Disclaimer – This model policy does not constitute legal advice. Fire Departments using this policy as a model should consult with your department's attorney for applicability in your state and to conform to and not conflict with existing companion policies or existing State or Federal laws.

Contributor – Eastside Fire & Rescue, Issaquah, Washington

SUBJECT: HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)

---

1 Purpose

1.1 To outline levels of access to Protected Health Information (PHI) by staff members and to provide a policy and procedure on limiting access, disclosure, and use of PHI.

1.2 This is a companion document to the routing of the Medical Incident Report Form (MIRF).

2 Reference

2.1 Federal Health Insurance Portability & Accountability Act (HIPAA)

3 Responsibility

3.1 Chief of the Department is responsible for enacting this policy.

3.2 The Privacy Officer shall be the Logistics Chief and review all requests for disclosure of PHI.

3.3 All _____ Fire Department Firefighters, EMTs, Battalion Chiefs, Officers, Training Captains and Staff, Volunteer Firefighters, Paramedics Paramedic Contract employees, Information Service Manager, Front Office Staff, Accounting Clerks, Dispatchers, and Department Managers are responsible to comply with the provisions contained herein.

3.4 All of the positions outlined above are responsible for completing the required on-line training as provided.

4 Policy

4.1 The _____ Fire Department retains strict requirements on the security, access, disclosure and use of PHI. Access, disclosure, and use of PHI is 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 essential job functions.

5 Procedures/Guidelines

5.1 When the PHI is accessed, disclosed, transmitted or used for department purposes, the individuals involved will make every effort, except in patient care situations, to limit access, disclosure and us of PHI so that only the minimum necessary information is used to accomplish the intended

purpose to include information related to PHI for employees of _____ Fire Department.

5.2 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 and the conditions, as appropriate that would apply to such access.

Job Title	Type of PHI	Conditions of Access
1st Responder	Intake forms (dispatch) Patient Care Reports	Access only during event post-event; only on-duty
EMT	Intake forms (dispatch) Patient Care Reports	Access only during event post-event; only on-duty
Paramedic	Intake forms (dispatch) Patient Care Reports	Access only during event post-event; only on-duty
Battalion Chief	Same as above	Same as above, plus QA and corrective counseling
Training Captain	Same as above	Only for training and QA, With patient ID redacted prior to use
Accounting Clerk	Intake forms, claim forms, remittance statements and other patient records	Access only for billing duties and follow-up; only on-duty
Dispatcher	Intake forms and CAD Info. On address	Access only during call close-out; only on-duty
Dept. Managers	Any Type	Access only to monitor compliance and to supervise and manager
Human Resources	Any Type	Access and Transfer of PHI information relevant to the employee.
QI/QA Committee	Any Type	Access and Transfer of PHI information relevant to the employee.

Contract Paramedic	Any Type	Access and Transfer of PHI information relevant to the employee.
Privacy Officer	Any Type	Shall screen PHI requests

Access to PHI is limited to the above-identified persons only, and to the identified PHI only, based on the Agency'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.

Access to a patient's entire file will not be allowed except when provided for in this and other policies and procedures. Justification for use of the entire medical record must be specifically documented.

5.3 Disclosures to and authorizations from the patient

5.3.1 Disclosures to the patient and disclosures authorized by the patient are exempt from these "minimum necessary" requirements unless the authorization to disclose PHI is requested by the Agency.

5.3.2 Authorizations received directly from third parties, such as Medicare or insurance companies, which direct the Agency to release PHI to those entities, are not subject to the minimum necessary standards.

5.3.2.1 For example, if we have a patient's authorization to disclose PHI to Medicare, Medicaid, or another health insurance plan for claim determination purposes, the Agency is permitted to disclose the PHI requested without making any minimum necessary determination.

5.4 Disclosures to and authorizations from the Employee.

5.4.1 Disclosures to the employee and disclosures authorized by the employee are exempt from these "minimum necessary" requirements unless the authorization to disclose PHI is requested by the Agency.

5.4.2 Authorizations received directly from third parties, such as Medicare or insurance companies, which direct the Agency to release PHI to those entities, are not subject to the minimum necessary standards. For example, if we have an employee's authorization to disclose PHI to Medicare, Medicaid, or another health insurance plan for claim determination purposes, the Agency is permitted to disclose the PHI requested without making any minimum necessary determination.

5.5 Agency Requests for PHI

5.5.1 If the Agency needs to request PHI from another health care provider on a routine or recurring basis, we must limit our requests to only the reasonably necessary information needed for the intended purpose, as described below. For requests not covered

below, you must make this determination individually for each request and you should consult your supervisor for guidance. For example, if the request is non-recurring or non-routine, like making a request for documents via a subpoena, we must ensure our request covers only the minimum necessary PHI to accomplish the purpose of the request.

Holder of PHI	Purpose of Request	Info. Reasonably Necessary
Nursing facilities	To have adequate Records for treatment	Patient face sheets, discharge billing summaries, physician statements
Hospitals	Same as above	Same as above
Mutual Aid Providers	Same as above, for joint billing of patients	Patient Care Reports

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

5.6 Incidental Disclosures

5.6.1 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. Incidental disclosures are inevitable, but these will typically occur in 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.

5.6.2 The fundamental principle is that all staff needs to be sensitive about the importance of maintaining the confidentiality and security of all PHI. 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.

5.6.3 All personnel must be sensitive to avoiding incidental disclosures to anyone who does 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:

5.7 Verbal Security

5.7.1 Waiting or Public Areas: If patients are in waiting areas, 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.

5.7.2 Garage Areas: 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.

5.7.3 Other Areas: Staff members should only discuss PHI 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 a 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. Gossip or story telling that includes direct or indirect PHI will not be tolerated and will be strictly enforced.

5.8 Physical Security

5.8.1 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 information for the completion of their job duties should have access to any paper records. All completed reports must be placed in a non-see through envelope upon completion of that report. Multiple reports can be sent to Billing as long as they are in a non-see through envelope.

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 ad in an area with access limited to those who need access to the information for the completion of their job duties.

5.8.2 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 assigned at all times. Never leave a computer screen with PHI displayed on it. If dispatched to

a call while working on a medical report, the report must be saved and logged off before responding to ensure proper PHI security.

5.9 Violations

5.9.1 Violations of this Policy shall fall under the provisions found in the Discipline Policy