



Carroll County Department of Fire and EMS

EMS Policies and Procedures

Standard Operating Procedure: 3.37	Effective Date: June 8, 2023
Subject: HIPAA Compliance	Section: Emergency Medical Services
Authorized: Michael Stoner, Assistant Chief	Revision Date: N/A

I. PURPOSE

The purpose of this Policy is to ensure that the Carroll County Department Fire and EMS (DFEMS) is compliant with the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, known as the Privacy Rule; Code of Federal Regulations, Title 45, Parts 160 and 164. DFEMS will remain in compliance with this law for the protection of patients' Protected Health Information (PHI), and will subsequently limit the access, disclosure, and use of PHI.

II. 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 a Covered Entity that uses or discloses individually identifiable health information. Business Associates include, but not limited to billing, quality assurance, peer review, and claims processing.

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.

Designated Record Set – Are a group of records that are created and/or maintained by the Department. The Designated Record Set for the Department are the Maryland

eMeds/Elite Electronic Patient Care Report (ePCR), Billing Statement, Refusal of Care Forms, and the State of Maryland Short Form.

Disclosure - The release, transfer, provision of access to, or divulging in any other manner information to another entity.

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 - 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 Compliance Officer - Individual assigned by the Department to oversee the Department's compliance with Federal, State, and Local laws regarding PHI.

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

Privacy Rule – The regulations entitled: The Standards of the Privacy of Individually Identifiable Health Information as promulgated by the United States Department of Health and Human Services.

Protected Health Information (PHI) - Individually Identifiable Health Information held or maintained by a Covered Entity or its Business Associates acting for the Covered Entity that is transmitted or maintained in any form or medium. This includes identifiable demographic or other information collected on an individual from a Health Care Provider relating to the past, present, or future physical or mental health or condition of the individual, or the provision or payment for Health Care to an individual that is created or received by a Health Care Provider.

Security Rule – Establishes national standards to protect individuals' electronic personal health information that is created, received, used, and/or maintained by a Covered Entity.

Transaction - The transmission of information between two parties to carry out financial or administrative activities related to Health Care.

Use - The sharing, employment, application, utilization, examination, or analysis of Individually Identifiable Health Information held within the entity that maintains the information.

III. PROCEDURES

- A. As a provider of emergency medical services that bills for such services, DFEMS is a Covered Entity and is required to act in accordance with the Administrative Simplification Provisions of HIPAA.
- B. This Policy will establish guidelines to ensure that DFEMS is compliant with these standards. The Privacy Rule portion of the Administrative Simplification Provisions establishes a foundation of Federal protections for the privacy of PHI.
1. DFEMS limits access to and disclosures of PHI in compliance with the laws, rules, and regulations set forth in HIPAA, the Code of Federal Regulations, and any applicable State laws and regulations. All will be strictly adhered to for the protection of a patient's PHI.
 2. DFEMS retains strict requirements on the security, access, disclosure, and use of PHI. Only certain personnel in the Department or Volunteer Corporations are permitted to access, use, and disclose PHI and may do so only when necessary to complete job requirements.
 3. Patients may exercise their rights to access, amend, restrict, and request an accounting of billing, as well as lodge a complaint with either the Department or the Secretary of the Department of Health and Human Services.
 4. DFEMS will implement a system-wide Compliance Program.
 5. DFEMS will designate a Compliance Officer to manage and coordinate the Department's compliance with applicable sections of the HIPAA privacy and security rule. The Compliance Officer will, in collaboration with the Department's compliance committee:
 - a. Develop, implement, maintain, and update as needed, policies and procedures related to the HIPAA privacy and security rules, state health privacy laws, and other laws and regulations as required.
 - b. Act as a resource for the Training, Safety and Health Officer regarding HIPAA training.
 - c. Receive, document, investigate, and monitor reported complaints, violations, and potential breaches.
 - d. Maintain 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.
 - e. Develop and implement privacy safeguards analyses and corrective action plans.

- f. Provide ongoing advice and periodic status reports on privacy issues to the Director/ Chief of Fire and EMS or designee.
- g. Serve as DFEMS point of contact concerning HIPAA privacy and security policies and procedures.

C. HIPAA AWARENESS TRAINING

1. DFEMS shall provide HIPAA awareness training to all employees, volunteers, and interns/students who may have contact with PHI, within a reasonable period of time following or before the commencement of their employment or service. DFEMS shall also provide training to these same categories of individuals whenever there is a material change to the HIPAA regulations.

D. CONFIDENTIALITY

1. All individuals identified above will have the responsibility of protecting patient privacy. Patient health information must remain confidential. All individuals identified above shall sign a Confidentiality form after completion of the HIPAA awareness training and confidentiality forms will become part of their respective training file.

E. NOTICE OF PRIVACY PRACTICES

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

F. SAFEGUARD

1. DFEMS shall have appropriate administrative, physical, and technical safeguards and shall monitor compliance with these safeguards.

G. SAFEGUARD RULE

1. DFEMS must comply with all applicable administrative, physical, and technical standards and implementation specifications of the HIPAA Security Rule. If an implementation specification is identified as being addressable, it must be implemented if reasonable and appropriate, or an equivalent alternative measure must be implemented.

H. QUESTIONS ABOUT THE POLICY AND ANY PRIVACY ISSUES

1. The HIPAA Compliance Officer oversees DFEMS policies and procedures on patient privacy, monitors compliance, and is available for consultation on any issues or concerns about how the DFEMS deals with PHI.
2. Any suspected violations may be reported anonymously through the Compliance hotline email, FEMScompliancehotline@carrollcountymd.gov or hotline telephone number, 410-386-6868.
3. DFEMS will not retaliate against any personnel who express a concern or complaint about any policy or practice related to the safeguarding of patient information and the Department's legal obligation to protect patient privacy.

IV. RECISION

This Standard Operating Procedure rescinds all directives regarding HIPAA Compliance or similar content previously issued for personnel of the Carroll County Department of Fire and EMS.