

Prosper Fire Department Operations Manual	RT	Standard Operating Guideline	1316.0
Issued: 04/2004		Confidentiality and Release of Information	
Revised:			Page 1 of 1

**Purpose:** To maintain patient confidentiality as required by applicable state, federal, and local laws and to establish a consistent process when there is a request for patient information.

**Policy:** It is the policy of the Prosper Fire Department to assure compliance with the Healthcare Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, enacted by Congress on August 21, 1996, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 and the Texas Department of Health, Health and Safety Code 773.092 concerning patient confidentiality laws.

**Definitions:**

**HIPAA:** The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996. One of its five titles addressed administrative simplification, and within 'administrative simplification' are the electronic commerce and privacy requirements.

**Covered Entity:** Under HIPAA, a covered entity is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction. HIPAA compliance is required of covered entities.

**Individually identifiable health information:** Any health information about a patient that includes the name, phone number, address, social security number, or other such identifier is considered individually identifiable health information.

**Protected health information (PHI):** Individually identifiable health information transmitted or maintained in any form or medium, which is held by a covered entity or its business associate, that identifies the individual or offers a reasonable basis for identification, is created or received by a covered entity or an employer, or relates to a past, present, or future physical or mental condition, provision of health care or payment for health care. A specific individual can be identified by any of the following: Name, insurance number, photographs, address, Medicare or Medicaid number, vehicle license or I.D. numbers, telephone number, social security number, professional license or certification numbers, fax number, driver license number, Email address, account numbers, all ages above 89, device I.D. and serial numbers, internet protocol addresses, or biometrics identifiers.

**Privacy Officer:** Chief of the Department

I. Privacy Officer

The Chief of the Department will act as the Department's Privacy Officer. The responsibilities are to oversee all confidentiality issues and to serve as a contact point for patients and their representatives to voice concerns or complaints, to access records, or to request amendments be made to their patient records. This individual will have authority to gain ready access to all patient records. The Privacy Officer will be responsible for reviewing all requests for release of protected medical information except those allowed for by law for treatment, payment, and healthcare operations. All requests for patient information/records should be referred to the Privacy Officer or acting Privacy Officer.

Prosper Fire Department Operations Manual	<i>RT</i>	Standard Operating Guideline	1316.0
Issued: 04/2004		Confidentiality and Release of Information	
Revised:			Page 2 of 2

The Privacy Officer will be responsible for monitoring employee and Department compliance with all state and federal privacy standards, and respond to complaints and inquiries in regard to the Department's HIPAA compliance efforts. Should a complaint or accusation arise against an employee or the Department regarding privacy issues, the Privacy Officer will investigate the situation. If the investigation supports the complaint, the Privacy Officer shall follow Department procedures regarding appropriate disciplinary action.

The Privacy Officer will provide initial and ongoing training regarding privacy issues to all personnel who have direct or indirect access to PHI. The Privacy Officer will also be responsible for ensuring that all personnel have signed a Confidentiality Statement and have attended appropriate training sessions.

## II. Permitted Uses of Protected Health (Medical) Information

Members of the Department should only disclose Protected Health Information (PHI) for the treatment of the patient, to seek payment for the treatment of the patient and for other healthcare operations including, but not limited by, the following: quality assurance, employee review, training of EMS students, licensing, public health purposes, and medical control oversight.

Members can release PHI as required by law for reporting of abuse and neglect. PHI can also be released to members of the patient's family or friends that are directly involved in the patient's care. If the patient possesses the present mental capacity to make a healthcare decision, the patient should be asked and given the opportunity to object to such disclosures of PHI. Other non-routine disclosures of PHI are required by law but should be reviewed by the Department's Privacy Officer prior to the release of PHI.

## III. Security and Privacy of PHI

It is important that all PHI be kept confidential and secure. Information pertaining to EMS incidents should be kept confidential and not reported to anyone (verbally or written) except for patient treatment, billing, healthcare operations, and what is allowed by law and included in these policies and procedures. All PHI, either written or electronic, should be kept secured to ensure those who do not have a need to know cannot access it. The following procedures will be used to make sure all PHI, both written and electronic, remain private and secure:

- A. Keep all written PHI and patient reports stored in a manner so that those persons who do not have a need to know cannot read them. All written reports should be kept secure before and after completion. This will require that the written reports not be left unattended and/or left on fire station desks or outboxes. It will be necessary to deposit all EMS reports into the provided locked file cabinet once completed. The paramedics on duty will have keys to the file cabinet. All EMS reports will be stored under lock and key in the station or storage cabinet. All EMS key holders are on a need to know basis for either administration or billing purposes and will continue to ensure the security of these

Prosper Fire Department Operations Manual	RT	Standard Operating Guideline	1316.0
Issued: 04/2004		Confidentiality and Release of Information	
Revised:			Page 3 of 3

records by keeping them in locked rooms, locked cabinets or drawers when not physically in use.

- B. All written material containing PHI not included in the official patient report will be destroyed by shredding prior to disposal. The fire station office has a shredder assigned for this purpose. All copies of official patient reports used for administrative purposes or issued to individual Fire Department employees for court appearances will be destroyed by shredding before disposal. Once the required retention period has been reached, archived hardcopies of patient records will be shredded and destroyed.

All requests by citizens to post medical alerts or notices at the fire station must go through the Chief of the Department for approval. All such notices will only be posted if the patient, or guardian of the patient, signs an authorization for the Fire Department to display the medical information inside the fire stations in public view.

- C. All electronic patient reports will be kept in a manner that will insure privacy and security of PHI. All software that is used to access PHI will be password protected. All Fire Department personnel will have a unique password that will not be shared with others. Levels of security will be established and maintained for Fire Department employee access to PHI on a need to know basis. All fire station computers that have access to PHI will be configured to ensure that a time out or auto log off feature is enabled. These features are designed to keep those who do not have a need to know from accessing PHI in cases where the computer is left logged on due to emergency response. All administrative personnel will ensure that they are logged off of software that contains PHI before leaving their workstations. Future PHI software upgrades will only be considered if they contain privacy and security functions that are in compliance with federal and/or state law, whichever is greater at the time of the upgrade.

. All software that contains PHI will be backed up on a regularly scheduled basis that is approved by the Prosper Fire Department.

All inquires, requests, subpoenas, subpoenas duces tecum, and requests containing authorization (medical releases) about PHI that are received at the fire station level should be directed to the Chief of the Department.

#### IV. Coordination with Law Enforcement

PHI can be exchanged with the Police Department in certain situations, but it must be noted that the Police Department is not a covered entity under HIPAA; therefore, the Fire Department does face restrictions on when and how much PHI it can share with them. No one is allowed a copy of the patient report except for the receiving facility. A subpoena, subpoena duces tecum, or authorization (medical release) must accompany all Police requests for copies of patient reports. All subpoenas, subpoenas duces tecum, and medical releases (authorizations) will be sent to the Chief of the Department.

The following is a list of situations in which PHI can be shared verbally with the Police Department:

Prosper Fire Department Operations Manual	RT	Standard Operating Guideline	1316.0
Issued: 04/2004		Confidentiality and Release of Information	
Revised:			Page 4 of 4

- A. Patient is a victim of a crime.
- B. Patient is in custody of the Police.
- C. Reporting of legally specified wounds (ex. gunshot, stabbing).
- D. Fire Department personnel reasonably believe patient is a victim of abuse, neglect, or domestic violence. (Can also release PHI to a government authority, including a social service or protective service organization, authorized by law to receive reports of such abuse, neglect, or domestic violence.) The patient must be informed that the report was or will be made. Fire Department personnel will not disclose the reporting of abuse, neglect, or domestic violence if:
  - 1. The disclosure could put the patient or an individual in serious harm.
  - 2. The disclosure would be given to the suspected perpetrator.
- E. If in the course of providing emergency care disclosure of PHI is necessary to alert law enforcement officials to the commission and nature of a crime, location of crime, location of victims of a crime, and/or the identity, description, and location of the perpetrator of such crime.
- F. Patient is deceased and Police are handling notification of medical examiner, coroner, justice of the peace, or funeral director. Fire Department personnel can also give PHI directly to medical examiners, coroners, justice of the peace, funeral directors or their designees.
- G. In response to a law enforcement officer's request for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided the PHI is limited to driver's license information, Social Security number, place of birth, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics.
- H. Patient has made an admission of harming someone or himself/herself.
- I. Patient is suspected of being a danger to himself/herself.
- J. Patient is suspected of being a danger to Fire Department personnel. Refer to the Prosper Fire Department Standard Operating Procedure on Hostile Operations 1206.0.
- K. Patient has a communicable disease that law enforcement personnel have been exposed to. Refer to the Prosper Fire Department Standard Operating Procedure on Exposure Protocols 1301.0.

Information that is contained on a patient's driver's license and automotive insurance card is not PHI by itself and can be given to law enforcement for their reporting requirements. It is also permissible to give law enforcement information about a patient's location in or around automobiles at the scene of a motor vehicle collision as well as the MICU hospital destination. At no time should law enforcement be given identification information by their direct viewing of the patient report.

#### V. Telephone, Fax, and Email Policy

It is recognized that within the scope of business practices of the Prosper Fire Department it is routinely necessary to transmit PHI over the telephone, fax machine, and through email. Safeguards must be taken to protect PHI from those who do not have a need to know. Persons that have telephone contact with the Fire Department should be verified as someone with a need to know before the release of any PHI.

Prosper Fire Department Operations Manual	RT	Standard Operating Guideline	1316.0
Issued: 04/2004		Confidentiality and Release of Information	
Revised:			Page 5 of 5

All telephone inquiries received by fire stations regarding PHI should be forwarded to the Chief of the Department. Fire Department employees should verify the identity of recipients prior to exchanging PHI over the telephone.

All fax machines that could be used to send or receive PHI will be physically located in spaces that are not accessible to the public or by other employees of the city not covered by a confidentiality agreement. All faxes and emails that contain PHI should be verified twice as to the intended recipient. In the event that an email or fax is inadvertently received by an individual who does not have a need to know, both fax cover sheets and endings to emails that contain PHI should contain the following confidentiality statement:

CONFIDENTIALITY NOTICE: If the reader of this notice is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, disclosure, distribution, or copying of this communication is strictly prohibited. Please notify the sender by e-mail or facsimile that you have received this in error and delete it from your files.

#### VI. Notice of Privacy Practices

A HIPAA required Notice of Privacy Practices will be posted inside all MICU's.

The attending paramedics are also required by law to give the patient a copy of the HIPAA Notice of Privacy Practices and to receive a signature from the patient acknowledging receipt of the notice. It is understood that this is not practical on all patients. If the patient is unable to sign an acknowledgment of receipt, the attending paramedics will document the reason why in the space provided on the acknowledgement form.

The complete Notice of Privacy Practices will be made available to any patient who requests a copy either from paramedics or from the Prosper Fire Department office. The complete notice will also be posted on the City of Prosper's web site as required by law.

#### VII. Patient Rights

Patients should be given a Notice of Privacy Practices and should acknowledge its receipt. Authorization forms (medical releases) should be completed for non-routine use of PHI. Patients have the right to:

- L. Access their health record;
- M. Request an amendment of their record;
- N. Receive an accounting of certain disclosures made of their record;
- O. Request restriction on use and on method of communicating;

#### VIII. Access and Amendment of Patient Medical Record

Prosper Fire Department Operations Manual	RT	Standard Operating Guideline	1316.0
Issued: 04/2004		Confidentiality and Release of Information	
Revised:			Page 6 of 6

Adult patients, or the legal guardians of minor patients, will be given a copy of their medical records when proper identification is provided and the Request for Record Form is signed. This form may be obtained from the Fire Department Office.

The patient may request in writing that their medical records be amended. The Fire Department may deny the patient request if the Department was not the originator of the information, or the Department believes the information is/was accurate at the time the patient was treated and/or evaluated. Patients who knowingly give false identification to paramedics, and later request that information to be changed by Fire Department, will be referred to law enforcement for verification of correct identification.

When an amendment is made, a note will be added to the record to indicate the change. However, the original information will not be deleted. If the patient's request is denied, an explanation will be provided to the patient and noted in the record. The patient may contest the denial and request that a separate explanation be added to the medical record. This explanation will be allowed provided it is in writing, no longer than one 8½ X 11" page in length, single spaced, single sided, with no smaller than an 8 font type.

#### IX. Accounting of Disclosures

Patients have a right to receive an accounting of certain disclosures of the patient's protected health information in the six years prior to the date of the patient's request. The request must be in writing and must contain the signature of the patient. Each disclosure of protected health information other than for treatment, payment, and healthcare operations will be documented in a database for future accounting requests. Certain disclosures may be withheld from the accounting process as provided by law.

The accounting to the patient will:

- P. Be in writing;
- Q. Include the dates of disclosure and to whom the information was sent;
- R. Describe what information was sent;
- S. State the purpose of the disclosure.

#### X. Restrictions on Use and Disclosure

The patient may request restrictions regarding disclosure of the patient's protected health information beyond those restrictions already imposed by the government. The Fire Department may elect NOT to accept the restriction. Accepting restrictions on the use of PHI other than those imposed by law is not encouraged. However, if the request is accepted, the Fire Department must abide by the request and may only reverse the position after the patient has been appropriately notified.

#### XI. Restrictions on Communications Method with Patient

Prosper Fire Department Operations Manual	RT	Standard Operating Guideline	1316.0
Issued: 04/2004		Confidentiality and Release of Information	
Revised:			Page 7 of 7

The Fire Department will accommodate, if practical, a patient's request to communicate by alternative means. The patient is not required to explain why he/she wants such an alternative means of communication. An agreement to use an alternative communication channel will be documented and included in the patient's medical record.

## XII. De-identification of Information

The privacy rule applies to "individually identifiable health information" and not to de-identified information. The Rule states *that one can share a de-identified record with anyone, any time, and for any reason.* To comply with the Rule, all identifiers listed in the definition section of these policies and procedures will be deleted before the health information is shared with anyone other than those that are approved under the law.

## XIII. PHI Confidentiality Agreement

All employees of the City of Prosper who have access to protected health information will be required to complete a PHI Confidentiality Agreement. This agreement certifies that they have read, understand, and will comply with the policy and procedures contained in this document regarding PHI privacy and security.

## XIV. Business Associate Agreement

All vendors who do business with the City of Prosper and have access to PHI will be required to enter into a Business Associate Agreement. HIPAA requires this agreement before any PHI can be given to a vendor. A separate agreement can be utilized or an existing contract with the vendor can be modified to fulfill this requirement. A database will be compiled and maintained by the Chief of the Department of all vendors who have access to the Department's PHI.

## XV. Eternal Vigilance

It will be the responsibility of all Department personnel to make sure that the policies and procedures regarding privacy and security of PHI contained in this document are adhered to. It will be the responsibility of the Chief of the Department to monitor daily compliance with these policies and procedures.

## XVI. Complaints

All complaints or potential violations of these policies should be forwarded to the Privacy

---

Prosper Fire Department Operations Manual	RT	Standard Operating Guideline	1316.0
Issued: 04/2004		Confidentiality and Release of Information	
Revised:			Page 8 of 8

Officer. Following a thorough investigation by the Privacy Officer, if the complaint or suspected violation is found to be valid and justified, then the following actions will be taken:

- A. The Privacy Officer will follow the Department chain of command for notification of the violation, including the names of specific employees and circumstances surrounding the event;
- B. Company disciplinary policies and procedures will be followed with the nature and severity of the infraction considered to determine appropriate action;
- C. The Privacy Officer will review the event to determine the need for individual or company training or policy revisions as indicated.

If the incident involves a filed complaint with the Secretary of the Department of Health and Human Services, all requested documentation, policies, and information regarding the related incident or any other requested HIPAA related documentation or information will be provided by the Privacy Officer to the investigating agency. All employees will make every attempt to comply with the investigating agency's requests, and any questions or concerns should be directed to the Privacy Officer.

If a patient is concerned their privacy rights have been violated, or they disagree with a decision that has been made about access to their medical records, they may contact the Chief of the Department or mail the complaint to:

Prosper Fire Department  
Attn: Ronnie Tucker, Chief  
P. O. Box 307  
Prosper, TX 75078

0

The patient may also send a written complaint to the U.S. Department of Health and Human Services. All complaints to the Prosper Fire Department will be logged into a computer database for documenting and tracking compliance as specified by HIPAA.