PURPOSE:

To outline levels of access to Protected Health Information (PHI) of various staff members of the Candia Fire Department and to provide a policy and procedure on limiting access, disclosure, and use of PHI. Security of PHI is everyone's responsibility.

SCOPE:

Applies to all department members.

POLICY:

The Candia Fire Department retains strict requirements on the security, access, disclosure, anduse 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.

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.

RESPONSIBILITY:

It is the responsibility of all Department members to comply with this policy. It is the responsibility of the Privacy Officer to ensure that the Department is compliant with this policy.

PROCEDURES:

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

Job Title	Description of PHI to BeAccessed	Conditions of Access to PHI
Firefighter/EMTs	Intake forms from dispatch,patient care reports	May access only as part of completion of a patient event and post-event activities.
Chief, Deputy Chief, Captains	Intake forms from dispatch, patient care reports	May access to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel.
Administrative Support Staff, EMS QI/QA Staff	Intake forms from dispatch, patient care reports, billing claim forms, remittance advice statements, other patient records from facilities	May access to the extent to necessary to maintain the Department's EMS records, complete patient billing, follow up, and to provide approved, requested information to persons authorized to access specific PHI.
Medical Business Services, LLC.	Patient care reports, billing claim forms, remittance advice statements, other patient records fromfacilities	May access only as part of duties to complete patient billing and follow up and as per contract between MBS, LLC, and Candia Fire & Rescue
Officers	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
Dispatchers	Intake forms, preplanned CAD information on patient name, address, and other appropriate information	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.
Medical Resource Hospital (Medical Director & EMS Coordinator)	Intake forms from dispatch, patient care reports	May access 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.

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.

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

Disclosures to and Authorization from the Patient:

You are not required to limit to the minimum amount of information necessary required to perform your job function, or your disclosures of PHI to patients who are the subject of the 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 Company.

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

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 Department is permitted to disclose the PHI requested without making any minimum necessary determination.

Department Request for PHI:

If the Candia Fire Department 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 the Privacy Officer for guidance. For example, if the request in non-recurring or non-routine, like making a request for documents via a subpoena, we must review make sure our request covers only the minimum necessary PHI to accomplish the purpose of the request.

Holder of PHI	Purpose of Request	Information Reasonably Necessary to Accomplish Purpose
Skilled Nursing Facilities	To have adequate patient records to determine medical necessity for service and to properly billfor services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity,Mobility Assessments
Physician Offices	To have adequate patient records to determine medical necessity for service and to properly billfor services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Hospitals	To have adequate patient records to determine medical necessity for service and to properly bill for services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Mutual Aid Ambulance or Paramedic Services	To have adequate patient records to conduct joint billing operations for patients mutually treated/transported by the Company	Dispatch Intake forms, Patient care reports

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

Incidental Disclosures:

The Candia Fire 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 need 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.

But 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.

Station 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 careof the patient.

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 beleft 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 safeguard of authorized users.