**Protected Health Information Privacy Practices Policy**

**Policy:** Protected Health Information (PHI) is defined as individually identifiable health information from past, present, or future health care or payment that is created or received by a health care provider. All PHI in the form of oral, written, photographic, electronic, digital, etc. will be treated in accordance to this policy and may include but is not limited to incident reports with patient information, verbal communications between health care providers, and patient records from hospitals and billing information.

All personnel entrusted with or having access to PHI is responsible for maintaining its security. Unauthorized disclosure of PHI is prohibited and is contrary to the interest of the Independence Fire District, its patients, and its personnel.

**Procedure:** In order to assure the security of PHI, the following guidelines are to be observed by all personnel to the extent reasonable and possible. This list is not intended to be all-inclusive.

1. Treatment - PHI may be freely shared only with other health care providers who also treat the patient. The EMT handling patient care should use the most secure method possible for disclosing information to avoid incidental disclosures.
2. Payment - PHI may used to file claims with payers and send bills to patients without consent or authorization.
3. Health Care Operations - PHI may be used for Quality Assurance, Training and certain management functions. Only the minimum amount of information needed to perform the function should be used.
4. Place all completed EMS run reports and other confidential papers in the locked run report box as soon as possible. Do not leave exposed for observation by unauthorized persons.
5. Shred or destroy any waste material that includes PHI.
6. All Requests for copies of EMS run reports or any other documents containing PHI will be forwarded to the Privacy Officer as designated by the Chief. No PHI will be given out without the written permission of the patient or Power of Attorney except where required by law.
7. Password protection to computers or networks where PHI is maintained will be implemented.
8. Include confidentiality statements on e-mails and fax cover sheets that include PHI.
9. Requests for PHI by radio, newspaper, or television personnel must be denied.
10. Avoid offering advice, diagnosis, prognosis, financial, or other information that might be construed as medical opinion.
11. When routing documents containing PHI, seal the routing envelope and mark “Confidential”.
12. No run reports or other documents containing PHI will be shared with any police officer with the exception of officers who are medically trained first responders also treating the patient. Any other requests must be made to the Privacy Officer.
13. A Notice of Privacy Practices will be given to all patients at the time of service. A signed acknowledgement of receipt must be completed by the patient and attached to the completed run report. If the patient is unable to receive this notice, such as during an emergency, the notice shall be mailed to them at the earliest possible time.
14. Observed or known indiscretion and failure to follow confidentiality guidelines and procedures are to be reported to appropriate officers for investigation and discipline if appropriate.

**Privacy Officer:**

1. Serves as the contact person for the dissemination of PHI to other health care providers;
2. Serves as the contact person for patient complaints and requests;
3. Processes patient requests for access to and amendment of health information and consent forms;
4. Processes all patient accounting requests;
5. Ensures the capture and storage of patient PHI for the minimum period required by law;
6. Cooperates with the state and federal government agencies charged with compliance reviews, audits and investigations.