone's responsibility.

Scope: This procedure applies to all Winter Park Fire-Rescue (WPFRD) personnel and Public Safety Personnel working with WPFRD.

300.07.01. Policy and Responsibility

WPFRD retains strict requirements on the security, access, disclosure and use of PHI. When PHI is accessed, disclosed and used, the individuals involved will make every effort, except in patient care situations, to only access, disclose and use PHI to the extent that only the minimum necessary information is used to accomplish the intended purpose.

Patients may exercise their rights to access, amend, restrict, and request an accounting, as well as lodge a complaint with either WPFRD or the Secretary of the Department of Health and Human Services.

It shall be the policy and responsibility of all personnel who may have or had access to PHI to understand and follow all policies and procedures related to HIPAA.

300.07.02. Procedure

As a health care provider, the group must be compliant with the HIPAA Privacy Rule by April 14, 2003. Therefore, beginning on that date, the following must be adhered to:

- **Administrative Personnel**

Under HIPAA, individuals have the right to access and to request amendment or restriction on the use of their PHI, and restrictions on its use that is maintained in **Designated Record Sets (DRS)**

A. Patient Access:

1. Upon presentation to the Privacy Officer or his/her designee, the patient or appropriate representative (a parent of a minor, a person with power of attorney for the patient, a court appointed guardian or family member of a deceased patient) will complete a **Request for Access Form**. A valid driver's license or military identification (a Social Security card will not be accepted) will be used to verify the identity of the patient or appropriate representative.
2. The Privacy officer or his/her designee will act upon the request immediately if the records are stored at WPFDRD's office. If the records are stored off site, the request will be made within fourteen (14) working days.
3. The privacy Officer or his/her designee will act upon the request immediately to retrieve stored records from the WPFDRD office, or designated storage area.

B. Amendment to PHI:

The patient or appropriate representative may request an amendment to their PHI. This request will be done through the Privacy Officer or his/her designee. The patient will do this by completing a Request for Amendment of PHI form provided by the Privacy Officer or his/her designee. The only PHI that can be amended are; name, address, current medical condition, past medical condition, current medications, allergies or insurance information.

C. Restriction of PHI use:

WPFDRD is not required to agree to any restrictions, and given the nature of our operation, we will not agree to a restriction without advice from legal counsel to do so.

D. Designated Record Sets:

1. Under the Privacy Rule, the Designated Records Set (DRS) includes medical records that are created by WPFRD to make decisions about the patient. Items that are considered part of a DRS are:
 - a. The Abbreviated EMS Report created by EMS field personnel (this includes photographs, monitor strips, Physician Certification Statements, Refusal of Care forms), or any other source of data that is incorporated and/or attached to the Abbreviated EMS Report.
 - b. The claims records or other paper records of submission of actual claims to Medicare or other insurance companies.
 - c. Any patient-specific claim information, including responses from insurance payers, such as remittance advice statements, Explanation of Medicare Benefits (EMOBs), charge screens, patient account statements, and signature authorization and agreement to pay documents.
 - d. Amendments to PHI, or statements of disagreement by the patient requesting the amendment, or an accurate summary of the statement of disagreement.
2. The DRS also includes copies of records created by other service providers and other health care providers such as first responder units, assisting ambulance services, air medical services, nursing homes, hospitals, police departments, coroners office, etc., that are used by WPFRD as part of treatment and payment purposes related to the patient.

E. Role Based Access:

Access to PHI will be limited to those who need access to PHI to carry out their duties. The following describes the categories or types of PHI to which such persons need access is defined and the conditions, as appropriate, that would apply to such access.

Job Title	Description of PHI to Be Accessed	Conditions of Access to PHI
EMT	Intake forms from dispatch, patient care reports	May access only as part of completion of a patient event and post-event activities and only while actually on duty
Paramedic	Intake forms from dispatch, patient care reports	May access only as part of completion of a patient event and post-event activities and only while actually on duty
Billing Clerk	Intake forms from dispatch, patient care reports, billing claim forms, remittance advice statements, other patient records from facilities	May access only as part of duties to complete patient billing and follow up and only during actual work shift
Field Supervisor	Intake forms from dispatch, patient care reports	May access only as part of completion of a patient event and post-event activities, as well as for quality assurance checks and corrective counseling of staff
Dispatcher	Intake forms, preplanned CAD information on patient address	May access only as part of completion of an incident, from receipt of information necessary to dispatch a call, to the closing out of the incident and only while on duty
Training Coordinator	Intake forms from dispatch, patient care reports	May access only as a part of training and quality assurance activities. All individually identifiable patient information should be redacted prior to use in training and quality assurance activities
Department Managers		May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel

Access to a patient's entire file will not be allowed except when expressly permitted by company policy or approved by the Privacy Officer.

300.07.03. Incidental Disclosures

WPFRD understands that there will be times when there are incidental disclosures about PHI in the context of caring for a patient. The privacy laws were not intended to impede common health care practices that are

essential in providing health care to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversation between health care providers, or when patient care information in written or computer form is left out in the open for others to access or see.

The fundamental principle is that all staff needs to be sensitive about the importance of maintaining the confidence and security of all material we create or use that contains patient care information. Coworkers and other staff members should not have access to information that is not necessary for the staff member to complete his or her job. For example, it is generally not appropriate for field personnel to have access to billing records of the patient.

However, all personnel must be sensitive to avoiding incidental disclosures to other health care providers and others who do not have a need to know the information. Pay attention to who is within earshot when you make verbal statements about a patient's health information, and follow some of these common sense procedures for avoiding accidental or inadvertent disclosures:

300.07.04. Verbal Security

Waiting or Public Areas: If patients are in waiting areas to discuss the service provided to them or to have billing questions answered, make sure that there are no other persons in the waiting area, or if so, bring the patient into a screened area before engaging in discussion.

Garage Areas: Staff members should be sensitive to that fact that members of the public and other agencies may be present in the garage and other easily accessible areas. Conversations about patients and their health care should not take place in areas where those without a need to know are present.

Other Areas: Staff members should only discuss patient care information with those who are involved in the care of the patient, regardless of your physical location. You should be sensitive to your level of voice and to the fact that others may be in the area when you are speaking. This approach is not meant to impede anyone's ability to speak with other health care providers freely when engaged in the care of the patient. When it comes to treatment of the patient, you should be free to discuss all aspects of the patient's medical condition, treatment provided, and any of their health information you may have in your possession with others involved in the care of the patient.

300.07.05. Physical Security

Patient Care and Other Patient or Billing Records: Patient care reports should be stored in safe and secure areas. When any paper records concerning a patient are completed, they should not be left in open bins or on desktops or other surfaces. Only those with a need to have the information for the completion of their job duties should have access to any paper records.

Billing records, including all notes, remittance advices, charge slips or claim forms should not be left out in the open and should be stored in files or boxes that are secure and in an area with access limited to those who need access to the information for the completion of their job duties.

Computers and Entry Devices: 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. Staff members should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All remote devices such as laptops and PDAs should remain in the physical possession of the individual to whom it is assigned at all times. See the ABC Ambulance Policy on Use of Computer Equipment and Information Systems.

300.07.06. Penalties for Violation

WPFRD takes its responsibility to safeguard patient information very seriously. There are significant legal penalties against companies and individuals that do not adhere to the laws that protect patient privacy.

Staff members who do not follow our policies on patient privacy will be subject to disciplinary action, up to and including verbal and written warnings, suspension and/or termination from the organization. WPFRD shall make every effort to provide remedial education and training as to our policies and procedures when there is a first time violation of our policies.

300.07.07. Questions About This Policy or Any Privacy Issues

WPFRD has appointed a Privacy Officer to oversee our policies and procedures on patient privacy and to monitor compliance. The Privacy Officer is also available to you for consultation on any issues or concerns you have about how WPFRD deals with protected health information. You should feel free to contact the Privacy Officer at any time with your questions or concerns.

WPFRD will not retaliate against any staff member who expresses a good concern or complaint about any policy or practice related to the safeguarding of patient information and WPFRD's legal obligations to protect patient privacy.

300.07.08. Medical Records of Employees:

WPFRD will, to the extent required by law, protect medical records it receives about employees or other staff in a confidential manner. Generally, only those with a need to know the information will have access to it, and, even then, will only have access to as much information as is minimally necessary for the legitimate use of the medical records. In accordance with laws concerning disability discrimination, all medical records of staff will be kept in separate files apart from the employee's general employment file. These records will be secured with limited access by management.

Employment records are not considered to be protected health information, or PHI, subject to HIPAA safeguards, including certain medical records of employees that are related to the job. These employment records not covered under HIPAA include, but are not limited to: information obtained to determine my suitability to perform the job duties (such as physical examination reports), drug and alcohol tests obtained in the course of employment, doctor's excuses provided in accordance with the attendance policy, work-related injury and occupational exposure reports, and medical and laboratory reports related to such injuries or exposures, especially to the extent necessary to determine workers' compensation coverage.

Nonetheless, despite the fact that such records are not considered HIPAA protected, WPFRD will limit the use and disclosure of these records to only those with a need to have access to them, such as certain management staff, WPFRD designated physician, and state agencies pursuant to state law.

With respect to staff members of WPFRD, only health information that is obtained about staff in the course of providing ambulance or other medical services directly to them is considered PHI under HIPAA. In other words, if WPFRD provides ambulance service to an employee, the protections typically given to such information of our ambulance service patients applies to the employee. These protections are subject to HIPAA exceptions, such as in the situation in which the staff member who used WPFRD was involved in a work-related injury while on duty.

As another example, if we receive a staff member's medical record in the course of providing the employee with treatment and/or transport, it does not matter that WPFRD happens to be the employer – that record is PHI. If, however, the employee submits a doctor's statement to a supervisor to

document an absence or tardiness from work, WPFRD does not need to treat that statement as PHI.

Any questions regarding application of the foregoing policies and procedures should be directed to the Privacy Officer, who may consult with legal counsel regarding the issue(s) if needed.