

<b>Standard Operating Procedure</b>  <b>HEALTH INSURANCE PORTABILITY AND ACCOUNTAVILITY ACT (HIPAA) ACCESS</b>	<b>PEORIA FIRE-MEDICAL DEPARTMENT EMS</b>  <b>400.16</b>  <b>Rev. 02/21/2008</b> <b>Page 1 of 5</b>
--	---

**PURPOSE**

- To outline levels of access to Protected Health Information (PHI) for various staff members of Peoria Fire-Medical Department (PFD)
- To provide a policy and procedure on limiting access, disclosure, and use of PHI.
- To provide policies outlining patient rights and PFD's responsibilities in fulfilling patient requests for PHI.

**POLICY**

PFD retains strict requirements on the security, access, disclosure and use of PHI. Access, disclosure and use of PHI will be based on the role of the individual staff member in the organization, and should be only to the extent that the person needs access to PHI to complete necessary job functions. Security of PHI is everyone's responsibility.

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 PFD or the Secretary of the Department of Health and Human Services.

<b>Standard Operating Procedure</b>	<b>PEORIA FIRE-MEDICAL DEPARTMENT</b>
<b>HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) ACCESS</b>	<b>EMS</b>
	<b>400.16</b>
	<b>Rev. 02/21/2008 Page 2 of 5</b>

### 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 specific categories or types of PHI to which such persons need access is defined and the conditions, as appropriate, that would apply to such access.

<b>Job Title</b>	<b>Description of PHI to Be Accessed</b>	<b>Conditions of Access to PHI</b>
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
Behavioral Health Specialist	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 on duty
Admin Staff Account & Records Clerks and Administrative personnel	Patient care reports, other patient records	May access only as part of duties to complete billing and follow up, statistical analysis and to comply with legal requests such as subpoenas and only during actual work shift
EMS Staff to include Paramedics, Nurses, Medical Director, and support Staff	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. May also access to complete billing and follow up, statistical analysis and to comply with legal requests such as subpoenas and only during actual work shift
Department Managers, Senior Staff, Battalion Chiefs, and support staff		May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel. 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.

<b>Standard Operating Procedure</b>  <b>HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) ACCESS</b>	<b>PEORIA FIRE-MEDICAL DEPARTMENT</b>  <b>EMS</b>  <b>400.16</b>  <b>Rev. 02/21/2008</b> <b>Page 3 of 5</b>
--	---

Access to PHI is limited to the above-identified persons only, and to the identified PHI only, based on the Department's reasonable determination of the persons or classes of persons who require PHI, and the nature of the health information they require, consistent with their job responsibilities.

For all other requests, determine what information is reasonably necessary for each on an individual basis.

**Incidental Disclosures**

The Department 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.

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:

**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.

<b>Standard Operating Procedure</b>  <b>HEALTH INSURANCE PORTABILITY AND ACCOUNTAVILITY ACT (HIPAA) ACCESS</b>	<b>PEORIA FIRE-MEDICAL DEPARTMENT</b>  <b>EMS</b>  <b>400.16</b>  <b>Rev. 02/21/2008</b> <b>Page 4 of 5</b>
--	---

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.

### **Physical Security**

Patient Care and Other Patient 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.

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

### **Penalties for Violation**

The Department takes its responsibility to safeguard patient information very seriously. There are significant legal penalties against entities 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. The Department 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.

