SUBJECT: EMS
TITLE: EMS Administrative Protocol updates
PURPOSE: Informational
ORIGINATING BUREAU: Training Bureau
EFFECTIVE DATE: September 26, 2016

The following policies have been added to the EMS Administrative Protocol. They will be published with the 2017 winter update. Please review.

1. EMS Compliance Policy
2. HIPAA General Policies and Procedures
3. HIPAA Privacy Rule Policy
4. HIPAA Security Rule Policy
5. Resource allocation for high use EMS patients

James E. Davis
Assistant Chief
Training Bureau

Kevin O’Connor
Fire Chief
EMS Compliance Policy

1. Section 1 Administration

PURPOSE:
The mission of the Columbus Division of Fire is to minimize injuries and death related to medical emergencies through the efficient delivery of effective prehospital treatment and patient transport. In order to execute this mission, the Division of Fire established an EMS reimbursement program to off-set the costs of providing EMS to assure that the organization is capable of maintaining current advancements in technology, education, and response. This program is set forth in Chapter 1934 of the Columbus City Code. The purpose of this policy is to create an administrative framework through which the Division of Fire will conduct an accountable, diligent, and effective compliance effort for EMS.

RESPONSIBILITY: It shall be the responsibility of each member to know, understand, and utilize these procedures as they apply to the situation at hand. It shall further be the responsibility of all Division Officers to train their subordinates in the proper application of these procedures and to implement and enforce the use of these procedures.

POLICY:
The Columbus Division of Fire shall implement and maintain an Emergency Medical Services Regulatory Compliance Program chaired by the Deputy Chief of Emergency Medical Services to provide centralized oversight and coordination in the Division of Fire’s compliance effort.

2. Section 2 – Deputy Chief of EMS

2.1.1. The Deputy Chief of Emergency Medical Services (EMS) will assure that:

1. The training bureau assigns on-line education to all members of the division a training module on:
   - Protected Health Information (HIPAA)
   - Blood Borne Pathogens
   - Patient Restraint
2. That the Ohio State Board of Pharmacy has received the fire division application for pharmacy license
3. That the Ohio State Board of Pharmacy has received an updated copy of the medical protocol when changes are made.
4. Obtain and maintain the Clinical Laboratory Improvement Amendments (CLIA) certificate of waiver.
5. That all division employees are evaluated to assure they are not on the excluded provider list for Medicare or Medicaid.
6. That those working in the EMS public records section have additional job specific training on handling and processing records requests that contain protected health information (PHI).

7. That the policies and directives for handling PHI are reviewed annually and in compliant with current federal and state health care program laws.
   - HIPAA General Policies and Procedures
   - HIPAA Privacy Rule Policies and Procedures
   - HIPAA Security Rule Policies and Procedures

8. That an annual audit is completed and documented to assure that the EMS section is maintaining PHI as required.

9. Work with other city agencies or outside vendors as directed to assist in assuring compliance with federal health care program requirements.

10. Develop and administer a Quality Improvement Program - Assure that a quality assurance program is maintained within the Division of Fire EMS offices and that the program adheres to acceptable guidelines and standards for assuring quality patient care.

11. That any information requests related to EMS delivery are processed in a timely and legal manner.

12. Create and chair an EMS regulatory compliance committee.

3. Section 3 – EMS Regulatory Compliance Committee

3.1.1. The Committee shall oversee and coordinate the Division’s compliance effort. The Committee should meet at a minimum twice per year. Because compliance is a daily effort, the Committee will help identify issues, create solutions, and recommend policy and procedure changes to ensure that compliance is achieved and/or maintained.

3.1.2. To be effective, the Committee should include a representative from each Bureau or Unit that has a stake in fulfilling the compliance objective. The following individuals or representatives should be included:

1. Deputy Chief of Emergency Medical Services
2. Medical Director or Assistant Medical Director
3. Fire Chief or their designee
4. Administration Bureau
5. Training Bureau
6. Support Services Bureau
7. Fire Alarm Office
8. Continuous Quality Improvement
9. Division Legal Advisor

4. Section 4 - Complaint Procedure

4.1. Any member of the organization or public that believes that any employee or contractor violates, either intentionally or negligently any internal compliance policies, applicable statues, regulations, or other federal
health care program requirements can make notification to the division of fire through the Professional Standard Unit at (614) 645-4046. Every attempt will be taken to protect the anonymity of the complainants where they so desire to remain anonymous.

5. Section 5 – Hospital Concerns

5.1. The CQI office will maintain a close working relationship with area hospitals. In the event a hospital staff member has a concern regarding CFD policy or procedures, the CQI captain will review the incident. The CQI captain, will gather all applicable data, request clarification from EMSO and/or crew. The CQI captain will review the concern with the Deputy Chief of EMS to determine if the concern is unfounded, can be addressed and resolved by CQI, develop a PIP for crew or needs to be forwarded to the Administrative Assistant Chief. If at any time it is discovered that an employee or contractor violated, either intentionally or negligently any internal compliance policies, applicable statues, regulations, or other federal health care program requirements, the case shall be sent to the Professional Standards Unit.

5.2. A hospital concern should be considered a part of the quality improvement process.
HIPAA General Policies and Procedures

Section 1. HIPAA Applicability and Purpose

1.1 The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, applies to the Division of Fire because the Division provides health care and submits claims for reimbursement electronically. These policies and procedures implement the standards as set forth by HIPAA for the security and privacy of protected health information.

1.2 The purpose of this policy and procedure is to implement the standards and specifications required by the rules set forth under HIPAA.

Section 2. Definitions

2.1 Division means the Columbus, Ohio Division of Fire and all of its employees, both uniformed and non-uniformed.

2.2 Designated Records Set means a record maintained by or for the Division that is a medical or billing record or is a record used, in whole or in part, by the Division to make decisions about individuals.

2.3 Protected Health Information (PHI) is information, transmitted or maintained in any form (paper or electronic); that is created, received, or maintained by the Division; that relates to the past, present, or future condition of an individual, provision of health care to an individual, or payment for the provision of health care to an individual in connection with a claim for reimbursement; and that identifies the individual or to which there is a reasonable basis to believe that the information can be used to identify the individual. PHI is not limited to patient care reports or billing information, but extends to any information that fits the definition of PHI regardless of the record within which the information is located.

2.4 Use or using means the sharing, employment, application, utilization, examination, or analysis of information within the Division.

2.5 Disclose or Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the Division.

2.6 Individual means the individual that the Division has a direct health care treatment relationship with and whom is the subject of the protected health information. In most cases, the term “individual” will refer to patient as defined under SOP 07-00-13(A). But, the Division may maintain PHI that does not refer to Division patients.

---

1 42 USC § 1320d-1(a)
2 45 C.F.R. 160.103. The definition of “protected health information” used in this policy incorporates the definition of “individually identifiable health information.” The purpose of the incorporation is to facilitate the understanding of what protected health information is for the purposes of the policy.
2.7 **Person** means a person, trust or estate, partnership, corporation, professional association or corporation, or other public or private entity to which a disclosure will be made; the person is not the subject of the PHI.

**Section 3. Security and Privacy Officer**

The Deputy Chief of Emergency Medical Services (EMS) will serve as the Division’s HIPAA Security and Privacy Officer. The specific duties of the Deputy Chief of EMS as the security and privacy officer will be stated under the respective security and privacy policies and procedures.

**Section 4. Training**

4.1 The Division will train all members, uniformed and non-uniformed, on these policies and procedures at least once during each three year recertification cycle. Training may be implemented on more frequently based upon changes in the laws and policies and procedures.

4.2 The method of training will be determined and implemented by the Training Bureau in conjunction with the Deputy Chief of EMS.

**Section 5. Records Retention**

The retention of all records required by or generated under this policy and procedure shall be accounted for on the Division of Fire’s Record Retention Schedule.
Section 1. Member Access to PHI

1.1 Member access to PHI and use of PHI will be the minimum necessary to carry out the member’s duties and must be consistent with this policy and procedure. Access will be monitored by the CQI Captain in accordance with the Security Rule to ensure compliance with this policy and procedure.

1.2 Members may create or access PHI when the member engages in treatment of individuals.

1.3 Members assigned to the Fire Chief’s Office, Training Bureau, Continuous Quality Improvement, EMS Officers and Supervisors, and the Administration Bureau may access PHI for payment or health care operations.

1.4 Members assigned to the EMS Records Office may access PHI to the extent permitted by this policy and procedure. The EMS Records Office is responsible for the management of PHI in both electronic and paper form.

Section 2. General Rules Regarding PHI

2.1 General Policy: All uses and disclosures of PHI by the Division will be consistent with this policy and procedure. A use or disclosure that is incidental to uses or disclosures in accordance with this policy and procedure are permitted so long as the initial uses or disclosures meet the requirements of Section 2.3 and are consistent with the Division’s Notice of Privacy Practices.

2.2 Minimum Necessary Requirement: When using or disclosing PHI, or when requesting PHI from another covered entity or business associate, the Division will make reasonable efforts to limit the use, disclosure, or request of PHI to the minimum necessary to accomplish the intended disclosure of the use, disclosure, or request. The minimum necessary requirement does not apply to the following circumstances:

2.2.1 Disclosures to or requests by a health care provider for treatment;

2.2.2 Uses or disclosures made to the individual;

2.2.3 Uses or disclosures made pursuant to an authorization by the individual;

2.2.4 Disclosures to the Secretary of Health and Human Services;

2.2.5 Uses or disclosures that are required by law; and

2.2.6 Uses or disclosures required for compliance with the HIPAA rules.
2.3 **Deceased Individual:** This policy and procedure will apply to the PHI of an individual who is deceased for a period of 50 years following death.

2.4 **Personal Representative:** The Division will treat a personal representative as the individual for the purposes of this policy and procedure. When the Division treats the personal representative as the individual, the personal representative has the same rights as the individual would have under this policy and procedure. Personal representatives include a parent, guardian, or other person acting in place of the parent or guardian of a minor, and an estate executor, estate administrator, or other person with the authority to act on behalf of a deceased individual. The Division may elect not to treat a personal representative as an individual in the following circumstances:

- **2.4.1** When a minor may legally consent to treatment as an adult, which occurs in the following circumstances: (1) diagnosis and treatment for venereal diseases; (2) alcohol and drug treatment; (3) HIV tests; (4) emergency medical services for sexual abuse victims; and (4) treatment when the minor is imprisoned and was prosecuted as an adult and was convicted or pled guilty; or

- **2.4.2** When the Division has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by the personal representative or when treating the person as a personal representative could endanger the individual; or

- **2.4.3** When the Division, in the exercise of professional judgment, decides it is not in the individual's best interest to treat the person as the individual's personal representative in situations that involve abuse, neglect, or endangerment.

2.5 **Notice of Privacy Practices:** This policy and procedure will be consistent with the uses and disclosures stated in the Division’s Notice of Privacy Practices. The Division will not use or disclose PHI in a manner that is inconsistent with the Notice of Privacy Practices or this policy, unless there is a valid authorization for such a use or disclosure.

2.6 **Required Uses and Disclosures:** The Division is required to disclose PHI to an individual when requested and required, and when required by the Secretary of the Department of Health and Human Services to investigate and determine the Division's compliance.

**Section 3. Individual Rights with Respect to PHI**

3.1 An individual has the right to request restrictions on certain uses and disclosures of PHI about the individual.

3.2 An individual has the right to receive confidential communications of PHI about the individual.
3.3 An individual has the right to inspect and copy PHI about the individual contained within the individuals designated records set.

3.4 An individual has the right to amend PHI about the individual.

3.5 An individual has the right to receive an accounting of disclosures of PHI about the individual.

3.6 An individual has the right to obtain a paper copy of the Division’s Notice of Privacy Practices.

Section 4. Authorizations and Restrictions to Use or Disclose PHI

4.1 Authorizations: If the Division obtains or receives a valid authorization, the Division will use or disclose PHI consistent with the authorization. An authorization is valid if the authorization contains the following:

4.1.1 Description of the information to be disclosed in a specific and meaningful fashion;

4.1.2 Name or other specific identification of the person authorized to make the requested use or disclosure;

4.1.3 Name or other specific identification of the person to whom the Division may make the requested use or disclosure;

4.1.4 Description of the purpose of the requested use or disclosure, which may be as general as “at the request of the individual” when the individual initiates the authorization; and

4.1.5 Expiration date or expiration of an event that relates to the individual or the purpose of the use or disclosure.

4.2 Restrictions: The Division will not use or disclose PHI if it has agreed to a restriction, unless an exception to the restriction applies as stated in the policy and procedure regarding individual rights.

4.3 The Division will maintain Authorizations and Restrictions for a period of 6 years after the authorization is no longer in effect.

Section 5. Uses and Disclosures for Treatment, Payment, or Health Care Operations

5.1 The Division may use and disclosure PHI for Treatment, Payment, or Health Care Operations.

5.2 Treatment: The Division may use PHI for its own treatment and may disclose PHI for treatment activities of another health care provider.
5.3 **Payment:** The Division may use PHI for its payment activities and may disclose PHI for the payment activities of a health care provider that receives the PHI.

5.4 **Health Care Operations—Use:** The Division may use PHI for health care operations. Health care operations include:

5.4.1 Conducting quality assessment and improvement activities;

5.4.2 Reviewing the competence or qualifications of health care professionals;

5.4.3 Evaluating provider performance;

5.4.4 Conducting training programs;

5.4.5 Credentialing or accreditation activities;

5.4.6 Conducting or arranging for medical review, legal services, and auditing functions; and

5.4.7 Business management and general administrative activities.

5.5 **Health Care Operations—Disclosure:** The Division may disclose PHI to another covered entity for health care operations of the entity that receives the information, if each entity has or had a relationship with the individual who is the subject of the PHI, the PHI pertains to that relationship, and the disclosure is for the purpose of:

5.5.1 Conducting quality assurance and improvement activities;

5.5.2 Reviewing the competence or qualifications of health care professionals;

5.5.3 Evaluating practitioner and provider performance or health plan performance;

5.5.4 Conducting training programs;

5.5.5 Credentialing or accreditation activities; and

5.5.6 Health care fraud and abuse detection or compliance.

**Section 6. Uses and Disclosures for Involvement in Care and Notification Purposes**

6.1 The Division may use or disclose PHI to a person involved in the individual’s care or for notification purposes when the individual has had an opportunity to agree or object to the use or disclosure.
6.2 **Involvement in the Individual’s Care:** The Division may disclose to an individual’s family member, other relative, close personal friend, or other person identified by the individual, PHI that is directly relevant to the person’s involvement with the individual’s health care or payment related to health care.

6.3 **Notification Purposes:** The Division may use or disclose PHI to notify, or assist in the notification of, a family member, personal representative, or another person responsible for the care of the individual of the individual’s location, general condition, or death.

6.4 **Disaster Relief Efforts:** The Division may use or disclose PHI to a public or private entity authorized to assist in disaster relief efforts for the notification purposes.

6.5 **Opportunity to Agree or Object:** If the individual is present and has the capacity to make health care decisions, the Division may use or disclose PHI only if the Division:

6.5.1 Obtains the individual’s agreement;

6.5.2 Provides the individual an opportunity to object and the individual does not express an objection; or

6.5.3 Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

6.6 If the individual is not present, or the opportunity to agree or object cannot be provided because of the individual’s incapacity or emergency circumstances, the Division may use or disclose PHI if it determines use or disclosure is in the patient’s best interests.

6.7 **Deceased Individual:** The Division may not notify a family member, personal representative, or another person responsible for the care of the individual of the individual’s death if doing so is inconsistent with any known prior expressed preference of the individual.

6.8 The Division may use or disclose PHI without the individual’s authorization or without giving the individual an opportunity to agree or object in the situations described in Section 7 through Section 14.

**Section 7. Uses and Disclosures Required by Law**

7.1 **Elder Abuse:** If the Division believes that an elderly adult is being abused, neglected, or exploited, or is in a condition which is the result of abuse, neglect, or exploitation, the Division will disclose PHI to report the belief to the county department of job and family services.

7.1.1 An elderly adult is any person sixty years of age or older within Ohio who is handicapped by the infirmities of aging or who has a
physical or mental impairment which prevents the person from providing for the person’s own care or protection, and who resides in an independent living arrangement.

7.1.2 The Division will inform the individual that such report will be or has been made, unless the Division believes that informing the individual or the individual’s personal representative will place the individual at risk of serious harm.

7.2 Violent Offense Causing Harm: If the Division knows or has reasonable cause to believe that any serious physical harm to an individual resulted from an offense of violence, the Division will disclose PHI to report that fact to law enforcement. In the case of Domestic Violence, the Division will inform the individual that such report will be or has been made. The Division is not required to notify the individual that such report will be or has been made if the Division believes that informing the individual or the individual’s personal representative will place the individual at risk of serious harm.

7.3 Judicial or Administrative Proceedings: The Division may disclose PHI in the course of any judicial or administrative proceeding.

7.3.1 If the Division receives an order from a court or administrative tribunal, the Division will disclose to the court or administrative tribunal only the PHI that is expressly authorized by such order.

7.3.2 If the Division receives a subpoena, discovery request, or other lawful process that is not accompanied by an order from a court or administrative tribunal, the Division must receive satisfactory assurances. The member responsible for complying with or facilitating the compliance with the subpoena, discovery request, or other lawful process will work with Division legal counsel to ensure the Division has received appropriate satisfactory assurances.

7.4 Law Enforcement Purposes: The Division may disclose PHI for certain law enforcement purposes.

7.4.1 GSW, Stabbing, Serious Harm—The Division will report to law enforcement any gunshot, stab wound, or other serious physical harm resulting from an offense of violence to an individual observed by the Division in the course of treating the individual.

7.4.2 Burns—The Division will report to the Division’s Fire and Explosion Investigation Unit, State Fire Marshal, or other fire and explosion investigation entity, a burn injury inflicted by an explosion, or other incendiary device.

7.4.3 Court Order, Warrant, Subpoena, or Summons—The Division will disclose PHI in compliance with a court order, warrant, subpoena or summons issued by a judicial officer, grand jury subpoena, or an
administrative request. The responsible Division member will contact legal counsel to assist with the disclosure of PHI.

7.4.4 Identification or Location—The Division may disclose limited PHI in response to a law enforcement officer’s official request for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person.

7.4.5 Victims—The Division may disclose PHI in response to a law enforcement officer’s official request for information about an individual who is or is suspected to be a victim of a crime so long as: the individual agrees to the disclosure; or if the Division is unable to obtain the individual’s agreement because of incapacity or emergency circumstance, the law enforcement official represents that the information is needed to determine whether there has been a violation of law and will not be used against the victim, law enforcement activity would be materially and adversely affected by waiting until the individual agrees, and the Division determines it would be in the individual’s best interests.

7.4.6 Suspicious Death—The Division may disclose PHI to alert law enforcement of an individual’s death, if the Division has a suspicion that the death may have resulted from criminal conduct.

7.4.7 Criminal Conduct on Premises—The Division may disclose PHI to a law enforcement official that the Division believes in good faith constitutes evidence of criminal conduct that occurred on Division premises.

7.4.8 Naloxone Administration—The Division will disclose the name and address of patients who received naloxone due to an actual or suspected drug overdose to the law enforcement agency with jurisdiction in the area where naloxone administration occurred.

Section 8. Uses and Disclosures for Public Health Activities

8.1 The Division may disclose PHI to a public health entity that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including the reporting of disease, injury, vital statistics, and the conduct of public health surveillance, public health investigations, and public health interventions.

8.2 Communicable Diseases: The Division will disclose PHI to report of a case or suspected case of a disease which is required to be reported under the Ohio Administrative Code, Chapter 3701-3-02.

8.3 Child Abuse: The Division will disclose PHI to report knowledge or reasonable cause to suspect that a child under the age of eighteen or a mentally retarded, developmentally disabled, or physically impaired child under twenty-one has suffered or faces a threat of suffering abuse or neglect. The Division will disclose PHI to the public children services
agency, municipal police department, or county sheriff in which the child resides or in which the abuse or neglect is occurring.

8.4 **Disease Transmission to EMS:** The Division will use, disclose, or request PHI if the EMS provider believes he or she had significant exposure to a contagious or infectious disease listed in Ohio Administrative Code, Chapter 3701-3-02.2.

8.5 **Mammal Bite:** The Division will disclose PHI to report knowledge of a dog or other mammal bite to the local department of public health.

**Section 9. Uses and Disclosures for Health Oversight Activities**

The Division may disclose PHI to a health oversight agency for oversight activities authorized by law. The responsible Division member will work with Division counsel to assist with the disclosure of PHI.

**Section 10. Uses and Disclosures about a Decedent**

10.1 The Division may disclose a deceased individual’s PHI to a coroner, medical examiner, or funeral director.

10.2 **Coroner or Medical Examiner:** The disclosure may be made to a coroner or medical examiner for the purposes of identifying a deceased person, determining a cause of death, or other duties authorized by law.

10.3 **Funeral Director:** The disclosure may be made to a funeral director as necessary for funeral directors to carry out their duties.

**Section 11. Uses and Disclosures for Organ, Eye, or Tissue Donation**

The Division may disclose PHI to organ procurement organizations for the purpose of facilitating organ, eye, or tissue donation and transplantation.

**Section 12. Uses and Disclosures for Specialized Government Functions**

12.1 The Division may use or disclose PHI for specialized government functions.

12.2 **National Security:** The disclosure may be made to federal officials authorized to receive PHI for the conduct of lawful intelligence, counter-intelligence, and other national security activities.

12.3 **Protective Services:** The disclosure may be made to authorized federal officials for the provision of protective services to the President or other persons or to foreign heads of state.

12.4 **Law Enforcement Custody:** The disclosure may be made to a correctional institution or a law enforcement official having lawful custody...
of an inmate or other individual if the disclosure of PHI is necessary for the:

12.4.1 Provision of health care to the individual;

12.4.2 Health and safety of the individual or other inmates;

12.4.3 Health and safety of the officers or employees at the correctional institution;

12.4.4 Health and safety of individuals or officers for the transporting of inmates;

12.4.5 Law enforcement on the premises of the correctional institution; or

12.4.6 Administration and maintenance of safety, security, and good order of the correctional institution.

Section 13. Uses and Disclosures for Workers’ Compensation

The Division may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers’ compensation.

Section 14. Uses and Disclosures for Research

The Division may use or disclose PHI for research purposes provided the Division has obtained authorization, the Division Privacy Board has authorized a waiver of the individual authorization to use or disclose PHI, or the PHI used for the research is used or disclosed pursuant to a limited data set agreement.

Section 15. Breach Notification and Investigation

15.1 The Division will promptly investigate any suspected breach of unsecured PHI and provide notifications to individuals when appropriate as required by 45 C.F.R. 164.404.

15.2 Breach Notification: Any member who has a reasonable belief that unsecured PHI has been acquired, accessed, used, or disclosed in a manner inconsistent with this policy and procedure which compromises the security and privacy of the PHI shall immediately notify the Privacy Officer in writing of the member’s belief. In addition to those uses or disclosures which are inconsistent with this policy and procedure, a breach may also include lost, stolen, or unaccounted for media or documents which contain PHI.

15.3 Written Investigation: Upon receipt of the notification, the Privacy Officer shall promptly investigate the suspected breach and create a report within 14 days containing the following elements:

15.3.1 Description of what occurred, including the date of the breach and the date of the discovery, if known;
15.3.2 The nature and extent of the PHI involved in the breach and whether or not the PHI was unsecured;

15.3.3 The identity of the person or entity, if known, who used the PHI or to whom the PHI was disclosed;

15.3.4 Whether or not the PHI was actually acquired or viewed, if known;

15.3.5 The extent to which the risk to the PHI has been mitigated; and

15.3.6 Description of what the Division is doing to investigate the breach, to mitigate harm to individuals whose PHI was included in the breach, and actions taken to protect against further breaches.

Section 16. Accounting of Uses and Disclosures

16.1 The Division will maintain an accounting of uses and disclosures of PHI relating to an individual for 6 years from the date of the use or disclosure.

16.2 The following uses or disclosures will be accounted for:

16.2.1 To a business associate—unless the disclosure is made for the purposes of the business associate providing treatment, payment, or health care operations activities on behalf to the Division;

16.2.2 Required by law, including mandatory reporting to local, state, and federal agencies and authorities;

16.2.3 For purposes of public health activities;

16.2.4 About victims of abuse, neglect, or domestic violence;

16.2.5 For health oversight activities;

16.2.6 For judicial and administrative proceedings;

16.2.7 For law enforcement purposes pursuant to process and for identification and location purposes;

16.2.8 To coroners, medical examiners, and funeral directors;

16.2.9 For organ procurement purposes;

16.2.10 For research purposes;

16.2.11 For specialized government functions, except for national security or intelligence purposes;

16.2.12 For workers’ compensation.
Section 17. De-Identified Health Information

17.1 If health information does not identify an individual or there is no reasonable basis to believe the information may be used to identify an individual, the health information is not individually identifiable health information and is not PHI. The Division may use or disclose such information without reference to this policy and procedure.

17.2 The Division may determine that health information is not individually identifiable health information.

17.3 The Division will only determine that health information is not individually identifiable health information if the following identifiers are removed:

- 17.3.1 Names;
- 17.3.2 All geographic subdivisions smaller than a state;
- 17.3.3 All elements of date;
- 17.3.4 Telephone numbers;
- 17.3.5 Fax numbers;
- 17.3.6 E-mail addresses;
- 17.3.7 Social security numbers;
- 17.3.8 Medical record numbers;
- 17.3.9 Health plan beneficiary numbers;
- 17.3.10 Account numbers;
- 17.3.11 Certificate/license numbers;
- 17.3.12 Vehicle identifiers and serial numbers, including license plate numbers;
- 17.3.13 Device identifiers and serial numbers;
- 17.3.14 Web universal resource locators;
- 17.3.15 Internet protocol address numbers;
- 17.3.16 Biometric identifiers, including voice and fingerprints;
- 17.3.17 Full face photographic images and any comparable images; and
- 17.3.18 Any other unique identifying number, characteristic, or code.
Section 1. Security Management Responsibility

1.1 Security Responsibility

The Deputy Chief of Emergency Medical Services shall be the assigned security official. His or her responsibilities include:

1.1.1 Establish and maintain all policies and procedures that implement the HIPAA Security Rule (45 CFR § 164.302 - § 164.318);

1.1.2 Investigate all information security incidents and breaches of PHI;

1.1.3 Implement workforce security training and awareness;

1.1.4 Conduct a periodic security risk analysis; and

1.1.5 Ensure that all documentation required by the HIPAA Security Rule is created and maintained in accordance with these policies and procedures and the CFD’s Record Retention Schedule.

1.2 Risk Assessment and Management

CFD shall conduct a risk assessment at minimum once every three years. A risk assessment may be more frequent if necessary based upon the change in technological infrastructure, legal requirements, or known or suspected breaches. This shall include an accurate and thorough assessment of the potential risks and vulnerabilities to PHI created or maintained by CFD. CFD shall conduct the risk assessment using a process guided by National Institute of Standards and Technology (NIST) Special Publication 800-30, Revision 1, Risk Management Guide for Information Technology Systems, (September 2012).

CFD will take all reasonable and practical steps to manage and mitigate all risks identified by the assessment shall be managed and mitigated by. CFD shall consider the capabilities and constraints of costs, staff ability, and hardware and software when determining the reasonableness and practicality of risk management and mitigation.

The risk assessment and all actions taken to manage and mitigate risks shall be appropriately documented and retained in accordance with Section 1.7 of this policy and CFD’s Record Retention Schedule.

1.3 Security Incidents

A “security incident” means a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach modification, or destruction of PHI maintained by CFD; interference with CFD’s information technology operations; or significant violation of this policy. Examples include: Computer system intrusion; Unauthorized or inappropriate use or disclosure of PHI; Suspected or actual breaches,
compromises, or other unauthorized access to CFD information systems, data, applications, or accounts; Unauthorized changes to computers or software; Loss or theft of computer equipment or other data storage devices and media (cardiac monitors, laptop, USB drives, or personally owned devices used for CFD work) used to store PHI; and Interference with the intended use or inappropriate or improper usage of information technology resources.

All security incidents shall be reported to the Deputy Chief of EMS. The Deputy Chief of EMS shall, in conjunction with the Department of Technology and any applicable business associate, investigate, take steps to mitigate, and document all reported security incidents. The Deputy Chief of EMS shall follow, to the extent practicable, the recommendations described in NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide, (August 2012).

1.4 System Usage Audits and Activity Reviews

The Continuous Quality Improvement (CQI) Captain, under the direction of the Deputy Chief of EMS, shall perform monthly audits of individuals who have authorization to create, view, amend, or delete PHI. The CQI Captain shall also review activity logs on a monthly basis to ensure that access to and use or disclosure of PHI is within the parameters set forth by CFD’s policies and procedures.

If the audits or reviews reveal a security vulnerability or inappropriate access to PHI, the Deputy Chief of EMS and the CQI Captain shall take immediate reasonable and appropriate steps to mitigate the vulnerability or inappropriate access.

1.5 Security and Compliance Evaluation

Annual evaluations shall be performed by the Deputy Chief of EMS or his or her designee to ensure CFD has implemented the appropriate Security Rule measures and continues to operate in compliance with these policies and procedures.

Section 2. General

2.1 Security Awareness and Training

All members of the Division of Fire, uniformed and non-uniformed, shall receive periodic security awareness and training at least once during a three-year recertification cycle to ensure awareness of these policies and procedures. All awareness and training shall be documented.

When a member’s access to PHI changes due to a change in position, for example when a member moves into a permanent or temporary role within the EMS Records Section, that member shall receive appropriate awareness and training to enable compliance with these policies and procedures and to maintain the security and integrity of electronic PHI.
2.2 **Workforce Access**

Authorization and clearance for access to PHI shall be determined by the chain of command based upon a member’s temporary or permanent assignment.

A member shall only have access to PHI to the minimum extent necessary to carry out the member’s duties.

2.3 **Workstation Use and Portable Media**

All workstations, including but not limited CFD assigned computers, tablets, and phones, are for business use and shall not be used in a manner that compromises the security or integrity of the workstation or its contents.

Members shall not share individual and unique log-in passwords, access codes, or other information necessary to access either a workstation or database.

PHI shall not be sent, copied, or removed from any workstation or database by any method except as part of an approved operation of CFD in conjunction with a member’s official duties.

All portable media, including but not limited to compact discs, USB storage drives, disks, or portable hard drives that contain PHI shall be reasonably tracked and monitored.

---

**Section 3. Information Access Management and Control**

3.1 **Access Management**

All access to PHI will be managed by the CQI Captain. The CQI Captain or his or her designee will grant access based upon the members’ temporary or permanent duties and to the minimum extent necessary to carry out those duties. The CQI Captain shall regularly review access lists and shall modify a member’s right to access, create, review, amend, or delete PHI accordingly.

If a member requires access to a greater extent than has been provided to carry out his or her duties, the member’s supervisor shall request access through the CQI Captain. The CQI Captain will then independently determine whether or not to grant the requested access.

When a member’s duties no longer require access to the extent which was granted, the CQI Captain or his or her designee shall promptly modify the member’s access to the minimum extent necessary to carry out the member’s duties. This includes, but is not limited to, when an employee separates from employment with CFD, changes positions, or is on extended leave regardless of the circumstances of the leave.

3.2 **PHI Electronic Storage**
PHI shall be appropriately secured when stored electronically. Access to files stored on CFD’s server shall be restricted to only those members who have duties that require access. Security of CFD’s server shall be governed by the policies and procedures set forth by the City of Columbus Department of Technology.

PHI shall not be routinely stored on a portable storage device or laptop or desktop hard drive. If PHI is stored on a portable storage device or laptop or desktop hard drive, access to files containing PHI shall be protected by a password.

3.3 **Physical Access Control and Workstation Security**

All physical locations where PHI is stored in any form shall be appropriately secured to prevent unauthorized access. Access will be granted to such locations in accordance with the member’s duties.

Workstations shall be secured by either electronic or physical measures when not attended to by a member when the workstation has the ability to access PHI or when PHI is stored on the workstation.

All visitors to CFD shall be escorted whenever in an area where PHI may be located. Access to these areas should only be permitted in limited and necessary situations.

3.4 **Technical Access Control and Authentication**

Technical access control and authentication of individual users shall be governed in accordance with the policies and procedures of City of Columbus Department of Technology and any business associate who maintains PHI on behalf of CFD. Technical access controls and authentication may include unique individual user identifications, passwords, and automatic log-off functions.

3.5 **Electronic Devices and Media Controls**

All devices and portable media that contain electronic PHI shall be tracked and monitored in a manner that permits CFD to appropriately respond to any breach, including the loss, theft, or destruction.

PHI shall be destroyed or removed from any electronic device or portable media that was used to store PHI prior to its reuse in another setting. Destruction or removal of the PHI will be done in accordance with a method approved by the City of Columbus Department of Technology or any business associate who maintains PHI on behalf of CFD when the business associate provides the electronic devices or portable media.

3.6 **Data Encryption and Integrity**

The encryption and integrity of data shall be maintained in accordance with methods approved by the City of Columbus Department of Technology.
3.7 Contracts and Memoranda of Understanding

CFD shall enter into written agreements with any entity that uses, discloses, or maintains PHI on behalf of CFD. Such agreements shall meet the requirements of 45 CFR § 164.308(b) and § 164.314(a).

Section 4. Data Backup and Contingency Plan

4.1 Data Backup

All data containing PHI shall be regularly and periodically backed up in accordance with procedures set forth by the City of Columbus Department of Technology or any business associate who maintains PHI on behalf of CFD. Data backups shall be sufficient to restore damaged data with a useful duplicate.

4.2 Contingency Plan

The Deputy Chief of EMS or his or her designee shall establish and annually review, test, and revise a contingency plan. The contingency plan shall provide for the continuation of essential and strategic operations that involve the creation, storage, transmission, or use of PHI.

The contingency plan shall include the following elements:

4.2.1 Applications and Data Criticality Analysis, to assess the relative criticality of specific applications;

4.2.2 Emergency Mode Operation plans and procedures, to ensure the continuation of essential and strategic operations in the event of the loss of CFD’s technological infrastructure; and

4.2.3 Disaster Recovery plans and procedures, to ensure the restoration of lost data and system access.
Appropriate Resource Allocation: Individuals with Frequent Access to the EMS System

Introduction

The Columbus Division of Fire must provide emergency medical services in an expedient, efficient, and safe manner to individuals in need of emergency medical response, care, and transport. The Division is also required by the Ohio Revised Code to implement quality assurance programs designed to improve the availability and quality of the emergency medical services its provides. This policy and procedure is an effort to accomplish these two responsibilities. This policy is designed to supplement existing EMS policies and procedures.

Purpose

The purpose of this policy and procedure is to link individuals with appropriate resources when EMS is not the most appropriate resource for the individual’s health or safety. It is not the purpose of this policy and procedure to exclude individuals from appropriate access to EMS.

Objectives

The objectives of this policy are to:

1. Provide care for the individual’s needs by linking the individual with the most appropriate resource and in the most appropriate setting;

2. Reduce the amount of time between identification of the need and connection to the appropriate resource;

3. Increase overall efficiency of emergency medical services;

4. Reduce costs associated with the delivery of unnecessary emergency medical services; and

5. Allocate emergency medical services resources in the most beneficial manner.

Appropriate Use

Prehospital emergency medical services are appropriate, effective, and efficient when EMS provides emergency care and allocates emergency resources to stabilize, assess, and provide appropriate treatment and transport for individuals who experience an acute illness or injury that requires immediate medical attention and transport by medic in order to reduce the potential for death and disability.
Non-Discrimination Statement

The Columbus Division of Fire will not refuse to respond to, assess, treat, or transport any individual based upon inability to pay, gender, ethnic background, religion, employment status, or financial status. All assessment, treatment, and transport will be based upon the appropriate medical standards for the condition from which the individual suffers.

Policy

The Columbus Division of Fire will identify individuals for whom EMS resources may not be appropriate in order to link those individuals with the most appropriate resources.

Procedure

I. Identify Inappropriate Utilization of EMS

A. The Continuous Quality Improvement (CQI) staff will identify individuals who inappropriately utilize EMS.

B. Identification will be based upon the following factors:

   1. Frequency of EMS response (12 or more times within 90-days); or

   2. Issues or conditions for which the EMS response is sought when EMS is not the appropriate resource to assist with the management of the issue or condition.

C. EMS personnel, hospitals, or law enforcement may also identify individuals who inappropriately utilize EMS by notifying the CQI staff. If notification comes through this route, CQI will conduct an independent review of the case.

II. Analysis and Internal Action Plan

A. After an individual has been identified as inappropriately utilizing EMS resources, the CQI Captain and EMS Medical Director will review the case to determine if further action under this policy is appropriate.

B. Further action will be based upon the underlying cause for the utilization. Situations in which EMS is not the most appropriate agency to manage the individual’s condition will be suitable for further action. These situations include, but are not limited to, the following:

   1. Substance abuse;
2. Mental health conditions;
3. Exacerbation of chronic medical conditions; or
4. Societal or environmental conditions.

C. If the CQI Captain and the EMS Medical Director determine further action is necessary, the following steps will be taken:

1. The EMS Medical Director, Deputy Chief of EMS, CQI Captain, and one regular EMS Supervisor for the battalion where most of the EMS responses occurred (the Internal Action Plan Committee) will create an internal action plan. The internal action plan will outline CFD’s response to the inappropriate utilization.

2. When creating the internal action plan, the following factors will be considered:
   a) Root cause of EMS utilization;
   b) Proper resource or resources to address the root cause of utilization; and
   c) Mechanism to link the individual with the appropriate resource.

3. CFD will attempt to link the individual with the resources that most appropriately address the individual’s needs.

4. Once the Internal Action Plan Committee has created CFD’s internal action plan, the Committee will submit the plan to the Columbus City Attorney’s Office for an independent review.

5. The internal action plan is protected health information as defined by HIPAA. This document is not a public record. This document is not included within the individual’s designated record set.

III. Individual User Notification

A. CFD will notify the individual that the individual’s utilization of EMS is not appropriate based upon the services EMS provides.

   1. Reasonable effort will be made to notify the individual in person.

   2. Notification may occur the next time the individual accesses the EMS system.

B. Notification will:

   1. Counsel the individual on the appropriate use of EMS;
2. Identify resources more appropriate for the individual’s needs; and

3. Be written and contain the following elements:

   a) Number of EMS responses over a defined period of time;
   b) Reason for the response and documented complaint upon arrival;
   c) Appropriate uses of EMS resources;
   d) Resources or organizations that can address the individual’s needs;
   e) CFD will monitor utilization of EMS over the next 90 days; and
   f) After the 90-day monitoring period, CFD will not transport the individual to an emergency department unless the individual seeks EMS for an appropriate use.

C. CFD may ask the individual to authorize CFD to disclose the individual’s protected health information to other health care providers or organizations that may most appropriately care for the individual’s needs.

D. If CFD determines the individual lacks the capacity to understand the notification due to medical, developmental, or degenerative issues, CFD may need to contact family members, guardians, or responsible caregivers to assist with allocating resources appropriately.

IV. Appropriate Resource Guidelines

A. Substance Abuse
   1. NetCare
   2. Columbus Public Health’s Alcohol and Drug Abuse Program (http://columbus.gov/publichealth/programs/alcohol-and-drug-abuse/)
   3. Other Services (https://prod.ada.ohio.gov/directory/)
   4. Hope thru Housing

B. Mental Health Conditions
   1. NetCare
   2. Other Services (http://mha.ohio.gov/Default.aspx?tabid=790)

C. Exacerbation of Chronic Medical Condition
   1. Columbus Neighborhood Health Centers
   2. Local Urgent Cares

D. Societal or Environmental Conditions
   1. Franklin County Social Services
   2. Columbus Public Health
   3. Alternative Transportation to seek health care
   4. Veteran’s Administration
E. This is a non-exhaustive list of additional resources which may be used. The use of specific resources will be dependent upon the individual's needs.

V. Monitoring EMS Utilization and Alternative Resource Allocation

A. After notifying the individual of the appropriate use of EMS and appropriate resources, CQI will initiate a 90-day monitoring period.

B. During the 90-day monitoring period the following steps will be taken:

1. At 30-day intervals CQI will create a report on the individual's utilization of EMS. The report will include the frequency of use and the individual's issues or conditions associated with each use.

2. After 90-days, CQI will create a report that compares the individual's utilization for the 90-day period prior to identification with the 90-day period following identification.

C. If there has been no meaningful reduction in the utilization of EMS resources upon comparing the two time periods and the utilization remains inappropriate, the Internal Action Plan Committee will review the individual's case to determine if further allocation of resources, including non-transport, is appropriate under the circumstances. The Committee will do the following:

1. Review the individual's case.

2. Determine if additional time is required to allow the individual to seek the appropriate resources to address the individual's need.

3. If additional time is not required, a report will be created with the following elements:

   a) Data on EMS responses and transports over a 180-day time period;
   b) Condition or issue for which EMS response and transport was sought;
   c) Statement as to why these responses and transports were not an appropriate utilization of EMS;
   d) Actions taken by the Division of Fire to reduce the inappropriate utilization of EMS; and
   e) Statement as to why additional time will not be beneficial to permit the individual to cease inappropriate utilization of EMS and seek appropriate resources for the individual's condition.

D. The report will be sent to the Fire Chief, the Department of Public Safety, and the City Attorney’s Office for independent review.
E. After the review, the Committee will notify the EMS Supervisors of the report. The EMS Supervisors will notify the appropriate medic crews.

F. CFD will notify the individual that it may not transport the individual to an emergency department for conditions or situations that involve the inappropriate utilization of EMS. Reasonable efforts will be made to notify the individual in person.

VI. EMS Response after Non-Transport Notice

A. CFD will always transport an individual by medic to the closest most appropriate emergency department if transport by medic is indicated based upon the individual’s condition, regardless of the individual’s status under this policy and procedure.

1. Generally, CFD’s medical protocols, assessment of the individual, and the diagnostic impression of the individual will be used to determine whether or not transport by medic is indicated.

2. If the individual does not have the mental capacity to refuse transport or treatment as stated in Refusal of Treatment/Transport, the EMS crew will transport the patient to the closest most appropriate facility.

3. If the individual is a psychiatric patient as stated in Psychiatric Patients, the EMS crew will transport the patient to the closest most appropriate facility.

B. After the responding EMS crews identify the individual as an individual who inappropriately utilizes EMS, an EMS Supervisor will be dispatched to the location.

1. EMS personnel will assess the individual based upon the individual’s current complaint and current medical condition.

2. EMS personnel will advise the patient of the assessment.

3. If the individual’s complaint and condition are inappropriate for the utilization of EMS, the EMS personnel will advise the individual he or she will not be transported to an emergency department by medic.

4. EMS will again advise the patient of additional resources more appropriate for the individual’s needs and alternative transportation to those resources.
C. CFD may use the EMS response as the first opportunity to notify the individual of the conclusion that the individual will not be transported due to his or her inappropriate utilization of EMS.

VII. Documentation

A. All interactions with an individual which occur pursuant to this policy will be appropriately documented.

B. Each request for and response by EMS, including responses that occur after the notice of non-transport, require a complete ePCR.

VIII. Additional Action

A. Additional action by CFD may be necessary under certain circumstances. This action may include, but is not limited to the following:

1. Criminal investigation for 911 abuse or disruption of public services; or

2. Seeking appointment of a guardian by a court.

B. If additional action is required, CFD will contact the agencies authorized to carry out that action.