City of Paris EMS HIPAA Policies

City of Paris EMS and all its employees must make every attempt to conform to all policies and regulations mandated by federal and state governments regarding patient confidentiality issues. The following policies must be adhered to:

Privacy Officer
City of Paris EMS will maintain a designated Privacy Officer to oversee all confidentiality issues and to serve as a contact point for patients and their families to voice concerns, 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. All requests for patient information/records should be referred to the Privacy Officer.

The Privacy Officer will be responsible for monitoring employee and company compliance with all state and federal privacy standards. Should a complaint or accusation arise against an employee or the company regarding privacy issues, the Privacy Officer will investigate the situation and follow company procedures regarding appropriate disciplinary action if the investigation supports the complaint.

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.

Confidentiality Statement
All personnel, riders, students, first responders, office managers, billing personnel or agency, administrators, board members, or any other individual who may have direct or inadvertent access to patient records will be required to sign a confidentiality statement that will remain in effect permanently. Should the person no longer be employed by City of Paris EMS or have no further access to patient records in the future, they must still maintain the necessary confidentiality of any PHI with which they may have had contact or knowledge during their employment, rotations, contact period, etc.

Patient Consent Form Signatures
All adult mentally competent patients must sign a consent form to use or disclose PHI on all patient contacts – transports and no transports. All transported patients must sign a billing authorization/financial responsibility form. The patient's legal guardian or adult parent (if a minor) should sign for the patient. Other next of kin may be able to sign if the patient can reasonably be expected not to be able to sign the form at a later date, if mailed to the patient.

If there is just cause why the patient or other authorized person cannot sign the form at the time of service, the reason must be documented on the consent form including a notation of when the follow up consent letter was mailed and the billing staff signature. The follow up letter should be mailed and the activity documented in the Follow up Consent Log. Reasonable efforts must be documented showing that attempts to gain the patient's signature were made. It is the crew's responsibility to ensure that proper consents are obtained from every patient at the time of service or appropriate follow up is completed.

Patient Care Record Security
All patient charts and associated paperwork are to be treated as highly confidential and security must be maintained at all times to ensure that PHI is not inadvertently shared with those who do NOT have the right to know. Verbal and written information being received from or given to other healthcare providers that is necessary to maintain the continuity of care is NOT to be withheld. While this information remains confidential, it must be shared under patient care circumstances to provide adequate assessment and treatment.

City of Paris EMS personnel should make every effort to minimize information that can be heard or read by those who do NOT have a "right to know." This includes bystanders, law enforcement officers, and even some family members. Because the decision on "who" has the right to know is so difficult to prove, City of Paris EMS personnel should not share information with anyone unless it is necessary to continue care for the patient. If in doubt, tactfully decline the information until proper lines of authority have been established.

Without exception, any information classified as PHI will not be shared in verbal, written, electronic or any other format unless it is required by the following criteria:

- As necessary for continuity of patient care, and treatment
- As necessary for payment or collection services
- Case reviews
- Education
- Obtaining legal and accounting services
- Business planning
- Resolving complaints
- Employee discipline
- Fundraising and marketing activities, including contacting the patients to tell them about services we can offer to them
- Medical research
- Databases that involve PHI but do not identify individual information
- Reminders of patient appointments for scheduled transports or care
- As indicated and mandated by state and federal requirements
- As legally required by law, either local, state, or federal such as:
- To law enforcement officials when necessary to identify someone who has committed a crime
- To law enforcement officials when there is an immediate need for the information to prevent or solve a crime
- To public health authorities to report births, deaths, or a disease that we are required to report
- To people who may have been exposed to a communicable disease by the patient
- To report child abuse, elder abuse, or domestic violence as required by law
- To the FDA and other agencies to report an adverse event from the use of a drug or medical device
- To government agencies who have a right to the information for conducting investigations, audits, inspections, disciplinary proceedings or other administrative or judicial actions in order to determine our compliance with the law
- In response to subpoenas, search warrants, and other legal requests or directives which require us to produce and disclose your PHI
- To government military, defense, investigative, security, and other agencies who have a right to your PHI in order to protect citizens, officials of the United States or a foreign country, and to investigate or prevent terrorist activities
- To public health officials of the US or foreign countries to avert a serious threat to the safety and health of the people
- As required by worker's compensation laws

When working on Patient Contact Reports (PCRs) prior to submitting them for Quality Improvement and billing, the employee must take extra care to ensure that no patient information or records are left out in the open where they can inadvertently be seen by those who have no "right to know ". All paperwork with patient information should be placed in the locked container provided. Appropriate personnel responsible for handling the

PCR for billing, Quality Improvement, or record keeping purposes will continue to ensure the security of these records by keeping them in locked rooms or locked cabinets or drawers when not physically in use.

Release of Records/Amendments/Restrictions
The patient or the patient's legal representative has the right to require us to restrict our use and disclosure of PHI with certain exceptions, but we don't have to agree if any of the following exceptions apply:

Exceptions:
We are not required to agree with the request for restriction if:

- The information requested might be used in a civil or criminal suit, proceeding, or other administrative action
- The information requested would reveal the source of confidential information provided by others
- The information requested could cause or produce a threat to any person's physical safety or life

Restrictions:
If we DO agree to the request for restrictions, we must honor them and must tell all others to whom we would normally disclose the patient's PHI about the restrictions and require them to honor them when we are required by law to disclose your information or when the PHI is needed for the patient's treatment in an emergency.

A patient or his/her legal guardian may also request a restriction for release of certain PHI by using the proper form supplied by the Privacy Officer. Such requests will also be evaluated and approval or denial will be postmarked within 60 days of the original request.

Amendment:
If a patient or patient's legal representative believes the PHI is not correct, he/she can ask us to amend it using the appropriate form. If we agree, we must do so within 60 days from the date of the original request. However, we can refuse the request if:

- We did not create the records
- We don't have access to the records or we can't get access to them
- We believe our records are correct
- Amendment would result in our being unable to obtain payment for services rendered to the patient

The patient or the patient's legal representative may request an accounting for our use and disclosures of the patient's PHI for a 6 year period prior to the request unless that time period involves records before April 14, 2003. We are not legally required to account for use and disclosures prior to April 14, 2003. We also do not have to account to the patient for disclosures made in connection with treatment, for payment, health care operations or disclosures that we were required by law to make. A patient has the right to one free accounting in any 12-month period; for additional accountings we may charge a reasonable fee.

Release:
All requests for PHI or any PCR information will be made through the Privacy Officer. All requests will be carefully reviewed prior to the approval or denial of such requests. Requests other than routine disclosures, state or federally mandated information releases, or other releases mandated by law will not require any other type of consent by the patient or the patient's legal guardian.

Any other record release or request for amendments to PHI shall be made utilizing the proper forms as provided by the Privacy Officer. Approvals or denials for release of records or amendments to records will be post-marked within 30 business days if held by us or 60 business days if held by another agency of the original written request.

Any approvals or denials for release of information, amendments to patient care records, or restrictions on PCR's will be based on accepted interpretation of the HIPAA rule.

Training
All City of Paris EMS personnel will be provided with initial training and updates on HIPAA rules and policies. Such training is considered to be mandatory. This training may be live or through other media presentations as indicated. Personnel must ensure that they have completed and signed the roster for each training session provided.

Complaint Procedure
All complaints or potential violations of these policies should be forwarded to the Privacy Officer. If the complaint or suspected violation is found to be valid and justified, following a thorough investigation by the Privacy Officer, then the following actions will be taken:

- The Privacy Officer will follow the company-designated chain of command for notification of the violation, including the names of specific employees and circumstances surrounding the event
- Company disciplinary policies and procedures will be followed with the nature and severity of the infraction considered to determine appropriate action
- The Privacy Officer will review the event to determine 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