PHOENIX FIRE DEPARTMENT
Volume 1 – Management Procedures

HIPAA PRIVACY AND SECURITY POLICY

M.P. 102.15	**New:** 01/2026
This policy is for internal use only and does not expand an employee's legal duty or civil liability in any way. This policy should not be construed as creating a duty to act or a higher duty of care with respect to third-party civil claims against employees, the Phoenix Fire Department (PFD) or the City of Phoenix. A violation of this policy, if proven, can only form the basis for non-judicial administrative action by the employer in accordance with the laws and rules governing employee discipline.	
Related Policies: ETS HIPAA Privacy and Security Policy G001.026 Reference: 45 CFR Part 160 and 164, Subpart E	

PURPOSE

The purpose of this Policy is to ensure that the Phoenix Fire Department (PFD) is compliant with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the subsequent amendments, including the Health Information Technology for Economic and Clinical Health (HITECH) Act. PFD protects patients' Protected Health Information (PHI), and accordingly limits the access, disclosure, and use of PHI.

PFD expects each employee to protect the privacy and security of all protected health information (PHI) and electronic PHI (e-PHI) in accordance with PFD privacy and security policies, procedures and practices, as required by federal and state law, and in accordance with general principles of professionalism as a health care provider. Failure to comply with PFD's policies and procedures regarding the privacy and security of PHI and e-PHI may result in disciplinary action up to and including termination of employment.

DEFINITIONS

Authorized Representative - An individual who is permitted to sign in lieu of the patient for the purposes of HIPAA consent and billing authorization.

Breach - The acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of PHI

Business Associate - A person or organization that performs a service for PFD that uses or discloses individually identifiable health information. Business Associates may include but are not limited to entities that assist with billing, quality assurance, peer review, and claims processing. A written agreement is required for all Business Associates.

Covered Entity - A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction involving the transmission of information between two entities and bills for services. PFD is a covered entity.

Designated Record Set – A group of records that are created and/or maintained by the Department. The Designated Record Set for the Department is the Electronic Patient Care Report (ePCR), and the Billing Statement.

Electronic Protected Health Information (ePHI): PHI transmitted by electronic media or maintained in electronic media.

EMS Billing Specialist - An individual assigned by the Department to manage the EMS billing program.

Health Care - Care, services, or supplies related to the health of an individual.

Health Care Operation - Activities not directly related to treatment or payment such as quality assessment, protocol development, improvement activities, training programs, fraud and abuse detection, and compliance programs.

Health Care Provider – A provider of medical or health services and any other person who bills, furnishes, or is paid for health care in the normal course of business.

Health Information - Any information, oral or recorded in any form or medium, that is created or received by a Health Care Provider and relates to the past, present or future physical or mental health/condition of an individual, or the past, present or future payment for health care services provided to an individual.

HIPAA – A federal law that sets national standards to protect the privacy and security of patients' health information.

HIPAA Compliance Officer - Individual assigned by PFD to oversee PFD's compliance with federal, state, and local laws regarding PHI. The HIPAA Compliance Officer role may be divided into the roles of Privacy Officer and Security Officer.

Individually Identifiable Health Information - Information that is a subset of Health Information, to include demographic information, that is created or received by a Health Care Provider that identifies an individual or provides a reasonable basis to believe the information could identify an individual.

Minimum Necessary Standard: Access to and disclosure of PHI should adhere to the "minimum necessary" standard, which means limiting the use, disclosure, and requests for PHI to the least amount required to fulfill the intended purpose.

Privacy Officer – Individual assigned by PFD to oversee compliance with the HIPAA Privacy Rule and ensure the proper handling of protected health information (PHI). The Privacy Officer is responsible for developing, implementing, and maintaining privacy policies and procedures that govern how PHI is collected, used, disclosed, and safeguarded. They serve as the primary point of contact for privacy-related issues within the organization.

Privacy Rule – The HIPAA Privacy Rule sets national standards for protecting individuals' medical records and other PHI. It governs how EMS agencies, as covered entities, may use and disclose PHI, ensuring patient confidentiality while permitting necessary information sharing for treatment, payment, and operations. The rule also gives patients the right to access and amend their health information.

Protected Health Information (PHI) - PHI is health information created, received, stored, or transmitted by a covered entity or its business associate in any form -- electronic, paper, or oral, when that information can identify the individual through personal identifiers such as name, address, or medical record number. It includes data related to an individual's past, present, or future physical or mental health, healthcare services provided, or payment for care.

Security Officer – Individual assigned by PFD to develop, implement, and oversee policies and procedures to protect electronic Protected Health Information (ePHI) from unauthorized access, disclosure, or alteration. The Security Officer ensures compliance with the HIPAA Security Rule**.**

Security Rule – Establishes national standards to protect individuals' electronic personal health information that is created, received, used, and/or maintained by a Covered Entity. The Security Rule requires periodic risk assessments and encryption for all electronic Protected Health Information (ePHI) at rest and in transit, using industry-standard encryption methods.

PROCEDURE

As a provider of emergency medical services that bills for such services, PFD is a Covered Entity and is required to act in accordance with HIPAA.

PFD limits PHI access and disclosure to what is necessary for job duties, following HIPAA and state laws. All personnel must comply with security and privacy requirements.

PFD has strict requirements on the security, access, disclosure, and use of PHI. Personnel may do so only when necessary to complete job requirements.

PFD will ensure that access to, use of, and disclosure of Protected Health Information (PHI) is limited to the minimum necessary to accomplish the intended purpose, in compliance with the HIPAA Privacy Rule.

Patients may exercise their rights to access, amend, restrict, and request an accounting of billing, as well as lodge a complaint with either PFD or the Secretary of the Department of Health and Human Services.

PFD will designate either a Compliance Officer, or both a Privacy Officer and Security Officer, to manage and coordinate the Department's compliance with applicable sections of the HIPAA privacy and security rule. These Officers will assume the responsibilities listed in their appointments letters including:

- Developing, implementing, maintaining, and updating as needed, policies and procedures related to the HIPAA privacy and security rules, state health privacy laws, and other laws and regulations as required.
- Acting as a resource regarding HIPAA training.
- Receiving, documenting, investigating, and monitoring reported complaints, violations, and potential breaches.
- Maintaining all required HIPAA privacy rule documentation for a period of six years from the date created or the date last in effect, whichever is later.
- Developing and implementing privacy safeguard analyses and corrective action plans.

- Providing ongoing advice and periodic status reports on privacy and data security issues to the Fire Chief, ETS leadership and the EMS Assistant Chief.
- Serving as PFD's points of contact concerning HIPAA privacy and security policies and procedures.

CONFIDENTIALITY

All employees, volunteers, and interns/students who may have contact with PHI will have the responsibility of protecting patient privacy. Patient health information must remain confidential.

HIPAA AWARENESS TRAINING

PFD shall provide HIPAA training to all employees, volunteers, and interns/students who may have contact with PHI, within a reasonable period of time before or following their employment or service. PFD will also provide training to these same categories of individuals whenever there is a material change to the HIPAA regulations. Records of this training shall be maintained for a period of six years. A record of the individual's completion of the HIPAA awareness training will become part of their employee training file.

SAFEGUARD RULE

PFD must comply with all applicable administrative, physical, and technical standards and implementation specifications of the HIPAA Security Rule. PFD shall have appropriate administrative, physical, and technical safeguards and shall monitor compliance with these safeguards.

BREACH NOTIFICATION

Any suspected violations may be reported anonymously to the Privacy or Security Officer or the employee's supervisor. If a suspected breach occurs, EMS, ETS or the relevant division will notify the Assistant City Attorney assigned to PFD, the Privacy Officer and Security Officer. If a breach has occurred, PFD will, within sixty days, notify affected individuals, the Secretary of Health and Human Services, and if the breach involves more than 500 individuals, the media, following HIPAA regulations.

NOTICE OF PRIVACY PRACTICES

PFD is required to have a Notice of Privacy Practices. The distribution and posting of such notices shall be in accordance with applicable HIPAA regulations.

QUESTIONS ABOUT THE POLICY AND ANY PRIVACY ISSUES

The Privacy Officer oversees PFD policies and procedures on patient privacy, monitors compliance, and is available for consultation on any issues or concerns about how PFD deals with PHI.