

Alton Fire & Rescue Department Standard Operating Guidelines (SOG)

SOG 1.1.8 Protected Health Information – Access, Security and Disclosure
(Reference SOP 1.1.8)

PURPOSE: This guideline outline levels of access to Protected Health Information (PHI) for various members of the Department, and to provide for the limits of access, disclosure, and use of PHI; and to provide guidelines outlining patient rights and the Department’s responsibility in fulfilling patient requests.

SCOPE: All Protected Health Information attained by the Department.

SPECIFICS: The Department ensures that the rules and regulations set forth by the Health Insurance Portability and Accountability Act (HIPAA) will be strictly adhered to for the protection of patient’s Protected Health Information.

DATE: Approved November 3, 2008

Alton Fire & Rescue Department

Standard Operating Procedures (SOP)

SOP 1.1.8 Protected Health Information – Access, Security and Disclosure

PURPOSE: To outline the specific procedures implementing the guidelines set for by the Health Insurance Portability and Accountability Act (HIPAA) regarding patient's Protected Health Information (PHI).

SCOPE: All protected health information.

SPECIFICS:

1. The 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 individual personnel in the Department, and only to the extent access is necessary to complete job requirements.
2. When PHI is accessed, disclosed, and used, personnel 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.
3. Patients may exercise their rights to access, amend, restrict, and request an accounting, as well as lodge a complaint with either the Department or the Secretary of the Department of Health and Human Services.
4. The following describes role based access. Access to PHI is limited to those who need it to carry out their duties. Each category or type of PHI is described as well as the conditions as appropriate that would apply to such access.
 - a. Emergency Medical Services personnel (First Responder, EMT-B, EMT-I, Paramedic). Intake forms, patient care reports. Accessed only as part of completion of a patient event and post-event activities and only while actually on duty.
 - b. Billing Clerk. Intake forms, patient care reports, billing claim forms, remittance advice statements, other patient records from facilities. Accessed only as part of duties to complete patient billing and follow up and only during actual working hours.
 - c. Incident Commander. Intake forms, patient care reports. Accessed only as part of completion of a patient event and post-event activities and only while actually on duty.
5. Access to PHI is limited to the above identified personnel and PHI only, based on the Department's reasonable determination of the person or

persons who require PHI, and the nature of the health information they require, consistent with job responsibilities.

6. Access to a patient's entire file will not be allowed except when expressly permitted by Department policy or approved by the privacy officer.
7. Disclosures to and Authorizations from the patient:
 - a. Personnel are not required to limit disclosure to the minimum amount of information necessary when disclosing PHI to other health care providers for patient treatment. This includes doctors, nurses, etc at the receiving hospital, any mutual aid provider, fellow crew members involved in the call, and any other person involved in the treatment of the patient who has a need to know that patient's PHI. In addition, disclosures authorized by the patient are exempt from the minimum necessary requirements unless the authorization to disclose PHI is requested by the Department.
 - b. Authorizations received directly from third parties, ie, Medicare, or other insurance companies which direct the Department to release PHI to those entities are not subject to the minimum necessary standards. If there is a patient's authorization to disclose PHI to Medicare, Medicaid, or to another health insurance plan for claim determination purposes, the Department may disclose PHI requested without making a minimum necessary determination.
 - c. For all other uses and disclosures of PHI, the minimum necessary rule is likely to apply. As an example: when the Department conducts reviews of activities, it is generally not necessary to disclose certain patient information such as name, address, social security number, etc. Any such sensitive information should be blacked out or redacted from the patient care report used in the review.
8. Department Requests for PHI:
 - a. If the Department needs to request PHI from another health care provider on a routine or recurring basis, request must be limited to only the reasonably necessary information for the intended purpose.
 - b. If a request is non-recurring or non-routine, the Department must review the request to insure it covers only the minimum necessary PHI to accomplish the purpose of the request.
9. Incidental Disclosures:
 - a. The Department understands that there will be times when there are incidental disclosures about PHI in the context of caring for a patient. Privacy laws were not intended to impede common health care practices essential in providing health care. Incidental disclosures are inevitable, but 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 for others to access or see.

- b. The fundamental principle is that all personnel need to be sensitive about maintaining the confidence and security of all material created or used that contains patient care information (PHI). Other personnel should not have access to information not necessary to complete his or her job (eg, it is generally not appropriate for field personnel to have access to billing records of a patient).
- c. All personnel must be sensitive to avoid incidental disclosures to other health care providers or to others who do not have a need to know. Attention must be paid to who is within earshot when making verbal statements about PHI. Common sense procedures should be followed to avoid accidental or inadvertent disclosures.
 - i. Waiting or public areas – if patients are in a waiting or public area to discuss the service provided to them or have billing questions, make sure there are no other persons in the waiting area, or, if so, take them into a private area before engaging in discussion.
 - ii. Engine room or ready room areas – personnel should be sensitive to the fact the members of the public and other agencies may be present in the engine room or 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.
 - iii. Other areas – personnel should only discuss patient care information with those involved in the care of the patient, regardless of the physical location, being sensitive to voice level and the fact others may be in the area when speaking.
- d. Physical Security:
 - i. Patient care and other patient or billing records – patient care reports should be stored in safe and secure areas. Completed paper records concerning a patient 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.
 - ii. Billing records – eg, notes, remittance advice, charge slips, claim forms – should not be left in the open and should be stored in secure files or boxes that are in an area with limited access, available only to those who need access to the information for the completion of their job duties.
 - iii. Computers and entry devices – computer access terminals and other remote entry devices (PDA's, laptops) should be kept secure. Access to any computer device should be by **password** only. Personnel should be sensitive to who may be in viewing range of the screen and take simple steps to shield viewing by unauthorized persons. All remote

devices should remain in the physical possession of the individual to whom it is assigned at all times.

- e. Penalties for Violation:
 - i. The Department takes its responsibility to safeguard patient information seriously. There are significant legal penalties against organizations and individuals that do not adhere to the laws that protect patient privacy.
 - ii. Personnel who do not follow policies on patient privacy are subject to disciplinary action, up to and included termination from the Department.
- f. Questions About the Policy or any Privacy Issues:
 - i. The Department's privacy officer oversees policies and procedures on patient privacy, monitors compliance, and is available for consultation on any issues or concerns about how the Department deals with protected health information. Persons are free to contact the Department with questions or concerns.
 - ii. The Department will not retaliate against personnel who express a good concern or complaint about any policy or practice related to the safeguarding of patient information and the Department's legal obligations to protect patient privacy.

DATE: Approved November 3, 2008