



City of Winter Park Fire-Rescue Standard Operating Guideline

300.06

Title: HIPAA Compliance - Operations

Original Date Issued: December 6th, 2005

Date Last Revised: October 5th, 2010

Revision Number: 1

Total Pages: 4

Purpose: To provide a policy and procedure on limiting access, disclosure, and use of *Protected Health Information* (PHI) and to provide policies outlining patient rights and Winter Park Fire-Rescue Department's (WPFDR) responsibilities in fulfilling patient requests; and to establish an acceptable format and consistent procedure to enable WPFDR 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 WPFDR personnel and Public Safety Personnel working with WPFDR.

300.06.01. Policy and Responsibility

WPFDR 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 WPFDR or the Secretary of the Department of Health and Human Services. If such request or complaint arises, you should provide the patient with the name and contact information of the Privacy Officer, and report such request or complaint to the Privacy Officer.

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.

300.06.02. 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:

- **Personnel/Employees**

1. Under HIPAA, it is mandatory that all patients receive a copy of “The Notice of Privacy Practices”. The WPFD will provide this notice to all patients that are treated. Each patient is required to sign an acknowledgement that he/she has received such Notice.
 - a. Emergency Settings or Unconscious Patients: If a patient is unable to receive a Notice or is unable to sign an acknowledgement of receipt, you are required to either:
 - (1) Give such notice to a family member and have such family member sign the acknowledgment of receipt on behalf of patient;
 - (2) Provide the Notice to hospital or other EMS personnel who assumes care for the patient and have such personnel sign the acknowledgment and give the patient or his/her family a copy of the Notice; or
 - (3) Indicate in detail why the patient was unable to receive the Notice or sign the acknowledgement of receipt, and provide such information to the Privacy Officer.
 - b. If the patient refuses transport, it will be required that the Notice be provided to them at the time of refusal. The patient is then to sign the appropriate section on the refusal form. At the end of each shift any applicable refusal forms must be forwarded to the office where they will be kept on file for six (6) years.
2. Patient care reports must be completed according to SOG 300.02 “Patient Care Report”. It is imperative that all Patient Care Reports be signed and closed at the end of each shift. This action will ensure that all PHI is properly secured. All copies of the Patient Care Reports, other than those provided to and maintained by the Privacy Officer or other WPFD administration personnel, shall be shredded in the stations.
3. Oral Communications – Under HIPPA, WPFD may transmit information to receiving facilities for the purpose of relaying information about incoming patients. However, at the time of patient transfer, please ensure you patient report is securely relayed and only to the appropriate staff.
4. Disclosure of PHI to First Responders and Law Enforcement – As a general rule, WPFD will not disclose PHI to First Responders beyond that which is genuinely needed for treatment purposes. WPFD may give PHI to law enforcement only if the information is requested through subpoena or a Court order, and only such information which is explicitly requested in such subpoena and Court order, nothing more (a/k/a the “minimum necessary rule”).

5. WPDF personnel shall make every attempt to secure a patient's PHI from view of others not directly involved in the treatment of such patient.
6. WPDF personnel shall not discuss or provide a patient's PHI with others who are not directly involved in the treatment of that patient, except to the WPDF administration responsible for securing the PHI or responsible for billing Medicare, Medicaid or other insurers.

300.06.03. 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 / Bay Areas: Staff members should be sensitive to the 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.

300.06.04. 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.

300.06.05. Penalties for Violation

WPFDD 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.

300.06.06. Questions About This Policy or Any Privacy Issues

WPFDD 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 WPFDD deals with protected health information. You should feel free to contact the Privacy Officer at any time with your questions or concerns.

WPFDD 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 WPFDD's legal obligations to protect patient privacy.

If you have any questions about how medical information about you is used and disclosed by WPFDD, please contact our Privacy Officer.



James E. White
Chief of Department