Carroll County Department of Fire & EMS

EMS Policy and Procedures

Standard Operating Procedure: 3.35	**Effective Date: June 1, 2023**
Subject: HIPAA Breach Notification & Inv.	**Section: Emergency Medical Services**
Authorized: Michael Stoner, Assistant Chief	**Revision Date:** N/A

I. PURPOSE

The purpose of this General Order is to ensure that Carroll County Department of Fire and EMS (DFEMS) complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the HIPAA Privacy Rule, 45 CFR Parts 160 and 164, and the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, as well as other applicable laws, governing unauthorized disclosures of Protected Health Information (PHI) and notice to affected persons in the event of a breach of patient privacy.

It is the policy of DFEMS to investigate all instances of written HIPAA complaints and suspected HIPAA violations to determine the cause, mitigate the effects, and minimize any recurrence. This policy delineates the formal process for investigating and documenting all written HIPAA complaints and suspected HIPAA violations, determining if a breach has occurred, and articulating the steps to be taken if a violation is deemed to be a HIPAA Breach. All personnel, operating volunteers, students/interns, and observers (guests of DFEMS given permission to ride with emergency services personnel) of DFEMS must comply with all HIPAA regulations as well as all County and Departmental HIPAA policies and procedures.

II. DEFINITIONS

Access – The act of acquiring, using, reading, writing, modifying, or communicating data/information or the ability to do so.

Breach – An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a

breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person who used the protected health information or to whom the disclosure was made.
3. Whether the protected health information was acquired or viewed; and,
4. The extent to which the risk to the protected health information has been mitigated.

Disclosure – The release, transferring, providing, sharing, or divulging in any other manner of information.

Protected Health Information (PHI) – Any information, whether oral or recorded in any medium, which related to:

1. The past, present or future physical or mental health or condition of an individual.
2. The provision of healthcare to an individual; or,
3. The past, present or future payment for the provision of healthcare to an individual; and,
4. There is a reasonable basis to believe the information can be used to identify the individual.
5. PHI includes demographics, insurance, billing, medical and other information DFEMS collects, creates, or receives in the course of providing healthcare to an individual. It includes oral information and information recorded in all media, for example: paper, electronic, film, etc.

III. PROCEDURES

A. DFEMS personnel shall maintain the privacy and security of patients' PHI consistent with HIPAA, the HIPAA Privacy Rule, other applicable laws, and Departmental policies. DFEMS shall notify the patient, the United States Department of Health and Human Services (HHS), and in some cases, local media if there is a Breach of unsecured PHI unless DFEMS can demonstrate a low probability that the information has been compromised.

B. DFEMS Billing Specialist is responsible for receiving, investigating, and documenting all reported written complaints and suspected HIPAA violations as well as making recommendations for resolution.

C. HIPAA COMPLAINTS

1. Individuals who have received services from DFEMS may file a written complaint with DFEMS Billing Specialist. All written

complaints shall be investigated in accordance with this policy. The final dispositions of the complaint shall be documented by the DFEMS Billing Specialist.

D. HIPPA VIOLATIONS

1. HIPAA violations may be reported by any individual. All personnel who know of an actual or suspected violation of any HIPAA regulation or DFEMS HIPAA policy or procedure shall immediately report this to his/her supervisor and the DFEMS Billing Specialist.

E. INVESTIGATION PROCEDURES

1. Upon receipt of a written complaint or report of a suspected or actual violation of any HIPAA regulations as well as all County and Departmental HIPAA policies and procedures, the DFEMS Billing Specialist working in collaboration with the Assistant Chief of EMS shall facilitate an investigation and conduct a risk assessment to determine whether a potential Breach has occurred and what actions, if any, are necessary.
2. Following the discovery of a potential Breach, the DFEMS Billing Specialist and/or Assistant Chief of EMS shall notify the Director/Chief of DFEMS, who must inform County Administration and Office of Law as soon as possible after learning of the potential breach.
3. All investigations shall be completed within 30 business days after the receipt of the complaint.

F. VIOLATION DETERMINATION

1. The Billing Specialist in consultation with the Director/Chief and Office of Law, shall decide whether the alleged action(s) constituted a violation of the HIPAA regulations and whether the violation resulted in a Breach.
2. Any question, access, use, or disclosure of PHI in a manner not permitted under the HIPAA regulations is presumed to be Breach unless DFEMS demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
    a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-dentification; and,
    b. The unauthorized person who used the PHI or to whom the disclosure was made; and,
    c. Whether the PHI was acquired or viewed; and,
    d. The extent to which the risk to the PHI has been mitigated.

G. BREACH NOTIFICATION

1. If a HIPAA violation resulted in a Breach, the Billing Specialist, in consultation with the Assistant Chief of EMS, shall oversee the Breach notification process as required by HIPAA regulations.

H. BREACH NOTIFICATION TO INDIVIDUALS

1. If a Breach is substantiated and notification is required, the Assistant Chief of EMS, in consultation with the Director/Chief, shall direct and oversee the process to notify each individual whose unsecured health information has been, or reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such Breach.
2. Notification shall occur without unreasonable delay and in no case later than 60 calendar days after the discovery of a Breach. If a Breach is deemed by the Billing Specialist to require immediate notice because of possible imminent misuse of unsecured PHI, notice may ben provided to individuals by telephone in addition to written notice.
3. Written notification must be made to individuals by first-class mail to their last known address.
4. If DFEMS knows that an individual is deceased and has the address of the next of kin or personal representative of the individual (parent, legal guardian, durable medical power of attorney, etc.) written notification must be provided by first-class mail to either the next of kin or personal representative.
5. The notification may be provided in one or more mailings as information becomes available.
6. Specifications of the notification to affected individuals must include:
    a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.
    b. A description of the type of unsecured PHI that was involved in the Breach (such as full name, date of birth, home address, account number, or diagnosis).
    c. Any steps individuals should take to protect themselves from potential harm resulting from the Breach. Depending on the nature of the Breach, the following steps may be suggested to individuals:
        - Alert financial institutions.
        - Place fraud alerts on credit files.
        - Monitor credit files and account statements closely.
        - Purchase identity theft protection.
    d. A brief description of what the County is doing to investigate the Breach, mitigate harm to affected individuals, and protect against further Breaches.

e. Contact information for individuals to ask questions or request additional information.

I. SUBSTITUTE NOTICE

1. The Billing Specialist shall use substitute forms of notice reasonably calculated to reach the individual when:
    a. There is insufficient or out-of-date contact information that precludes written notification to an individual.
    b. There is insufficient or out-of-date contact information for fewer than ten individuals.
    c. There is insufficient or out-of-date contact information for ten or more individuals, and the substitute notice must:
        i. Be in the form of either a conspicuous posting for a period of 90 days on the home page of the County's website, or conspicuous notice in a major print or broadcast media in geographic areas where individuals affected by the Breach reside. The County Administrator, or designee, shall make the final determination as to which of these methods is employed. The Billing Specialist shall work with DFEMS and County Public Information Officer to provide the required notification.
        ii. Include a toll-free phone number that remains active for at least 90 days where an individual may all for additional information and to determine if their unsecured PHI may be included in the Breach.
2. **Media notification for Breaches of 500 or more individuals**
    a. For a Breach of unsecured PHI involving more than 500 individuals, the following must occur
        i. DFEMS Billing Specialist, in conjunction with the County's Public Information Officer, must provide notification to prominent media outlets serving Carroll County without unreasonable delay and in no case later than 60 calendar days after the discovery of a Breach. The media notification must meet all the requirements set forth in the Breach Notification to Individuals section of this policy.
    b. Media notification is to supplement, not replace, written notice to affected individuals.
    c. Notification to the HHS by the Billing Specialist as stated below.
3. **Notification to HHS:** The Billing Specialist must notify HHS of a Breach in the following circumstances:
    a. For Breaches involving fewer than 500 individuals, the Billing Specialist must maintain a log or other documentation of such Breaches and, not later than 60 days

after the end of the calendar year, provide notification to HHS in the manner specified on the HHS website. The Billing Specialist shall consult with the Director/Chief, to determine when to report the Breach to HHS.

b. For Breaches involving 500 or more individuals, the Billing Specialist, under the direction of the Director/Chief, must provide notification to HHS in the manner specified on the HHS website. This notification must be made contemporaneously with the notice provided to individuals affected by the Breach.

J. BUSINESS ASSOCIATE RESPONSIBILITY TO NOTIFY

1. As set forth in Business Associate Agreements, a Business Associate must notify DFEMS without unreasonable delay after the disclosure of unsecured PHI resulting in a Breach.

K. DOCUMENTATION

1. The Billing Specialist and the Assistant Chief of EMS are responsible for completing a report of the investigation that provides a summary of the investigation and any recommended policy or procedural changes.
2. The Billing Specialist shall be responsible for maintaining all documentation related to the investigation consistent with DFEMS approved record retention schedule. Such information shall extend from either the date of the investigation's conclusion or the date of last activity regarding the investigation, whichever is later.

IV. **RECISION**

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