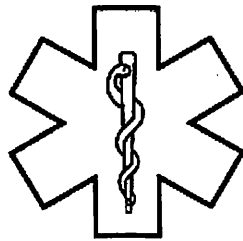
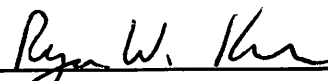


# CITY OF WASHINGTON EMS



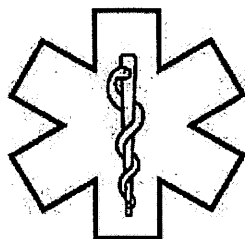
## HIPAA COMPLIANCE PLAN

Adopted: December 2, 2013

  
\_\_\_\_\_  
Ryan W. Kern, Mayor

Denise M. Powell  
City Clerk

# CITY OF WASHINGTON EMS



## HIPAA COMPLIANCE PLAN

DRAFT COPY

---

Adopted: December 2, 2013

**Table of Contents**

Health Insurance Portability and Accountability Act Compliance Plan..... 5

HIPAA Risk Analysis ..... 6

Assignment of Responsibilities: The HIPAA Compliance Officer..... 8

Job Description for HIPAA Compliance Officer..... 10

Job Title    HIPAA Compliance Officer ..... 10

HIPAA Compliance Officer Designation ..... 12

Position Description Language for HIPAA Compliance - All Positions..... 13

Updating HIPAA Policies, Procedures and Training Policy ..... 14

HIPAA Training Policy ..... 16

HIPAA Training Log..... 17

Workforce Sanctions for Violations of HIPAA Policies and Procedures Policy ..... 18

Minimum Necessary Requirement and Role-Based Access to PHI Policy ..... 20

Staff Use and Distribution of Notice of Privacy Practices Policy and Procedure..... 23

Notice of Privacy Practices..... 24

Consent to Treatment and Transport, Assignment of Benefits Authorization, Responsibility for Payment, and Acknowledgement of Receipt of Notice of Privacy Practices..... 29

Patient Requests for Access to Protected Health Information Policy..... 31

Patient Request for Access to Protected Health Information ..... 34

Denial of Patient Request for Access ..... 36

Patient Requests for Amendment of Protected Health Information Policy..... 38

Patient Request for Amendment of Protected Health Information ..... 41

Acceptance of Patient Request for Amendment..... 42

Parties That Need My Amended PHI..... 43

Denial of Patient Request for Amendment ..... 44

Patient Requests for Restriction of Protected Health Information Policy ..... 45

Patient Request for Restriction of Protected Health Information..... 48

Review of Patient Request for Restriction of Protected Health Information..... 49

Acceptance of Patient Request for Restriction ..... 50

Denial of Patient Request for Restriction..... 51

Requests for Accounting of Disclosures of Protected Health Information Policy ..... 52

Patient Request for Accounting of Disclosures of Protected Health Information ..... 55

Accounting Log for Disclosures of PHI ..... 56

Patient Requests for Confidential Communications of Protected Health Information Policy..... 57

Patient Request for Confidential Communications of Protected Health Information FORM..... 59

Review of Patient Request for Confidential Communications of Protected Health Information ..... 60

Acceptance of Patient Request for Confidential Communications.....	61
Denial of Patient Request for Confidential Communications .....	62
ACTION PLAN: Patient Requests Relating to PHI FOR HIPAA COMPLIANCE OFFICER.....	63
Designated Record Sets Policy .....	64
Patient Authorization to Use and Disclose Protected Health Information .....	66
Procedure for Filing Complaints About Privacy Practices.....	68
Log for Processing Complaints About Privacy Practices .....	69
Use of Computer and Information Systems and Equipment POLICY.....	70
Releasing PHI to Family Members and Others Policy .....	74
Release of Protected Health Information Pursuant to Legal Process Policy.....	76
Release of Protected Health Information to Law Enforcement Without Legal Process Policy .....	80
Action Plan: Release of PHI to Law Enforcement Without Legal Process.....	86
Action Plan: Court-Ordered Requests for PHI .....	89
Action Plan: Administrative Requests for PHI from Government Agencies .....	90
Action Plan: Attorney-Issued Subpoenas and Discovery Requests.....	91
News Media Interaction POLICY .....	93
Action Plan: News Media Interaction .....	95
Staff Member Medical Records Policy.....	96
Physical Security of PHI and e-PHI Policy.....	98
General Security of Electronic and Other Patient and Business Information.....	102
Facility and Computer Access Point Controls.....	105
Third Party Access to e-PHI Policy.....	109
Persons Who May Access Computer Systems and Secured Areas in the Event of an Emergency .....	112
Persons With Keys to City Of Washington EMS Business Office .....	113
Inventory of Hardware & Mobile Electronic Devices .....	114
Computer Hardware/Peripherals/Software Inventory .....	116
Password Authorization Form.....	118
Staff Member Access to e-PHI POLICY .....	119
Staff Member Electronic Communications.....	122
Use of Electronic Mail and Facsimile Transmissions.....	126
Creating Backups of e-PHI Policy.....	128
EMERGENCY CONTACT LIST.....	130
Electronic Information System Activity Review and Auditing POLICY .....	131
Encryption of e-PHI policy .....	132
Access to Server/Tape Backup Information & Emergency Contact Information .....	134
Electronic Information System Activity Review and Auditing policy .....	135



Contingency Planning Policy .....	136
Disaster Management and Recovery of e-PHI Policy .....	138
Access Log to Secure Areas .....	139
Security Incident Management Policy.....	140
Breaches of Unsecured Protected Health Information Policy .....	142
Internal Breach/Security Incident Reporting Form .....	147
Log for Tracking Breach Incidents .....	148
Individual Notice of Breach of Unsecured PHI.....	149
Action Plan: Breach Analysis Steps.....	151
Contracting With Business Associates Policy.....	154
City of Washington EMS Business Associate List .....	156
Guest/Trainee Confidentiality and Non-Disclosure Agreement.....	157
STUDENT/GUEST/TRAINEE ACKNOWLEDGEMENT AND RELEASE FORM .....	158
Staff Member HIPAA Assurances.....	159
Staff Member Termination Checklist.....	161
Identity Theft Policy .....	162

# **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT COMPLIANCE PLAN**

## **PURPOSE**

The City of Washington EMS is committed to protecting our staff members, the patients we serve and the company from illegal or damaging actions by individuals and the improper release of protected health information and other confidential or proprietary information.

The purpose of this information is to outline the acceptable use of Protected Health Information (PHI) at the City of Washington EMS, as well as to determine how our company handles and safeguards the PHI of our patients. These rules are in place to protect the employees and patients of the City of Washington EMS. Inappropriate use exposes the City of Washington EMS to risks including breach of patient confidentiality and other legal claims.

The information collected herein is the Health Insurance Portability and Accountability Act (HIPAA) compliance plan for the City of Washington EMS.

The information gathered in the development and implementation of the following policies, procedures, and forms was obtained through the law firm of Page, Wolfberg & Wirth, LLC.

# **HIPAA RISK ANALYSIS**

## **PURPOSE**

City of Washington EMS is responsible, under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), to ensure the privacy and security of all protected health information ("PHI") that we use or disclose. The foundation of compliance with HIPAA is the completion of a "Risk Analysis" to identify existing risks and vulnerabilities in the way we create, receive, maintain or transmit our PHI. This policy describes our general approach to our HIPAA Risk Analysis.

## **SCOPE**

City of Washington EMS's HIPAA Risk Analysis includes an assessment of potential risks and vulnerabilities to the confidentiality, availability and integrity of all PHI that City of Washington EMS creates, receives, maintains or transmits. This includes assessing any risks and vulnerabilities to the confidentiality, integrity and availability of non-electronic PHI (such as papers and documents) and electronic protected health information (e-PHI). At a minimum, the risk analysis will include a review of City of Washington EMS's:

- General security hardware and procedures to protect our facility, vehicles, and electronic assets;
- Computer servers (on or off-site) that store PHI;
- Computer network (including any local and wide area networks, communications servers and bandwidth connections, and storage devices and hardware);
- Databases where patient information is created, stored, and accessed by City of Washington EMS, whether on or off-site;
- Electronic media that store e-PHI such as hard drives, disks, CDs, DVDs, USB drives or other storage devices, transmission media, or portable electronic media;
- Electronic devices used for processing patient information (such as laptops and field data collection devices);
- Workstations and access points where PHI is created, accessed and used;
- Policies and procedures (written and unwritten) that involve the creation, use, or access to e-PHI; and
- Vendors, billing companies, clearinghouses and others who create, receive, maintain or transmit PHI for City of Washington EMS.

## **PROCEDURE**

The HIPAA Compliance Officer will utilize City of Washington EMS's HIPAA Risk Analysis Tool to identify all current and potential risks and vulnerabilities to PHI at City of Washington EMS and to develop a plan to manage those risks.

## **ANNUAL RISK ANALYSIS**

City of Washington EMS will, on an annual basis, undertake a risk analysis that includes the following:

1. Identifying and documenting all places where the physical (paper) PHI and e-PHI is stored, received, maintained or transmitted at City of Washington EMS (*i.e.*, all sources of PHI at City of Washington EMS whether on or off-site).
2. Identifying and documenting all current and potential risks to the confidentiality, security, integrity and availability of all PHI sources identified at City of Washington EMS.
3. Assessing the likelihood of each identified risk and assigning the risk to a "risk level" and "potential impact" category.
4. Identifying and documenting any measures that City of Washington EMS currently has in place to address each identified risk, including any policies, procedures, hardware/software, security devices, etc. Then, identifying any methods that are not currently in place that may eliminate or mitigate the risk.
5. Providing recommendations to City of Washington EMS that might remedy identified risks and vulnerabilities and improve the security, integrity and availability of all PHI sources identified at City of Washington EMS.
6. Implementing methods that might remedy identified risks and vulnerabilities and improve the security, integrity and availability of all PHI sources identified at City of Washington EMS.

## **IMPLEMENTATION SPECIFICATIONS**

Implementation specifications under HIPAA that are "required" must be implemented and documented that they were in fact implemented, including how the specification was implemented. Implementation specifications under HIPAA that are "addressable" will be implemented as follows:

1. If the implementation specification is reasonable and appropriate, City of Washington EMS will implement it.
2. If the implementation specification is determined to be inappropriate and/or unreasonable, but the security standard cannot be met without implementation of an additional security safeguard, City of Washington EMS may implement an alternative measure that achieves the addressable specification.
3. If City of Washington EMS meets the standard through alternative measures, the decision not to implement the specification will be documented, including the reason for the decision, the rationale, and a description of the alternative safeguard that was implemented.

## **ASSIGNMENT OF RESPONSIBILITIES: THE HIPAA COMPLIANCE OFFICER**

### **PURPOSE**

City of Washington EMS is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

### **SCOPE**

This policy applies to all City of Washington EMS staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It outlines the role of the HIPAA Compliance Officer and how those responsibilities relate to all City of Washington EMS staff members.

### **PROCEDURE**

Both privacy and security compliance under HIPAA are very important responsibilities. City of Washington EMS will assign the responsibility of HIPAA Compliance Officer to a staff member knowledgeable about the Privacy and Security Rules, and who will be able to devote the time and energy to the important responsibilities that come with this assignment.

The HIPAA Compliance Officer is a high level position in the organization and as such, the person assigned to these responsibilities will have access to the highest levels of management to review and discuss policies and procedures, as well as compliance issues and concerns related to the HIPAA Privacy and Security Regulations.

Since the privacy-related responsibilities between the Privacy Rule and the Security Rule are similar in many respects, the HIPAA Compliance responsibilities may be assigned to just one person. City of Washington EMS may also break out the privacy and security compliance responsibilities into two separate positions, depending on workload and organizational need. The HIPAA Compliance Officer may delegate appropriate duties to other responsible staff members.

The following is an overview of the compliance responsibilities of both functions:

### **HIPAA COMPLIANCE OFFICER RESPONSIBILITIES**

The HIPAA Compliance Officer oversees all activities related to the development, implementation, and maintenance of City of Washington EMS's policies and procedures covering the privacy and security of all patient health information, electronic or otherwise. This person serves as the key compliance officer for all federal and state laws that apply to the privacy of patient information, including the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Privacy Regulations and Security Regulations under that law.

This individual is tasked with the responsibility of ensuring that all of the organization's patient information privacy policies and procedures related to the privacy of, and access to, patient health information are followed.

- Develops policies and procedures on staff training related to the privacy of patient health information and protected health information.
- Defines levels of staff access to PHI and minimum necessary requirement for staff based on the required job responsibilities.
- Oversees, directs, delivers, and ensures the delivery of initial and ongoing privacy training and orientation to all staff members, employees, volunteers, students and trainees.
- Serves as the contact person for the dissemination of PHI to other health care providers.
- Serves as the contact person for patient complaints and requests.
- Processes patient requests for access to and amendment of health information and consent forms.
- Processes all patient accounting requests.
- Ensures the capture and storage of patient PHI for the minimum period required by law.
- Ensures ambulance service compliance with all applicable Privacy Rule requirements and works with legal counsel and other managers to ensure the company maintains appropriate privacy and confidentiality notices and forms and materials.
- Cooperates with the state and federal government agencies charged with compliance reviews, audits and investigations related to the privacy of patient information.
- Ensures that the necessary and appropriate HIPAA related policies are developed and implemented to ensure the security and integrity of all e-PHI within our Company and as provided to our business associates.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to develop and implement the necessary HIPAA- related policies with respect to the security of e-PHI.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to assess, analyze, monitor, and review City of Washington EMS's compliance with all HIPAA-related security policies.
- Develops policies on the security of health care information, including computer and password security and patient data integrity.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to provide a mechanism for reporting security incidents and HIPAA security violations.
- Acts as a spokesperson and single point of contact for City of Washington EMS in all issues related to HIPAA security.
- Periodically reviews all security policies to ensure that they maintain their viability and effectiveness.
- Develops and conducts educational programs for City of Washington EMS staff to help ensure their compliance with all e-PHI policies and procedures.
- Cooperates with the state and federal government agencies charged with compliance reviews, audits and investigations related to the security of patient information.

## **JOB DESCRIPTION FOR HIPAA COMPLIANCE OFFICER**

Job Title                      HIPAA Compliance Officer

### **JOB IDENTIFICATION**

Department: Ambulance

Reports to: Ambulance Service Director and City Administrator

### **SUMMARY OF HIPAA COMPLIANCE OFFICER'S ROLE**

City of Washington EMS's HIPAA Compliance Officer oversees all activities related to the development, implementation, and maintenance of City of Washington EMS's policies and procedures related to the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This includes policies and procedures related to all protected health information ("PHI"), including electronic protected health information ("e-PHI").

This person serves as the key compliance official for all federal and state laws that relate to protecting the privacy and security of patient information created, maintained, used or disclosed by City of Washington EMS, its staff members, and our business associates who perform work on our behalf involving PHI. This individual is tasked with the responsibility of ensuring that all of the organization's HIPAA policies and procedures are in place, updated, followed and enforced and that all workforce members are properly trained regarding those policies and procedures.

### **DUTIES AND RESPONSIBILITIES**

#### *Principle Responsibilities – HIPAA Compliance*

- Develops and updates all required HIPAA policies and procedures.
- Ensures the delivery of initial and ongoing HIPAA training and orientation to all staff members, employees, volunteers, students and trainees.
- Determines appropriate levels of staff access to PHI and oversees compliance with the minimum necessary requirement for different job responsibilities.
- Serves as the contact person for issues regarding the dissemination of PHI to outside parties.
- Serves as the contact person for, and processes, patient complaints and requests under HIPAA, or directs such requests to the appropriate party.
- Ensures the retention of PHI for the minimum period required by law.
- Ensures City of Washington EMS's compliance with all applicable HIPAA requirements and works with legal counsel and other managers to ensure the company maintains appropriate notices, forms and materials.
- Cooperates with the state and federal government agencies charged with HIPAA compliance reviews, audits and investigations.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to secure PHI at City of Washington EMS.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to assess, analyze, monitor, and review City of Washington EMS's compliance with all HIPAA related security policies.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to provide a mechanism for detecting and reporting security incidents, breaches of unsecured PHI and other HIPAA violations.

- Acts as a spokesperson and single point of contact for City of Washington EMS in all issues related to HIPAA.
- Periodically reviews all electronic systems related to the security of e-PHI to ensure that they maintain their viability and effectiveness.
- Annually reviews "Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals" and implements necessary changes pursuant to the Guidance. Available at: <http://www.hhs.gov/ocr/privacy>.
- Ensures that business associate agreements are in place with appropriate parties and updates business associate agreements when necessary.

## **QUALIFICATIONS**

### *Educational Requirements*

- High school Diploma or GED Equivalent. Working knowledge of the HIPAA Privacy, Security and Breach Notification Rules required.
- Maintains current knowledge of applicable federal and state privacy laws and monitors changes in privacy and security practices including ambulance industry "best practices," to ensure current organizational compliance.

### *Physical and Mental Requirements of the Position*

- Must be able to sit for extended periods of time at a desk or similar workstation.
- Must be able to visually inspect workstations and other computer communications equipment.
- Must be able to occasionally lift computer equipment weighing up to 20 pounds from the floor to a desk level height.
- Must have vision tolerance that will allow the incumbent to work at a computer screen or monitor for extended periods of time.
- Must be able to analyze information from a variety of sources and be able to complete multiple mental tasks at once.
- Must be able to tolerate long periods of concentration and have good problem solving skills.
- Good reading and writing skills are required. Experience working with the public is essential.
- Demonstrated organizational, facilitation, communication and presentation skills are essential.



## **HIPAA COMPLIANCE OFFICER DESIGNATION**

The following individual is responsible for all aspects of City of Washington EMS's HIPAA Compliance and should be contacted whenever an issue arises involving the privacy or security of PHI gathered and maintained by City of Washington EMS. This person is the primary point of contact regarding all HIPAA-related inquiries, or complaints, and all parties requesting PHI or with questions regarding the use or disclosure of PHI of City of Washington EMS should be referred to this individual. All known and suspected breaches of unsecured PHI shall be reported to this individual, as well as any known or suspected violations of City of Washington EMS's HIPAA policies and procedures.

Caroline Scoville  
PO Box 296  
301 C Street  
Washington, KS 66968  
785-325-2284  
washems@washingtonks.net

## **POSITION DESCRIPTION LANGUAGE FOR HIPAA COMPLIANCE - ALL POSITIONS**

### **JOB RESPONSIBILITIES RELATED TO HIPAA COMPLIANCE**

1. The incumbent is expected to protect the privacy and security of all protected health information (PHI) and electronic PHI (e-PHI) in accordance with the Company's 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 the Company'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 or of membership or association with City of Washington EMS.
2. The incumbent may access PHI and e-PHI only to the extent that is necessary to complete your job duties. The incumbent may only share such information with those who have a need to know specific patient information you have in your possession to complete their job responsibilities related to treatment, payment or other company operations.
3. The incumbent is encouraged and expected to report, without the threat of retaliation, any concerns regarding the Company's policies and procedures on patient privacy or security and any observed practices in violation of those policies to the designated HIPAA Compliance Officer.
4. The incumbent is expected to actively participate in Company privacy and security training and is required to communicate privacy policy information to coworkers, students, patients and others in accordance with Company policy.

### **DISCLAIMER**

The information provided in this description has been designed to indicate the general nature and level of work performed by incumbents within this job. It is not designed to be interpreted as a comprehensive inventory of all duties, responsibilities, qualifications and working conditions required of employees assigned to this job. Management has sole discretion to add or modify duties of the job and to designate other functions as essential at any time. This job description is not an employment agreement or contract.

# **UPDATING HIPAA POLICIES, PROCEDURES AND TRAINING POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires City of Washington EMS to ensure that its HIPAA policies, procedures and training materials are up to date and effective in safeguarding the confidentiality, integrity and availability of protected health information ("PHI"). This policy outlines our commitment to adjust and update our policies and procedures accordingly, based on periodic reviews and evaluations of our existing practices and in light of new and changing risks to PHI. City of Washington EMS will also evaluate and consider new technologies and methodologies for securing PHI, as specified by guidance from the Secretary of Health and Human Services ("HHS").

## **SCOPE**

This policy applies to all City of Washington EMS staff members who are responsible for evaluating and updating current HIPAA policies and procedures and providing the updates to staff members. The HIPAA Compliance Officer will have the overall responsibility for monitoring all new developments in patient privacy and security of PHI and will recommend updates to our HIPAA Compliance Plan, as necessary. The HIPAA Compliance Officer should perform these duties in consultation with City of Washington EMS management and solicit the input of appropriate City of Washington EMS staff members, when appropriate.

## **PROCEDURE**

### *Maintaining Knowledge*

1. The HIPAA Compliance Officer will strive to keep current with all changes in the law and regulations that address the privacy and security of PHI.
2. The HIPAA Compliance Officer will review journals and newsletters on the subject of HIPAA, and will sign up for appropriate list-serves to obtain current information.
3. The HIPAA Compliance Officer will monitor HIPAA websites, such as the site for the Office of Civil Rights, for new information on HIPAA compliance.
4. The HIPAA Compliance Officer will participate in seminars and conferences on HIPAA as needed and as the budget allows.
5. The HIPAA Compliance Officer will consult with legal counsel as necessary to learn of new legal developments that could affect City of Washington EMS with respect to HIPAA issues.

### *Evaluation of HIPAA Policies and Procedures*

1. On at least an annual basis, the HIPAA Compliance Officer will convene a committee of managers and/or appropriate staff members to identify and review all existing HIPAA policies and procedures for compliance with current HIPAA laws and regulations.
2. Any member of the review committee or any other staff member may suggest changes to our HIPAA Policies or Procedures by submitting the suggestion to the HIPAA Compliance Officer for consideration.

3. The annual policy and procedure review will identify all changes that need to be made to our policies, based on the experience of staff and management, technological developments and changes in the regulatory environment during the prior year.
4. Any critical changes in the law or regulations that require a change in our privacy practices will be addressed immediately and incorporated into our privacy compliance program.
5. All complaints and concerns regarding the safeguarding of patient information will be evaluated by the HIPAA Compliance Officer to determine if policy or procedure changes need to be implemented.
6. Unwritten procedures and practices will also be reviewed to ensure compliance with HIPAA regulations.

*Evaluating and Updating HIPAA Training Programs*

1. The HIPAA Compliance Officer annually reviews all HIPAA-related training materials and will update those materials and keep them current with recent changes in privacy practices as necessary.
2. Additional in-service training will be scheduled as necessary to ensure that all current staff members are kept up to date on our current HIPAA policies and procedures.

## **HIPAA TRAINING POLICY**

### **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires that all members of City of Washington EMS's workforce be trained on our policies and procedures regarding privacy and security. This policy is meant to ensure that all of City of Washington EMS staff - including all employees, volunteers, students and trainees (collectively referred to as "staff members") - who have access to protected health information ("PHI") understand and are trained regarding City of Washington EMS's HIPAA policies and procedures.

### **SCOPE**

This policy applies to all City of Washington EMS staff members. This includes those who have access to PHI in any form.

### **PROCEDURE**

1. All current staff members must be trained on City of Washington EMS's HIPAA policies and procedures in accordance with HIPAA.
2. All new staff members will be required to undergo privacy training within a reasonable time upon association with City of Washington EMS.
3. All staff members who have undergone initial HIPAA training will be required to undergo HIPAA training within a reasonable time after there is a material change to City of Washington EMS's HIPAA policies and procedures.
4. The HIPAA training will be coordinated and tracked on the "HIPAA Training Log" Form by the HIPAA Compliance Officer or his or her designee. Training documentation will be maintained for six (6) years.
5. All staff members will receive copies of City of Washington EMS's HIPAA policies and procedures.
6. All staff members must personally complete the HIPAA training and verify completion and agree to adhere to City of Washington EMS's HIPAA policies and procedures.
7. Training will be conducted through the following method: Classroom Training.
8. All staff members shall sign the "HIPAA Training Log" after completing HIPAA training.



# **WORKFORCE SANCTIONS FOR VIOLATIONS OF HIPAA POLICIES AND PROCEDURES POLICY**

## **PURPOSE**

City of Washington EMS is responsible under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to administer appropriate sanctions to its workforce members who violate the HIPAA policies and procedures of the organization. This policy outlines our approach to violations of our HIPAA policies and procedures and emphasizes the fact that City of Washington EMS takes any breach of our policies and procedures very seriously.

## **SCOPE**

This policy applies to all City of Washington EMS staff members, including those staff members who may learn of patient information indirectly, and even if use of this information is not part of the staff member's responsibilities with City of Washington EMS.

**NOTE:** Any sanctions under this policy or any other policy will not apply to staff members who: 1) file a complaint with the federal government about potential HIPAA violations; 2) testify, assist, or participate in an investigation or compliance review proceeding or official government proceeding investigating HIPAA issues; and 3) oppose any actions by City of Washington EMS that are unlawful under HIPAA, when that opposition is made with the good faith belief that City of Washington EMS was violating HIPAA (as long as any opposition or filing of a complaint did not result in improper disclosure of PHI).

## **PROCEDURE**

1. City of Washington EMS will implement sanctions that are to be used when any staff member fails to comply with or violates our HIPAA policies and procedures.
2. Sanctions will be administered in a progressive manner, wherever possible. City of Washington EMS will administer sanctions to the degree necessary to correct improper behavior and to ensure the protection of patient privacy. The nature of the PHI involved in the incident will be considered.

(EXAMPLE: A first time violation where an employee revealed PHI to another staff member without any need to know may receive a verbal counseling or written warning, but if a first violation resulted in revealing PHI to someone who was not a staff member or business associate, a suspension may be warranted.)

3. Progressive sanctions may include the following:
  - a. Remedial HIPAA training and education;
  - b. Informal verbal counseling;
  - c. Formal verbal counseling with written documentation of the counseling;
  - d. Written warning;
  - e. Suspension;
  - f. Termination or expulsion from City of Washington EMS.

4. Staff members have an affirmative duty to report to management or the HIPAA Compliance Officer any suspected violation of our HIPAA policies and procedures.
5. Staff members shall be educated about this policy and the serious nature of violating our HIPAA policies. Staff members will be made aware of the potential sanctions that may occur, and will be made aware of any changes to this sanction policy.
6. A record of individual staff member sanctions will be kept in the respective staff member's file. Adherence to our HIPAA policies may also be considered as part of the staff member's performance evaluation.
7. In the event of a suspected or reported violation of our HIPAA policies, the HIPAA Compliance Officer will initiate an objective and comprehensive investigation that will include:
  - a. Interviews of potential witnesses;
  - b. Interviews of the alleged violator;
  - c. Preparation of an investigative report;
  - d. Presentation of the report to management with recommendations for sanctions (if any) or changes in our policies or practices.
8. At all times, whenever there is a suspected violation of our HIPAA policies or other breach of privacy, the HIPAA Compliance Officer will recommend immediate action to be taken to mitigate the violation and its impact on City of Washington EMS and any other parties.



# **MINIMUM NECESSARY REQUIREMENT AND ROLE-BASED ACCESS TO PHI POLICY**

## **PURPOSE**

Generally, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires that City of Washington EMS only use or disclose the minimum amount of protected health information ("PHI") that is needed to accomplish the intended purpose for which the use or disclosure is made. This policy outlines City of Washington EMS's commitment to adhere to HIPAA's "minimum necessary requirement." In order to effectively meet our obligations, this policy outlines the appropriate levels of access to PHI that specific staff members of City of Washington EMS should have – "Role Based Access." This policy does not in any way limit the amount of PHI that may be exchanged between City of Washington EMS staff members or between City of Washington EMS staff members and other individuals during the course of treating patients.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who have any degree of access to PHI at City of Washington EMS.

## **PROCEDURE**

City of Washington EMS retains strict requirements on the security, access, disclosure and use of PHI. Access, disclosure and use of PHI will be based on the role of the individual staff member in the organization, and only to the extent that the person needs to access and use the PHI to complete necessary responsibilities for City of Washington EMS. When PHI is accessed, disclosed and used, the individuals involved will make every effort, except in patient care situations, to only access, use, and disclose the minimum necessary amount of information needed to accomplish the intended purpose.

## **ROLE BASED ACCESS**

Access to PHI will be limited to those who need access to carry out their duties. The following table describes the specific categories or types of PHI to which identified persons need access, and any conditions that would apply to such access.

<b>Job Title</b>	<b>Description of PHI to Be Accessed</b>	<b>Conditions of Access to PHI</b>
FR/EMT/ EMT-I/ RN/MICT	Intake information from dispatch, patient care reports, QA and QI reports, records received from other facilities regarding patient care	May access only as part of completion of a patient event and post-event activities and only while actually on duty.
Full-Time EMT/City Clerk/City Treasurer/City Administrator	Intake information from dispatch, patient care reports, billing claim information, remittance advice, other patient information from facilities necessary for billing	May access only as part of duties to complete patient billing and follow up and only while actually on duty.
Dispatcher	Intake information, preplanned CAD information on patient	May access only as part of completion of an incident, from receipt of information necessary

	address	to dispatch a call, to the closing out of the incident and only while on duty.
Training Coordinator	Intake information from dispatch, patient care reports, QA and QI reports	May access only as a part of training and quality assurance activities. All individually identifiable patient information should be redacted prior to use in training and quality assurance activities.
Service Director/Asst Service Director	Intake information from dispatch, patient care reports, QA and QI reports, billing claim forms, remittance advice, other patient information necessary for oversight	May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel and compliance with the law.
Medical Director	Intake information from dispatch, patient care reports, QA and QI reports, other patient information necessary for oversight	May access only as part of training and quality assurance activities. May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel and compliance with the law.

Access to a patient's entire file will not be allowed except when necessary for a legitimate treatment, payment, or healthcare operations-related reason.

### DISCLOSURES TO AND AUTHORIZATIONS FROM THE PATIENT

City of Washington EMS may freely disclose PHI to patients who are the subject of the information and we may freely use and disclose PHI to the extent authorized by a patient. City of Washington EMS is required to limit disclosure to the minimum amount of information necessary when releasing it pursuant to a patient request or formal Authorization.

### CITY OF WASHINGTON EMS REQUESTS FOR PHI FROM OTHER PARTIES

If City of Washington EMS needs to request PHI from another party on a routine or recurring basis, we must limit our requests to only the minimum amount of information needed for the intended purpose, as described in the table below. For requests not addressed in the table below, City of Washington EMS must make this determination individually for each request, and this determination should be made by the HIPAA Compliance Officer. For example, if the request is non-recurring or non-routine, like making a request for documents pursuant to an audit request, we must make sure our request covers only the minimum necessary amount of information needed to accomplish the purpose of the request.

Holder of PHI	Purpose of Request	Information Reasonably Necessary
Skilled Nursing Facilities	To have adequate patient records to treat the patient, determine medical necessity for service, and to properly bill for services provided.	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments, patient care reports.

<b>Hospitals</b>	To have adequate patient records to treat the patient, determine medical necessity for service, and to properly bill for services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments, patient care reports.
<b>Mutual Aid Ambulance or Paramedic Services</b>	To have adequate patient records to treat the patient, conduct joint billing operations for patients mutually treated/transported by the Company	Patient care reports.

**PHI REQUESTS TO CITY OF WASHINGTON EMS FROM OTHER PARTIES**

City of Washington EMS will make reasonable efforts to release only the minimum amount of PHI that is necessary to accomplish the actual purpose of a request from a third party.

**INCIDENTAL DISCLOSURES**

City of Washington EMS understands that there will be times when there are incidental disclosures about PHI in the context of caring for a patient. HIPAA was not intended to impede common healthcare practices that are essential in providing healthcare to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversations between healthcare providers, or when PHI is able to be viewed by others, despite reasonable efforts to protect the PHI from view.

But all personnel must be sensitive to avoiding incidental disclosures to other healthcare providers and others who do not have a need to know the information. City of Washington EMS staff should be attentive to who is within earshot when making verbal statements about a patient's health information, and follow some of these common sense procedures for avoiding accidental or inadvertent disclosures:

**MEASURES TO PROTECT PHI**

1. Verbal PHI. Staff members should only discuss PHI with those who are involved in the care of the patient, regardless of physical location. When discussing PHI with patients, staff members should make sure that there are no other persons (including other City of Washington EMS staff members) in the area that could overhear the discussion. If so, the patient should be brought into a screened area before engaging in discussion.
2. Hard Copy PHI. All paper patient care reports should be stored in safe and secure areas when not in use. No paper records concerning a patient should be left in open bins or on desktops or other surfaces. Only those with a need to have the information for the completion of their job duties should have access to any paper records. Additionally, billing records, including all notes, remittance advices, charge slips or claim forms should not be left out in the open and should be stored in files or boxes that are secure and in an area with access limited to those who need access to the information for the completion of their job duties.
3. E-PHI. Computer access terminals and other mobile devices should be kept secure. Staff members should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All mobile devices such as laptops, ePCR's and cell phones should remain in the physical possession of the individual to whom they are assigned at all times.

## **STAFF USE AND DISTRIBUTION OF NOTICE OF PRIVACY PRACTICES POLICY AND PROCEDURE**

### **PURPOSE**

To ensure the City of Washington EMS provides each patient or patient representative of our service with a copy of its Notice of Privacy Practices (NPP). It is a requirement of the HIPAA Privacy rule that each patient is provided with a copy of this notice to inform them of the ways in which medical information about him or her may be used and disclosed and how they may have access to that information.

### **POLICY**

The City of Washington EMS staff shall distribute a copy of the City of Washington EMS's Notice of Privacy Practices (NPP) to each and every patient or patient representative.

### **PROCEDURE**

The City of Washington EMS has a "Consent to Treatment and Transport, Assignment of Benefits Authorization, Responsibility for Payment, and Acknowledgement of Receipt of Notice of Privacy Practices" form which must be given to each patient or patient representative for them to sign during each patient encounter. This form indicates permission from the patient or patient representative for treatment, transport, assignment of benefits, and responsibility for payment. The patient or patient representative's signature also indicates they have received a copy of the Notice of Privacy Practices (NPP), describing how medical information about the patient may be used and disclosed and how the patient may get access to this information.

If the nature of the call is such that a signature cannot be obtained at the time of or prior to the completion of the call, documentation must be given as to why. There is space on the form to document the inability of the patient or patient representative to sign. This must be completed if a signature is not obtained, and a notation made in the patient run form to indicate that the NPP was left with the patient. If the NPP is NOT left with the patient or patient representative at the time of or prior to the completion of the call, documentation must be given as to why, and the HIPAA Compliance Officer must be notified so that one may be delivered to the patient or patient representative as soon as reasonably possible. There is space on the form to indicate the Notice of Privacy Practices (NPP) was not given to the patient or patient representative, and a notation shall be made in the patient run form to indicate that the NPP was not left with the patient or patient representative.

In the event that a patient refuses treatment and/or transport by the City of Washington EMS, the patient still must be provided with a NPP, and must acknowledge receipt. On the back of the City of Washington EMS patient run forms, there is a "Refusal of Treatment and/or Transport; Discharge From Scene Against Medical Advice" section. When a patient signs this section, he/she is also acknowledging receipt of the NPP, as indicated in that section. If NPP is not delivered to patient, or patient refuses to sign form, notation of such shall be made in the patient run form. If NPP is not delivered to patient, HIPAA Compliance Officer shall forward a copy of NPP to patient as soon as reasonably possible.

## **NOTICE OF PRIVACY PRACTICES**

IMPORTANT: THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

City of Washington EMS is committed to protecting your personal health information. We are required by law to maintain the privacy of health information that could reasonably be used to identify you, known as "protected health information" or "PHI." We are also required by law to provide you with the attached detailed Notice of Privacy Practices ("Notice") explaining our legal duties and privacy practices with respect to your PHI.

We respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times.

PLEASE READ THE ATTACHED DETAILED NOTICE. IF YOU HAVE ANY QUESTIONS ABOUT IT, PLEASE CONTACT CAROLINE SCOVILLE, OUR HIPAA COMPLIANCE OFFICER, AT 785-325-2284 or [washems@washingtorks.net](mailto:washems@washingtorks.net).

### **DETAILED NOTICE OF PRIVACY PRACTICES**

Purpose of This Notice: This Notice describes your legal rights, advises you of our privacy practices, and lets you know how City of Washington EMS is permitted to use and disclose PHI about you.

### **USES AND DISCLOSURES OF YOUR PHI WE CAN MAKE WITHOUT YOUR AUTHORIZATION**

City of Washington EMS may use or disclose your PHI *without* your authorization, or *without* providing you with an opportunity to object, for the following purposes:

*Treatment.* This includes such things as verbal and written information that we obtain about you and use pertaining to your medical condition and treatment provided to you by us and other medical personnel (including doctors and nurses who give orders to allow us to provide treatment to you). It also includes information we give to other healthcare personnel to whom we transfer your care and treatment, and includes transfer of PHI via radio or telephone to the hospital or dispatch center as well as providing the hospital with a copy of the written record we create in the course of providing you with treatment and transport.

*Payment.* This includes any activities we must undertake in order to get reimbursed for the services that we provide to you, including such things as organizing your PHI, submitting bills to insurance companies (either directly or through a third party billing company), managing billed claims for services rendered, performing medical necessity determinations and reviews, performing utilization reviews, and collecting outstanding accounts.

*Healthcare Operations.* This includes quality assurance activities, licensing, and training programs to ensure that our personnel meet our standards of care and follow established policies and procedures, obtaining legal and financial services, conducting business planning, processing grievances and complaints, creating reports that do not individually identify you for data collection purposes, fundraising, and certain marketing activities.

*Fundraising.* We may contact you when we are in the process of raising funds for City of Washington EMS. In addition, we may use your PHI for certain fundraising activities. For example, we may use PHI that we collect about you, such as your name, home address, phone number or other information, in order to contact you to raise funds for our agency. We may also share this information with another organization that may contact you to raise money

on our behalf. If City of Washington EMS does use your PHI to conduct fundraising activities, you have the right to opt out of receiving such fundraising communications from City of Washington EMS. If you do not want to be contacted for our fundraising efforts, you should contact our HIPAA Compliance Officer, Caroline Scoville, in writing, by phone, or by email. Contact information for our HIPAA Compliance Officer is listed at the end of this Notice. We will also remind you of this right to opt out of receiving future fundraising communications every time that we use your PHI to conduct fundraising and contact you to raise funds. City of Washington EMS will not condition the provision of medical care on your willingness, or non-willingness, to receive fundraising communications.

*Reminders for Scheduled Transports and Information on Other Services.* We may also contact you to provide you with a reminder of any scheduled appointments for non-emergency ambulance and medical transportation, or for other information about alternative services we provide or other health-related benefits and services that may be of interest to you.

### **OTHER USES AND DISCLOSURE OF YOUR PHI WE CAN MAKE WITHOUT AUTHORIZATION.**

City of Washington EMS is also permitted to use or disclose your PHI *without* your written authorization in situations including:

- For the treatment activities of another healthcare provider;
- To another healthcare provider or entity for the payment activities of the provider or entity that receives the information (such as your hospital or insurance company);
- To another healthcare provider (such as the hospital to which you are transported) for the healthcare operations activities of the entity that receives the information as long as the entity receiving the information has or has had a relationship with you and the PHI pertains to that relationship;
- For healthcare fraud and abuse detection or for activities related to compliance with the law;
- To a family member, other relative, or close personal friend or other individual involved in your care if we obtain your verbal agreement to do so or if we give you an opportunity to object to such a disclosure and you do not raise an objection. We may also disclose health information to your family, relatives, or friends if we infer from the circumstances that you would not object. For example, we may assume that you agree to our disclosure of your personal health information to your spouse when your spouse has called the ambulance for you. In situations where you are incapable of objecting (because you are not present or due to your incapacity or medical emergency), we may, in our professional judgment, determine that a disclosure to your family member, relative, or friend is in your best interest. In that situation, we will disclose only health information relevant to that person's involvement in your care. For example, we may inform the person who accompanied you in the ambulance that you have certain symptoms and we may give that person an update on your vital signs and treatment that is being administered by our ambulance crew;
- To a public health authority in certain situations (such as reporting a birth, death or disease, as required by law), as part of a public health investigation, to report child or adult abuse, neglect or domestic violence, to report adverse events such as product defects, or to notify a person about exposure to a possible communicable disease, as required by law;
- For health oversight activities including audits or government investigations, inspections, disciplinary proceedings, and other administrative or judicial actions undertaken by the government (or their contractors) by law to oversee the healthcare system;
- For judicial and administrative proceedings, as required by a court or administrative order, or in some cases in response to a subpoena or other legal process;
- For law enforcement activities in limited situations, such as when there is a warrant for the request, or when the information is needed to locate a suspect or stop a crime;
- For military, national defense and security and other special government functions;
- To avert a serious threat to the health and safety of a person or the public at large;



- For workers' compensation purposes, and in compliance with workers' compensation laws;
- To coroners, medical examiners, and funeral directors for identifying a deceased person, determining cause of death, or carrying on their duties as authorized by law;
- If you are an organ donor, we may release health information to organizations that handle organ procurement or organ, eye or tissue transplantation, or to an organ donation bank, as necessary to facilitate organ donation and transplantation; and
- For research projects, but this will be subject to strict oversight and approvals and health information will be released only when there is a minimal risk to your privacy and adequate safeguards are in place in accordance with the law.

## **USES AND DISCLOSURES OF YOUR PHI THAT REQUIRE YOUR WRITTEN CONSENT**

Any other use or disclosure of PHI, other than those listed above, will only be made with your written authorization (the authorization must specifically identify the information we seek to use or disclose, as well as when and how we seek to use or disclose it). Specifically, we must obtain your written authorization before using or disclosing your: (a) psychotherapy notes, other than for the purpose of carrying out our own treatment, payment or health care operations purposes; (b) PHI for marketing when we receive payment to make a marketing communication; or (c) PHI when engaging in a sale of your PHI. You may revoke your authorization at any time, in writing, except to the extent that we have already used or disclosed medical information in reliance on that authorization.

## **YOUR RIGHTS REGARDING YOUR PHI**

As a patient, you have a number of rights with respect to your PHI, including:

*Right to access, copy or inspect your PHI.* You have the right to inspect and copy most of the medical information that we collect and maintain about you. Requests for access to your PHI should be made in writing to our HIPAA Compliance Officer. In limited circumstances, we may deny you access to your medical information, and you may appeal certain types of denials. We have available forms to request access to your PHI, and we will provide a written response if we deny you access and let you know your appeal rights. If you wish to inspect and copy your medical information, you should contact Caroline Scoville, our HIPAA Compliance Officer.

We will normally provide you with access to this information within 30 days of your written request. If we maintain your medical information in electronic format, then you have a right to obtain a copy of that information in an electronic format. In addition, if you request that we transmit a copy of your PHI directly to another person, we will do so provided your request is in writing, signed by you (or your representative), and you clearly identify the designated person and where to send the copy of your PHI.

We may also charge you a reasonable cost-based fee for providing you access to your PHI, subject to the limits of applicable state law.

*Right to request an amendment of your PHI.* You have the right to ask us to amend protected health information that we maintain about you. Requests for amendments to your PHI should be made in writing and you should contact Caroline Scoville, our HIPAA Compliance Officer if you wish to make a request for amendment and fill out an amendment request form.

When required by law to do so, we will amend your information within 60 days of your request and will notify you when we have amended the information. We are permitted by law to deny your request to amend your medical

information in certain circumstances, such as when we believe that the information you have asked us to amend is correct.

*Right to request an accounting of uses and disclosures of your PHI.* You may request an accounting from us of disclosures of your medical information. If you wish to request an accounting of disclosures of your PHI that are subject to the accounting requirement, you should contact Caroline Scoville, our HIPAA Compliance Officer, and make a request in writing.

You have the right to receive an accounting of certain disclosures of your PHI made within six (6) years immediately preceding your request. But, we are not required to provide you with an accounting of disclosures of your PHI: (a) for purposes of treatment, payment, or healthcare operations; (b) for disclosures that you expressly authorized; (c) disclosures made to you, your family or friends; or (d) for disclosures made for law enforcement or certain other governmental purposes.

*Right to request restrictions on uses and disclosures of your PHI.* You have the right to request that we restrict how we use and disclose your medical information for treatment, payment or healthcare operations purposes, or to restrict the information that is provided to family, friends and other individuals involved in your healthcare. However, we are only required to abide by a requested restriction under limited circumstances, and it is generally our policy that we will not agree to any restrictions unless required by law to do so. If you wish to request a restriction on the use or disclosure of your PHI, you should contact Caroline Scoville, our HIPAA Compliance Officer, and make a request in writing.

City of Washington EMS is required to abide by a requested restriction when you ask that we not release PHI to your health plan (insurer) about a service for which you (or someone on your behalf) have paid City of Washington EMS in full. We are also required to abide by any restrictions that we agree to. Notwithstanding, if you request a restriction that we agree to, and the information you asked us to restrict is needed to provide you with emergency treatment, then we may disclose the PHI to a healthcare provider to provide you with emergency treatment.

A restriction may be terminated if you agree to or request the termination. Most current restrictions may also be terminated by City of Washington EMS as long we notify you. If so, PHI that is created or received after the restriction is terminated is no longer subject to the restriction. But, PHI that was restricted prior to the notice to you voiding the restriction must continue to be treated as restricted PHI.

*Right to notice of a breach of unsecured protected health information.* If we discover that there has been a breach of your unsecured PHI, we will notify you about that breach by first-class mail dispatched to the most recent address that we have on file. If you prefer to be notified about breaches by electronic mail, please contact Caroline Scoville, our HIPAA Compliance Officer, to make City of Washington EMS aware of this preference and to provide a valid email address to send the electronic notice. You may withdraw your agreement to receive notice by email at any time by contacting Caroline Scoville.

*Right to request confidential communications.* You have the right to request that we send your PHI to an alternate location (e.g., somewhere other than your home address) or in a specific manner (e.g., by email rather than regular mail). However, we will only comply with reasonable requests when required by law to do so. If you wish to request that we communicate PHI to a specific location or in a specific format, you should contact Caroline Scoville, our HIPAA Compliance Officer, and make a request in writing.

## **INTERNET, EMAIL AND THE RIGHT TO OBTAIN COPY OF PAPER NOTICE**



If we maintain a web site, we will prominently post a copy of this Notice on our web site and make the Notice available electronically through the web site. If you allow us, we will forward you this Notice by electronic mail instead of on paper and you may always request a paper copy of the Notice.

## **REVISIONS TO THE NOTICE**

City of Washington EMS is required to abide by the terms of the version of this Notice currently in effect. However, City of Washington EMS reserves the right to change the terms of this Notice at any time, and the changes will be effective immediately and will apply to all PHI that we maintain. Any material changes to the Notice will be promptly posted in our facilities and on our web site, if we maintain one. You can get a copy of the latest version of this Notice by contacting Caroline Scoville, our HIPAA Compliance Officer.

## **YOUR LEGAL RIGHTS AND COMPLAINTS**

You also have the right to complain to us, or to the Secretary of the United States Department of Health and Human Services, if you believe that your privacy rights have been violated. You will not be retaliated against in any way for filing a complaint with us or to the government.

Should you have any questions, comments or complaints, you may direct all inquiries to Caroline Scoville, our HIPAA Compliance Officer. Individuals will not be retaliated against for filing a complaint.

If you have any questions or if you wish to file a complaint or exercise any rights listed in this Notice, please contact:

Caroline Scoville, HIPAA Compliance Officer  
City of Washington EMS  
PO Box 296  
301 C Street  
Washington, KS 66968  
785-325-2284  
washems@washingtonks.net

Effective Date of the Notice: 12/2/2013

**CONSENT TO TREATMENT AND TRANSPORT, ASSIGNMENT OF BENEFITS  
AUTHORIZATION, RESPONSIBILITY FOR PAYMENT, AND ACKNOWLEDGEMENT OF  
RECEIPT OF NOTICE OF PRIVACY PRACTICES**

**Consent to Treatment and Transport:** I give my consent for treatment of my medical condition by the City of Washington EMS personnel and transportation to the hospital specified below. I understand that I will be taken to the hospital of my choice unless EMS personnel perceive an urgent or life-threatening condition which may threaten my life or future health, in which case I will be transported to the closest medical facility able to treat or stabilize my condition.

\_\_\_\_\_  
Patient or Patient Representative Signature

\_\_\_\_\_  
Receiving Hospital or Facility

\_\_\_\_\_  
Date

**Assignment of Benefits Authorization:** I understand that I am financially responsible for the services provided to me by the City of Washington EMS regardless of insurance coverage. I request that payment of authorized *Medicare, Medicaid, or other Commercial Insurance Companies* benefits be made either to me or on my behalf to the City of Washington EMS for any services furnished to me by the City of Washington EMS. I authorize and direct any holder of medical information or documentation about me to release to the Centers for Medicare and Medicaid Services and its carriers and agents, as well as to City of Washington EMS and its billing agents and any other payers or insurers, any information or documentation needed to determine these benefits or benefits payable for any services provided to me by City of Washington EMS, now or in the future. I agree to immediately remit to City of Washington EMS any payments that I receive directly from any source for the services provided to me and I assign all rights to such payments to City of Washington EMS.

**Responsibility for Payment:** If I do not have insurance coverage for the above services, or if my insurance carrier denies payments of the above services, for any and all reasons, I understand that I am responsible for payment of all non-covered and non-allowed services provided to me as well as for any deductible and/or co-insurance payments. I agree to contact the City of Washington EMS business office to make payment arrangements or establish a payment schedule upon receipt of the charges for the above services.

**Acknowledgement of Receipt of Notice of Privacy Practices:** I also acknowledge that I have received a copy of the City of Washington EMS's Notice of Privacy Practices. A copy of this form is as valid as the original.

\_\_\_\_\_  
Patient Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Patient Representative's Signature

\_\_\_\_\_  
Relationship to Patient

Patient unable to sign because:  
\_\_\_\_\_

\_\_\_\_\_ Please send me a copy of this document

\_\_\_\_\_ Check here if NPP not given to patient or patient representative



# **PATIENT REQUESTS FOR ACCESS TO PROTECTED HEALTH INFORMATION POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") grants individuals the right to access their protected health information ("PHI") contained in a designated records set ("DRS"). (See *Policy on Designated Records Sets*). City of Washington EMS must afford individuals this right of access in accordance with federal and state law. To ensure that City of Washington EMS complies with its obligations, this policy outlines our procedures for handling requests for patient access and establishes the procedures by which patients or authorized representatives may request access to PHI.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who receive requests from patients for access to PHI. Generally, all access requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all access requests.

## **PROCEDURE**

### *Requests for Access from the Patient or the Patient's Personal Representative*

1. Patients and their authorized representatives shall be granted a right of access to inspect and obtain a copy of their PHI contained in a DRS maintained by City of Washington EMS.
2. If a patient or their authorized representative requests access to or a copy of a patient's PHI, the requestor shall be referred to the HIPAA Compliance Officer. The HIPAA Compliance Officer shall request that the patient or authorized representative complete City of Washington EMS's "Request for Access to Protected Health Information" Form.
3. The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identity of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Request for Access to Protected Health Information Form" via email, mail or fax.
4. Upon receipt of the completed "Request for Access to Protected Health Information Form" and verification of the requestor's identity, the HIPAA Compliance Officer will act upon the request within 30 days, preferably sooner. Generally, City of Washington EMS must respond to requests for access to PHI within 30 days of receipt of the access request.
5. If City of Washington EMS is unable to respond to the request within these time frames, the requestor must be given a written notice no later than the initial due date for a response, explaining why City of Washington EMS could not respond within the time frame, and in that case City of Washington EMS may extend the response time by an additional 30 days.

### *Requests for Access from the Patient's Attorney*

1. If City of Washington EMS receives a request for a patient's PHI from the patient's attorney, the HIPAA Compliance Officer shall verify that the patient has authorized the release of PHI. Generally, the request should be accompanied by a form or letter, signed by the patient, stating that the patient authorizes the release of the requested PHI to the attorney. If there is a signed form or letter from the patient authorizing the release of the PHI requested (or some other valid authorization from the patient), then the HIPAA Compliance Officer may release the PHI to the attorney in accordance with what the authorization states.
2. If the request from the patient's attorney is not accompanied by a signed request form or letter from the patient (or some other valid patient authorization), the HIPAA Compliance Officer shall contact the attorney and inform the attorney that City of Washington EMS will not release the information without valid authorization from the patient. City of Washington EMS shall not release any PHI to the attorney until the patient authorizes the release.

#### *Approval of a Request for Access*

1. Upon approval of access, the patient or authorized representative should generally be provided the right of access in the manner requested on the Form. City of Washington EMS will either provide a copy of the PHI to the requestor in the format requested or arrange for a convenient time for the patient to come into City of Washington EMS to copy their PHI. If City of Washington EMS uses or maintains the PHI requested electronically, City of Washington EMS will provide a copy of the PHI in an electronic format if the patient or authorized representative requests an electronic copy. City of Washington EMS will also transmit a copy of the PHI directly to an entity or person designated by the patient or authorized representative, provided that the written direction is signed and clearly identifies the designated party.
2. City of Washington EMS will establish a reasonable charge for copying PHI for the patient or authorized representative in accordance with federal and state laws. The fee for providing an electronic copy of PHI shall not be greater than City of Washington EMS's labor costs in responding to the request for the copy. The HIPAA Compliance Officer shall consult with legal counsel regarding applicable laws regarding fee limitations.
3. The requestor will not be given access to the actual files or systems that contain the DRS. Rather, copies of the records shall be provided for the patient or requestor to view in a confidential area under the direct supervision of a designated Company staff member. UNDER NO CIRCUMSTANCES SHOULD ORIGINALS OF PHI LEAVE THE PREMISES.
4. Whenever a patient or requestor accesses a DRS, a note should be maintained in a log book indicating the time and date of the request, the date access was provided, what specific records were provided for review, and what copies were left with the patient or requestor.

#### *Denial of a Request for Access*

1. If the request for access is denied, the HIPAA Compliance Officer shall send the requestor a "Denial of Request for Access to Protected Health Information Form," outlining the reason for the denial and explaining the individual's rights regarding the denial. Patient access may be denied for the reasons listed below:

- a. If the information the patient requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
  - b. If the information the patient requested was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information;
  - c. If a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
  - d. If the PHI makes reference to another person (other than a healthcare provider) and a licensed health professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person; or
  - e. If the request for access is made by a requestor as a personal representative of the individual and a licensed health professional has determined, in the exercise of professional judgment, that access is reasonably likely to cause harm to the individual or another person.
2. If the denial of the request for access to PHI is for reasons c., d., or e above, then the patient may request a review of the denial of access by sending a written request to the HIPAA Compliance Officer.
- a. City of Washington EMS will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. City of Washington EMS will promptly refer the request to this designated review official. The review official will determine within a reasonable period of time whether the denial is appropriate. City of Washington EMS will provide the patient with written notice of the determination of the designated reviewing official.
  - b. The patient may also file a complaint in accordance with City of Washington EMS's "Procedure for Filing Complaints About Privacy Practices" if the patient is not satisfied with City of Washington EMS's determination.

## PATIENT REQUEST FOR ACCESS TO PROTECTED HEALTH INFORMATION

Patient Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Email: \_\_\_\_\_

Date of Birth: \_\_\_\_\_ SSN: \_\_\_\_\_

### *Right to Request Access to Your PHI and Our Duties:*

You (or your authorized representative) have the right to inspect or obtain a copy of your protected health information ("PHI") that we maintain in a designated record set. If we maintain your PHI in electronic format, then you also have a right to obtain a copy of that information electronically. In addition, you may request that we transmit a copy of your PHI directly to another person and we will honor that request when required by law to do so. Requests to transmit PHI to another party must be in writing, signed by you (or your representative), and clearly identify the designated person to whom the PHI should be sent, and where the PHI should be sent.

Generally, we will provide you (or your authorized representative) access to your PHI within thirty (30) days of your request. We may verify the identity of any person who requests access to PHI, as well as the authority of the person to have access to the PHI by asking the requestor to provide the patient's social security number, date of birth, legal authority to act on behalf of the patient (such as a power of attorney) or other information necessary to verify that the requestor has the right to access PHI. In limited circumstances, we may deny you access to your PHI, and you may appeal certain types of denials. We may also charge you a reasonable cost-based fee for providing you access to your PHI, subject to the limits of applicable state law.

### Request for Access to PHI:

Below, please describe the PHI that you are requesting access to with as much specificity as possible. Specify dates of service and other details that will allow City of Washington EMS to accurately and completely fulfill your request.

---

---

---

### Specify How You Would Like us to Provide Access:

Please check all that apply and fill out the requested information, where indicated.

Please provide me with a copy of my PHI.

Mail. Please send a copy of my PHI to me at the following address:

Street: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Format (paper copy, digital copy on a disc, etc.):  
\_\_\_\_\_

\_\_\_\_ Email. Please email a copy of my PHI to the following email address in the specified format:

Email address: \_\_\_\_\_

Format (PDF, Word, etc.): \_\_\_\_\_

\_\_\_\_ Please transmit a copy of my PHI to the following party at the following mailing address or email address in the specified format:

Designated Party: \_\_\_\_\_

Street: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Email address: \_\_\_\_\_

Format (Paper, PDF, Word, etc.): \_\_\_\_\_

\_\_\_\_ I would like to inspect a copy of my PHI at City of Washington EMS's place of business (City of Washington EMS will arrange a convenient time and place for you to inspect a copy of your PHI during normal business hours.)

Signature of Requestor: \_\_\_\_\_ Request Date: \_\_\_\_\_

Requestor Information (if requestor is different from patient):

Name: \_\_\_\_\_

Relationship to Patient (parent, legal guardian, etc.): \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_



## **DENIAL OF PATIENT REQUEST FOR ACCESS**

Date

City of Washington EMS  
PO Box 296  
301 C Street  
Washington, KS 66968

Name of Requestor  
Address  
City, State, Zip

Dear [INSERT REQUESTOR'S NAME]:

We have carefully reviewed your request to have access to certain protected health information (PHI). Unfortunately, we are unable to grant your request for access to this information. The basis for this denial is that:

1. \_\_\_ The information you requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
2. \_\_\_ The information you requested was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information;
3. \_\_\_ A licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
4. \_\_\_ The protected health information makes reference to another person (other than a healthcare provider) and a licensed health professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person; or
5. \_\_\_ The request for access is made by you as a personal representative of the individual about whom you are requesting the information, and a licensed health professional has determined, in the exercise of professional judgment, that access by you is reasonably likely to cause harm to the individual or another person.

The denials for reasons #1 or #2 are final and you may not appeal the decision to deny access to the information. Denials of access for reasons #3, #4, or #5 may be reviewed in accordance with the review procedures described below.

### **REVIEW PROCEDURES**

If the denial of your request for access to PHI is for reasons #3, #4, or #5, you may request a review of the denial of access by sending a written request to Caroline Scoville, our HIPAA Compliance Officer, at the above address.

We will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny you access. We will promptly refer your request to this designated review official. The review official will

determine within a reasonable period of time whether the denial is appropriate. We will provide you with written notice of the determination of the designated review official.

You may also file a complaint in accordance with our complaint procedures (available upon request) if you are not satisfied with our determination.

Sincerely,

Caroline Scoville  
HIPAA Compliance Officer  
City of Washington EMS

# **PATIENT REQUESTS FOR AMENDMENT OF PROTECTED HEALTH INFORMATION POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") grants individuals the right to request that City of Washington EMS amend their protected health information ("PHI") contained in a Designated Record Set ("DRS"). (See *Policy on Designated Record Sets*). City of Washington EMS has an obligation to afford individuals the right to request an amendment to their PHI in accordance with federal and state law. To ensure that City of Washington EMS complies with its obligations, this policy outlines procedures for handling patient requests for amendment of their PHI and establishes the procedures by which patients or authorized representatives may make a request for an amendment to PHI.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who handle requests from patients for amendment to PHI. Generally, all requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all requests for amendment of PHI.

## **PROCEDURE**

### *Requests for Amendment of PHI*

1. Patients or their authorized representatives shall be granted the right to request an amendment to a patient's PHI contained in the DRS.
2. If a patient or authorized representative requests an amendment to PHI, the requestor shall be referred to the HIPAA Compliance Officer. The HIPAA Compliance Officer shall request that the patient or authorized representative complete City of Washington EMS's "Patient Request for Amendment of Protected Health Information" Form.
3. The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identity of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Request for Amendment of Protected Health Information Form" via email, mail or fax.
4. City of Washington EMS must act upon a request for amendment of PHI within 60 days of the request. If City of Washington EMS is unable to act upon the request within 60 days, it must provide the requestor with a written statement of the reasons for the delay, and in that case may extend the time period in which to comply by an additional 30 days.

### *Granting the Request for Amendment of PHI*

1. If the HIPAA Compliance Officer grants the request for amendment, then the requestor will receive a letter (See "Acceptance of Patient Request for Amendment" Form), indicating that the appropriate amendment to the PHI or record that was the subject of the request has been made.
2. The letter will contain a form for the patient to complete, sign, and return to City of Washington EMS. On the form, the patient must identify individuals who may need the amended PHI and sign the statement giving City of Washington EMS permission to provide them with the updated PHI.
3. City of Washington EMS must provide the amended information to individuals identified by the patient as well as persons or business associates that have such information and who may have relied on or could be reasonably expected to rely on the amended PHI.

#### *Denying the Request for Amendment of PHI*

1. City of Washington EMS may deny a request to amend PHI for the following reasons:
  - (a) If City of Washington EMS did not create the PHI at issue;
  - (b) The information is not part of the DRS;
  - (c) The PHI is accurate and complete;
  - (d) The information would not be available for inspection as provided by law; or
  - (e) The information was received from someone else under a promise of confidentiality.
2. City of Washington EMS must provide a written denial (See "Denial of Patient Request for Amendment" Form), and the denial must be written in plain language and contain the following information:
  - (a) The reason for the denial;
  - (b) The individual's right to submit a statement disagreeing with the denial and how the individual may file such a statement;
  - (c) A statement that, if the individual does not submit a statement of disagreement, the individual may request that City of Washington EMS provide the request for amendment and the denial with any future disclosures of the PHI; and
  - (d) A statement that the individual may file a complaint with City of Washington EMS or with the Office for Civil Rights of the Department of Health and Human Services.
3. City of Washington EMS shall provide a copy of our "Procedure for Filing Complaints About Privacy Practices" if the requestor indicates that he or she wants to file a complaint against City of Washington EMS.
4. If the individual submits a "statement of disagreement," City of Washington EMS may prepare a written rebuttal statement to the patient's statement of disagreement. The statement of disagreement will be appended to the PHI, or at City of Washington EMS's option, a summary of the disagreement will be appended, along with the rebuttal statement of City of Washington EMS.

#### *Administrative Obligations*

1. If City of Washington EMS receives a notice from another covered entity, such as a hospital, that the other covered entity has amended its own PHI in relation to a particular patient, City of Washington EMS must amend

its own PHI that may be affected by the amendments. The HIPAA Compliance Officer shall be responsible for performing this task.

2. City of Washington EMS will add the "Patient Request for Amendment of Protected Health Information Form," the denial or granting of the request, as well as any statement of disagreement by the patient and any rebuttal statement by City of Washington EMS to the DRS. The HIPAA Compliance Officer shall be responsible for performing this task.

**PATIENT REQUEST FOR AMENDMENT OF PROTECTED HEALTH INFORMATION**

Patient Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Email: \_\_\_\_\_ Date of Birth: \_\_\_\_\_

**Right to Request Amendment of Your PHI and Our Duties:**

You (or your authorized representative) have the right to ask us to amend protected health information (PHI) that we maintain about you in a designated record set. When required by law to do so, we will amend your information within 60 days of your request and will notify you when we have amended the information. We are permitted by law to deny your request to amend your medical information in certain circumstances, such as when we believe the information you have asked us to amend is correct. City of Washington EMS is entitled to perform and bill for services based on PHI in its current form or upon which it has already relied until such time as the amended information becomes effective.

**Request for Amendment of PHI:**

Below, please describe the PHI that you are requesting us to amend and how this information should be amended with as much specificity as possible. Specify dates of service and other details that will allow City of Washington EMS to accurately and completely fulfill your request.

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Signature of Requestor:** \_\_\_\_\_ **Request Date:** \_\_\_\_\_

**Requestor Information (if requestor is different from patient):**

Name: \_\_\_\_\_

Relationship to Patient (parent, legal guardian, etc.): \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

**ACCEPTANCE OF PATIENT REQUEST FOR AMENDMENT**

Date

City of Washington EMS  
PO Box 296  
301 C Street  
Washington, KS 66968

Name of Requestor  
Address  
City, State, Zip

Dear [INSERT NAME OF REQUESTOR]:

We have reviewed your request for amendment to protected health information (PHI). Please be advised that we have made the appropriate amendment to the PHI or record that was the subject of your request.

We are now requesting that you grant us permission to notify persons who may have relied upon the original PHI or who may need to see the amended PHI. On the attached Authorization form, please identify to us any individuals you know of who may need the amended PHI and then sign the statement giving us permission to provide them with the updated PHI. Then, please return that form to City of Washington EMS to the address listed above, Attn: Caroline Scoville.

If you have any questions, please contact City of Washington EMS's HIPAA Compliance Officer at 785-325-2284 or [washems@washingtonks.net](mailto:washems@washingtonks.net).

Sincerely,

Caroline Scoville  
HIPAA Compliance Officer  
City of Washington EMS

Enclosure: Parties That Need My Amended PHI Form

**PARTIES THAT NEED MY AMENDED PHI**

(To be attached to Acceptance of Request for Amendment of PHI Form and mailed to patient)

I request that City of Washington EMS provide my amended PHI to the following persons (list contact information for individuals that need the amended PHI):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Signature of Requestor: \_\_\_\_\_ Date: \_\_\_\_\_

**Requestor Information**

Name: \_\_\_\_\_

Relationship to Patient (if patient is not requestor): \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_



## **DENIAL OF PATIENT REQUEST FOR AMENDMENT**

Date

City of Washington EMS  
PO Box 296  
301 C Street  
Washington, KS 66968

Name of Requestor  
Address  
City, State, Zip

Dear [INSERT PATIENT NAME]:

We have reviewed your request for amendment to your protected health information. Please be advised that we must deny your request to amend this information at this time.

The basis for this denial is:

1. \_\_\_ City of Washington EMS did not create the PHI at issue;
2. \_\_\_ The PHI is not part of a designated record set;
3. \_\_\_ City of Washington EMS has determined that the PHI at issue is accurate and complete;
4. \_\_\_ The PHI is not available for inspection as provided by law; or
5. \_\_\_ The PHI was received from someone else under a promise of confidentiality.

You have the right to submit a written statement to us if you disagree with our denial of your request. You may file your statement directly to our HIPAA Compliance Officer at the address listed above, Attn: Caroline Scoville.

If you do not submit a statement disagreeing with our decision to deny your amendment request, you may request that we provide your initial request for amendment, and a copy of our denial of your request with any future disclosures of the protected health information (PHI) that was the subject of your request for denial.

You also have the right to file a complaint with us or with the federal government if you disagree with our decision to deny your request to amend your PHI. Please contact Caroline Scoville at 785-325-2284 or [washems@washingtonks.net](mailto:washems@washingtonks.net) for more information about filing a complaint with City of Washington EMS or the Office for Civil Rights.

Sincerely,

Caroline Scoville  
HIPAA Compliance Officer  
City of Washington EMS

# **PATIENT REQUESTS FOR RESTRICTION OF PROTECTED HEALTH INFORMATION POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") grant individuals the right to request that City of Washington EMS restrict its use of PHI contained in a Designated Record Set ("DRS"). (See Policy on Designated Record Sets). City of Washington EMS has an obligation to abide by a requested restriction in accordance with federal and state law. To ensure that City of Washington EMS complies with its obligations under HIPAA and the HITECH Act, this policy outlines procedures for handling requests for restrictions on the use of PHI and establishes the procedures by which patients or their authorized representatives may request a restriction on the use of PHI.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who handle requests from patients for a restriction on the use of their PHI. Generally, all requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all requests for restrictions on the use of PHI.

## **PROCEDURE**

### *Requests for Restriction*

1. City of Washington EMS will permit patients to request restrictions on the use and disclosure of their PHI: (i) to carry out treatment, payment or health care operations and/or (ii) to people involved in their care or for notification purposes.
2. All requests for restriction on the use and disclosure of PHI shall be referred to the HIPAA Compliance Officer who shall request that the patient or authorized representative complete and submit City of Washington EMS's "Patient Request for Restriction of Protected Health Information" Form. All requests will be reviewed and denied or approved by the HIPAA Compliance Officer in accordance with this policy. The HIPAA Compliance Officer shall utilize the "Review of Patient Request for Restriction of Protected Health Information" Form when reviewing restriction requests.
3. The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identify of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Patient Request for Restriction of Protected Health Information" Form via email, mail or fax.
4. Under most circumstances, City of Washington EMS is not legally required to agree to any request to restrict the use and disclosure of PHI, and given the emergent nature of our operation, City of Washington EMS generally will not agree to a restriction unless required by law to do so. However, City of Washington EMS is required to abide by any restrictions that it agrees to.

### *Granting a Request for Restriction*

1. City of Washington EMS will and must comply with a requested restriction if: (i) the request concerns the disclosure of PHI to a health plan for purposes of carrying out payment or healthcare operations; and (ii) the request pertains to a service for which City of Washington EMS has been paid out-of-pocket in full. In other words, City of Washington EMS must grant patients the right to pay for a service out-of-pocket and abide by a request not to submit a claim to the insurer for that service.
2. If City of Washington EMS receives a request from a patient or authorized representative asking City of Washington EMS to refrain from submitting PHI to a health plan and the HIPAA Compliance Officer determines that City of Washington EMS has either been paid in full, or that City of Washington EMS has received reasonable assurances that it will be paid in full for that service, then City of Washington EMS will grant the request for restriction and not submit a claim to insurance for that service. Patients must make a new request for all subsequent services.
3. If City of Washington EMS agrees to a requested restriction, the HIPAA Compliance Officer shall inform the patient of that fact in writing, by sending an "Acceptance of Request for Restriction of Protected Health Information" letter to the patient. The HIPAA Compliance Officer shall also note on the "Review of Patient Request for Restriction of Protected Health Information" Form that the request was accepted and document all pertinent information regarding the request and acceptance (date, payment received, etc.).
4. City of Washington EMS may not use or disclose PHI in violation of the agreed upon restriction. Notwithstanding, if the individual who requested the restriction is in need of an emergency service, and the restricted PHI is needed to provide the emergency service, then City of Washington EMS may use the restricted PHI or may disclose such PHI to another healthcare provider to provide treatment to the individual.
5. The HIPAA Compliance Officer shall also inform all other necessary parties at City of Washington EMS and its business associates, such as its billing company, about the accepted restriction and take all appropriate steps to ensure that those parties abide by the restriction.
6. The HIPAA Compliance Officer shall add the "Patient Request for Restriction of Protected Health Information" Form, the Acceptance letter and documentation regarding the acceptance of the request to the DRS.

#### *Denying the Request for Restriction*

1. Unless City of Washington EMS is required by law to agree to a request for restriction of PHI, the HIPAA Compliance Officer shall deny the request in writing, by dispatching a "Denial of Patient Request for Restriction of PHI" letter to the patient.
2. The HIPAA Compliance Officer shall also note on the "Patient Request for Restriction of Protected Health Information" Form that the request was denied, and document all pertinent information regarding the request and denial (date, reason for denial, etc.).

#### *Termination of Restrictions*

1. A restriction may be terminated if the individual agrees to or requests the termination.
2. Oral agreements to terminate restrictions must be documented.

3. Most restrictions may also be terminated by City of Washington EMS as long as City of Washington EMS notifies the patient that PHI created or received after the restriction is removed is no longer restricted. PHI that was restricted prior to the notice voiding the restriction must continue to be treated as restricted PHI.
4. City of Washington EMS should not terminate a restriction regarding PHI that pertains to a service for which City of Washington EMS has been paid in full and where a patient has requested that such PHI not be disclosed to the patient's health plan. Such restriction will only apply with respect to that service and not to subsequent services. The patient must make another request, and pay out-of-pocket for each service.

## **PATIENT REQUEST FOR RESTRICTION OF PROTECTED HEALTH INFORMATION**

Patient Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Email: \_\_\_\_\_ Date of Birth: \_\_\_\_\_

### *Right to Request Restrictions Regarding Your PHI and Our Duties:*

You (or your authorized representative) have the right to request that we restrict how we use or disclose your PHI for treatment, payment or healthcare operations, or to restrict the information that is provided to family, friends and other individuals involved in your healthcare. However, we are only required to agree to a requested restriction when you ask that we not release PHI to your health plan (insurer) about a service for which you have paid City of Washington EMS in full. We are permitted, but not required, to agree to other requested restrictions. But, we are required to abide by any restrictions that we have agreed to honor.

### *Request for Restriction of PHI:*

Below, please explain your request for restricted uses and disclosures of your PHI. Please indicate for what purposes you would like to restrict the PHI and specific parties to whom you would like us to not provide PHI. City of Washington EMS will consider your request and promptly let you know whether or not we agree to your requested restriction(s).

---

---

---

Signature of Requestor: \_\_\_\_\_ Request Date: \_\_\_\_\_

### *Requestor Information (if requestor is different from patient):*

Name: \_\_\_\_\_

Relationship to Patient (parent, legal guardian, etc.): \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

**REVIEW OF PATIENT REQUEST FOR RESTRICTION OF PROTECTED HEALTH INFORMATION**

**FOR CITY OF WASHINGTON EMS USE ONLY:**

(To Be Completed by City of Washington EMS HIPAA Compliance Officer after a request for restriction)

Patient Name: \_\_\_\_\_ Date Request Received: \_\_\_\_\_

**RESTRICTION REQUEST DENIAL**

Date of Denial: \_\_\_\_\_ Date Patient Notified: \_\_\_\_\_

Reason for Denial:

\_\_\_\_\_  
\_\_\_\_\_

**RESTRICTION REQUEST ACCEPTANCE**

Date of Acceptance: \_\_\_\_\_ Date Patient Notified: \_\_\_\_\_

Type of PHI to be Restricted:

\_\_\_\_\_

Parties to Restrict PHI to:

\_\_\_\_\_

If request was for restriction to insurance company, did patient pay in full for the service? \_\_\_\_\_

Date of Payment: \_\_\_\_\_

**Additional Comments:**

\_\_\_\_\_

*(Keep in Patient File With Completed Patient Request for Restriction of Protected Health Information Form)*

## **ACCEPTANCE OF PATIENT REQUEST FOR RESTRICTION**

Date

City of Washington EMS  
PO Box 296  
301 C Street  
Washington, KS 66968

Name of Requestor  
Address  
City, State, Zip

Dear [INSERT NAME OF REQUESTOR]:

We have reviewed your request for a restriction of your protected health information ("PHI"). Please be advised that we have agreed to your request and we will refrain from releasing any PHI to [INSERT NAME OF HEALTH PLAN OR OTHER PARTIES TO WHOM THE SERVICE WILL NOT DISCLOSE PHI PURSUANT TO THE PATIENT'S REQUEST] regarding services that we rendered to you on [INSERT DATE OF SERVICE]. This restriction will be made part of your patient records and can only be terminated pursuant to the terms outlined in our Notice of Privacy Practices.

If you have any questions, please contact City of Washington EMS's HIPAA Compliance Officer at 785-325-2284 or [washems@washingtonks.net](mailto:washems@washingtonks.net).

Sincerely,

Caroline Scoville  
HIPAA Compliance Officer  
City of Washington EMS

**DENIAL OF PATIENT REQUEST FOR RESTRICTION**

Date

City of Washington EMS  
PO Box 296  
301 C Street  
Washington, KS 66968

Name of Requestor  
Address  
City, State, Zip

Dear [INSERT NAME OF REQUESTOR]:

We have reviewed your request for a restriction of your protected health information ("PHI"). Please be advised that we are denying your request to restrict your PHI. City of Washington EMS is not legally required to agree to your request and, given the emergent nature of our operation, we generally will not agree to a restriction unless required by law to do so.

If you disagree with our denial of your request, you have the right to file a complaint with us or with the federal government. Please contact Caroline Scoville at 785-325-2284 or washems@washingtonks.net for more information about filing a complaint with City of Washington EMS or the Office for Civil Rights. You may also request a copy of our "Procedure for Filing Complaints About Privacy Practices."

Sincerely,

Caroline Scoville  
HIPAA Compliance Officer  
City of Washington EMS



# **REQUESTS FOR ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") grants individuals the right to an accounting of disclosures of their protected health information ("PHI") from paper and electronic records. City of Washington EMS has an obligation to render an accounting to individuals in accordance with federal and state law. To ensure that City of Washington EMS complies with its obligations, this policy outlines our procedures for handling requests for an accounting and establishes the procedures by which patients or their authorized representatives may request an accounting of disclosures of PHI from City of Washington EMS.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who receive requests from patients for an accounting of disclosures of PHI. Generally, all requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all accounting requests.

## **PROCEDURE**

### *Requests for an Accounting*

1. Patients and their authorized representatives shall have a right to request an accounting of certain disclosures of PHI made by City of Washington EMS.
2. If a patient or their authorized representative requests an accounting of disclosures of PHI, the requestor shall be referred to the HIPAA Compliance Officer. The HIPAA Compliance Officer shall request that the patient or authorized representative complete City of Washington EMS's "Patient Request for Accounting of Disclosures Protected Health Information" Form.
3. The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identity of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Patient Request for Accounting of Disclosures of Protected Health Information" Form via email, mail or fax.
4. Upon receipt of the completed "Patient Request for Accounting of Disclosures of Protected Health Information" Form and verification of the requestor's identity, the HIPAA Compliance Officer will respond to a request for an accounting of disclosures within 60 calendar days of receipt of a request, preferably sooner.
5. If City of Washington EMS is unable to provide the accounting within 60 calendar days, City of Washington EMS may extend the time for responding to the request by no more than 30 calendar days, provided that within the 60 day period City of Washington EMS provides a written statement to the individual explaining

the reasons for delay and the date by which the accounting will be provided. Only one 30-day extension may be exercised per accounting request.

## **FULLFILLING AN ACCOUNTING REQUEST**

1. City of Washington EMS will provide the patient or their authorized representative with a written or electronic accounting of disclosures of their PHI made by City of Washington EMS or its business associates on City of Washington EMS's behalf, as required by HIPAA. City of Washington EMS will render an accounting of all disclosures of PHI during the period requested by the patient or other requestor. If the requestor does not specify a time period for the accounting, City of Washington EMS will render an accounting of disclosures of PHI made during the past six (6) years. The following disclosures are excluded from the HIPAA accounting requirement:
  - a. Disclosures to carry out treatment, payment or health care operations;
  - b. Disclosures made to the patient or to the patient's authorized representative;
  - c. Disclosures incident to a use or disclosure otherwise permitted or required by HIPAA;
  - d. Disclosures pursuant to the patient's authorization;
  - e. Disclosures for a facility directory or to persons involved in the patient's care;
  - f. Disclosures for national security or intelligence purposes;
  - g. Disclosures to correctional institutions or law enforcement officials to provide them with information about a person in their custody; and
  - h. Disclosure made as part of a limited data set.

City of Washington EMS will not render an accounting for disclosures that are exempt from the HIPAA accounting requirement.

2. All accountings shall include the following information regarding each disclosure of PHI addressed in the accounting:
  - a. The date of the disclosure;
  - b. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
  - c. A brief description of the PHI disclosed; and
  - d. A brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure.

## **TRACKING DISCLOSURES OF PHI**

1. In order to fulfill its obligations to render an accounting of disclosures of PHI under HIPAA, City of Washington EMS shall track all necessary disclosures of PHI. The HIPAA Compliance Officer is responsible to ensure City of Washington EMS is tracking disclosures when required by HIPAA to do so.
2. Generally City of Washington EMS shall track all disclosures for or pursuant to:
  - a. Research purposes, unless authorized by the patient;
  - b. Subpoenas, court orders or discovery requests;
  - c. Abuse and neglect reporting;
  - d. Communicable disease reporting; and
  - e. Other reports to a Department of Health.

The HIPAA Compliance Officer may utilize the "Accounting Log for Disclosures of PHI" Form for this purpose and track all information required on the Form.

#### **ADMINISTRATIVE REQUIREMENTS**

City of Washington EMS shall retain the following documentation, in either written or electronic form, for 6 years:

1. Written requests by an individual for an accounting of disclosures;
2. Accountings of disclosures that have been provided to an individual, including the titles of the persons and offices responsible for receiving and processing the request for accounting; and
3. Copies of any notices to the individual explaining that City of Washington EMS requires an extension of time to prepare the requested accounting.

**PATIENT REQUEST FOR ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION**

Patient Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Email: \_\_\_\_\_ Date of Birth: \_\_\_\_\_

*Right to Request an Accounting of Disclosures of PHI and Our Duties:*

You (or your authorized representative) have the right to receive an accounting of certain disclosures of your PHI made within six (6) years immediately preceding your request. But, we are not required to provide you with an accounting of disclosures of your PHI: (a) for purposes of treatment, payment, or healthcare operations; (b) for disclosures that you expressly authorized; (c) disclosures made to you, your family or friends; or (d) disclosures made for law enforcement or certain other governmental purposes.

*Request for an Accounting of Disclosures of PHI:*

Below, please specify the period of time for which you are requesting an accounting of disclosures of your PHI. If you do not specify a time period, City of Washington EMS will provide an accounting of disclosures during the previous six (6) years that we were required to track.

*Period of time for which I am requesting an accounting:* \_\_\_\_\_

*Signature of Requestor:* \_\_\_\_\_ *Request Date:* \_\_\_\_\_

*Requestor Information (if requestor is different from patient):*

Name: \_\_\_\_\_

Relationship to Patient (parent, legal guardian, etc.): \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

## ACCOUNTING LOG FOR DISCLOSURES OF PHI

Date of Disclosure	Patient Name	Requestor Name/Company/Title and Address	Purpose of Disclosure	PHI Disclosed (Describe)	Compliance Officer Review

# **PATIENT REQUESTS FOR CONFIDENTIAL COMMUNICATIONS OF PROTECTED HEALTH INFORMATION POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") grants individuals the right to request that City of Washington EMS send PHI to an alternate location (e.g., somewhere other than a home address), or through alternate means (e.g., by email rather than regular mail). This is called the right to "confidential communications." City of Washington EMS has an obligation to grant patients this right and it must abide by a request for confidential communications of PHI in accordance with federal and state law. To ensure that City of Washington EMS complies with its obligations, this policy outlines procedures for handling requests for confidential communications of PHI and establishes the procedures by which patients or their authorized representatives may request confidential communications.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who handle requests from patients for confidential communications of their PHI. Generally, all requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all requests for confidential communications.

## **PROCEDURE**

### *Requests for Confidential Communications*

1. City of Washington EMS will permit patients to request that City of Washington EMS send PHI to individuals at an alternate location (e.g., somewhere other than a home address), or in a specific manner (e.g., by email rather than regular mail).
2. All requests for confidential communications PHI shall be referred to the HIPAA Compliance Officer who shall request that the patient or authorized representative complete and submit City of Washington EMS's "Patient Request for Confidential Communications of Protected Health Information" Form. All requests will be reviewed and denied or approved by the HIPAA Compliance Officer in accordance with this policy. The HIPAA Compliance Officer shall utilize the "Review of Patient Request for Confidential Communications of Protected Health Information" Form when reviewing requests for confidential communications of PHI.
3. The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identify of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Patient Request for Confidential Communications of Protected Health Information" Form via email, mail or fax.
4. City of Washington EMS is required to and will agree to any "reasonable requests" for confidential communications.

### *Granting a Request for Confidential Communications*

1. City of Washington EMS will and must comply with a confidential communications request if the request is "reasonable." The HIPAA Compliance Officer shall take into account logistical reasons and other factors, such as the cost of making the alternate confidential communications, when determining whether the request is reasonable.
2. If City of Washington EMS receives a request from a patient or authorized representative asking City of Washington EMS to communicate PHI in an alternate manner and City of Washington EMS determines that the request is reasonable, it will agree to the request and the HIPAA Compliance Officer shall inform the patient of that fact, in writing, by sending an "Acceptance of Request for Confidential Communications of Protected Health Information" letter to the patient. The HIPAA Compliance Officer shall also note on the "Review of Patient Request for Confidential Communications of Protected Health Information" Form that the request was accepted and document all pertinent information regarding the request and acceptance.

### *Denying the Request for Confidential Communications*

1. If the HIPAA Compliance Officer determines, after taking into account logistical reasons and other factors, that the request is not reasonable, the HIPAA Compliance Officer shall deny the request, in writing, by dispatching a "Denial of Patient Request for Confidential Communications of PHI" letter to the patient.
2. The HIPAA Compliance Officer shall also note on the "Review of Patient Request for Confidential Communications of Protected Health Information" Form that the request was denied, and document all pertinent information regarding the request and denial.

**PATIENT REQUEST FOR CONFIDENTIAL COMMUNICATIONS OF PROTECTED HEALTH INFORMATION FORM**

Patient Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Email: \_\_\_\_\_ Date of Birth: \_\_\_\_\_

**Right to Request Confidential Communications of Your PHI and Our Duties:**

You (or your authorized representative) have the right to request that we send your PHI to an alternate location (e.g., somewhere other than your home address), or in a specific manner (e.g., by email rather than regular mail). We will only comply with reasonable requests when required by law to do so. We will notify you about our decision regarding your request by phone or email. Please provide us with appropriate contact information.

**Requested Confidential Communications:**

Below, please describe the manner in which you would like us to communicate PHI to you and specify what PHI you would like us to communicate in that manner. Specify dates that this request would apply during, and other details that will allow City of Washington EMS to accurately and completely fulfill your request.

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Signature of Requestor:** \_\_\_\_\_ **Request Date:** \_\_\_\_\_

**Contact Information to Notify You About Our Decision Regarding Your Request:**

Phone: \_\_\_\_\_ Email \_\_\_\_\_

**Requestor Information (if requestor is different from patient):**

Name: \_\_\_\_\_

Relationship to Patient (parent, legal guardian, etc.): \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_



**REVIEW OF PATIENT REQUEST FOR CONFIDENTIAL COMMUNICATIONS OF PROTECTED HEALTH INFORMATION**

**FOR CITY OF WASHINGTON EMS USE ONLY:**

(To Be Completed by City of Washington EMS HIPAA Compliance Officer after a request for confidential communications)

Patient Name: \_\_\_\_\_ Date Request Received: \_\_\_\_\_

**CONFIDENTIAL COMMUNICATIONS REQUEST DENIAL**

Date of Denial: \_\_\_\_\_ Date Patient Notified: \_\_\_\_\_

Reason for Denial:

\_\_\_\_\_  
\_\_\_\_\_

**CONFIDENTIAL COMMUNICATIONS REQUEST ACCEPTANCE**

Date of Acceptance: \_\_\_\_\_ Date Patient Notified: \_\_\_\_\_

Describe the confidential communications agreed to:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

*(Keep in Patient File With Completed Patient Request for Confidential Communications of Protected Health Information Form)*

**ACCEPTANCE OF PATIENT REQUEST FOR CONFIDENTIAL COMMUNICATIONS**

Date

City of Washington EMS  
PO Box 296  
301 C Street  
Washington, KS 66968

Name of Requestor  
Address  
City, State, Zip

Dear [INSERT NAME OF REQUESTOR]:

We have reviewed your request for a confidential communications of your protected health information ("PHI"). Please be advised that we have agreed to your request and we will abide by your request as follows: [DESCRIBE HOW CITY OF WASHINGTON EMS WILL ABIDE BY THE CONFIDENTIAL COMMUNICATIONS REQUEST].

If you have any questions, or if you want to alter this request at any time, please contact City of Washington EMS's HIPAA Compliance Officer at 785-325-2284 or washems@washingtonks.net.

Sincerely,

Caroline Scoville  
HIPAA Compliance Officer  
City of Washington EMS

## **DENIAL OF PATIENT REQUEST FOR CONFIDENTIAL COMMUNICATIONS**

Date

City of Washington EMS  
PO Box 296  
301 C Street  
Washington, KS 66968

Name of Requestor  
Address  
City, State, Zip

Dear [INSERT NAME OF REQUESTOR]:

We have reviewed your request for a confidential communications of your protected health information ("PHI"). Please be advised that we are denying your request because City of Washington EMS is not legally required to agree to your request because it is unreasonable.

**If you disagree with our denial of your request, you have the right to file a complaint with us or with the federal government. Please contact Caroline Scoville at 785-325-2284 or [washems@washingtonks.net](mailto:washems@washingtonks.net) for more information about filing a complaint with City of Washington EMS or the Office for Civil Rights. You may also request a copy of our "Procedure for Filing Complaints About Privacy Practices."**

Sincerely,

Caroline Scoville  
HIPAA Compliance Officer  
City of Washington EMS

## **ACTION PLAN: PATIENT REQUESTS RELATING TO PHI FOR HIPAA COMPLIANCE OFFICER**

<p><b>Step 1:</b> Whenever a request is made regarding a patient's PHI, the HIPAA Compliance Officer must first verify that the requestor is the patient. Or, if the requestor is not the patient, the HIPAA Compliance Officer must verify the name and identity of the requestor and verify whether the requestor has the authority to act on the patient's behalf as a personal representative. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for making this verification. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the appropriate request form via email, mail or fax.</p>	
<p><b>Step 2:</b> The HIPAA Compliance Officer will ask the requestor what type request is being made, provide the requestor with the appropriate request form, and handle the request in accordance with the appropriate policy. The general process for handling patient requests regarding PHI is outlined in this Action Plan.</p>	
<p><b>Request for Access to PHI – Request Form</b></p> <p>The HIPAA Compliance Officer shall request that the patient or authorized representative complete City of Washington EMS's "Request for Access to Protected Health Information" Form.</p>	<p><b>Request for Access to PHI – General Procedure</b></p> <p>Upon receipt of the completed "Request for Access to Protected Health Information" Form, the HIPAA Compliance Officer will act upon the access request within 30 days, preferably sooner. The HIPAA Compliance Officer will proceed to handle the request in accordance with City of Washington EMS's "Policy on Patient Requests for Access to Protected Health Information." Most access requests must be granted within 30 days.</p>
<p><b>Request for Amendment of PHI – Request Form</b></p> <p>The HIPAA Compliance Officer shall request that the patient or authorized representative complete City of Washington EMS's "Patient Request for Amendment of Protected Health Information" Form.</p>	<p><b>Request for Amendment of PHI – General Procedure</b></p> <p>Upon receipt of the completed "Patient Request for Amendment of Protected Health Information" Form, the HIPAA Compliance Officer must either grant or deny the patient's amendment request within 60 days in accordance with City of Washington EMS's "Policy on Patient Requests for Amendment of Protected Health Information." Many requests for amendment will be denied if City of Washington EMS determines that the current record that the requestor is asking City of Washington EMS to amend is true and correct.</p>
<p><b>Request for Restriction of PHI – Request Form</b></p> <p>The HIPAA Compliance Officer shall request that the patient or authorized representative complete and submit City of Washington EMS's "Patient Request for Restriction of Protected Health Information" Form.</p>	<p><b>Request for Restriction of PHI – General Procedure</b></p> <p>Upon receipt of the completed "Patient Request for Restriction of Protected Health Information" Form, the request will be reviewed and denied or approved by the HIPAA Compliance Officer in accordance with City of Washington EMS's "Policy on Patient Requests for Restriction of Protected Health Information," as soon as possible. The HIPAA Compliance Officer shall utilize City of Washington EMS's "Review of Patient Request for Restriction of Protected Health Information" Form when reviewing restriction requests. Under most circumstances, City of Washington EMS is not legally required to agree to any request to restrict the use and disclosure of PHI and City of Washington EMS generally will not agree to a restriction unless required by law to do so. City of Washington EMS is required to agree to a restriction if a patient pays City of Washington EMS in full for a service and requests that City of Washington EMS not to submit a claim to the patient's insurer for that service.</p>
<p><b>Request for Accounting of Disclosures of PHI – Request Form</b></p> <p>The HIPAA Compliance Officer shall request that the patient or authorized representative complete City of Washington EMS's "Patient Request for Accounting of Disclosures Protected Health Information" Form.</p>	<p><b>Request for Accounting of Disclosures of PHI – General Procedure</b></p> <p>Upon receipt of the completed "Patient Request for Accounting of Disclosures of Protected Health Information" Form, the HIPAA Compliance Officer will respond to a request for an accounting of disclosures within 60 calendar days of receipt of a request in accordance with City of Washington EMS's "Policy on Requests for Accounting of Disclosures of Protected Health Information." City of Washington EMS will render an accounting of certain disclosures of PHI during the period requested, or, if the requestor does not specify a time period for the accounting, City of Washington EMS will render an accounting for certain disclosures of PHI made during the past six (6) years. However, most disclosures are excluded from the HIPAA accounting requirement, including disclosures related to treatment, payment or health care operations. City of Washington EMS will not render an accounting for disclosures that are exempt from the HIPAA accounting requirement.</p>
<p><b>Requests for Confidential Communications – Request Form</b></p> <p>Individuals can request that City of Washington EMS send PHI to an alternate location (e.g., somewhere other than a home address), or through alternate means (e.g., by email rather than regular mail). This is called the right to "confidential communications." Upon receipt of a request for confidential communication of PHI, the HIPAA Compliance Officer shall request that the patient or authorized representative complete and submit City of Washington EMS's "Patient Request for Confidential Communications of Protected Health Information" Form.</p>	<p><b>Requests for Confidential Communications – General Procedure</b></p> <p>All requests for confidential communications of PHI will be reviewed and denied or approved by the HIPAA Compliance Officer in accordance with City of Washington EMS's "Policy on Patient Requests for Confidential Communications of Protected Health Information." The HIPAA Compliance Officer shall utilize the "Review of Patient Request for Confidential Communications of Protected Health Information" Form when reviewing these requests. City of Washington EMS will and must comply with a requested confidential communications request if the request is "reasonable." If City of Washington EMS agrees to the request, the HIPAA Compliance Officer shall inform the patient of that fact in writing, by sending a version of City of Washington EMS's "Acceptance of Request for Confidential Communications of Protected Health Information" letter to the patient.</p>

## **DESIGNATED RECORD SETS POLICY**

### **PURPOSE**

To ensure that City of Washington EMS patients and their authorized representatives are granted rights regarding Protected Health Information ("PHI") in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), this policy establishes what protected health information ("PHI") at City of Washington EMS should be accessible to patients as part of a Designated Record Set ("DRS"). Under HIPAA, a DRS includes medical records that are created or used by City of Washington EMS to make decisions about the patient.

### **SCOPE**

This policy applies to all City of Washington EMS staff members responsible for the designation of PHI into designated record sets and those responsible for fulfilling patient requests pertaining to PHI. All staff members should be familiar with the types of information that will be part of a DRS. Generally, the HIPAA Compliance Officer will be responsible for fulfilling patient requests related to PHI and for ensuring that the correct information is made part of the DRS.

### **PROCEDURE**

The DRS should only include PHI as defined under HIPAA, and should be comprised of individually identifiable healthcare and billing information created, received, maintained or transmitted by or on behalf of City of Washington EMS that is used, in whole or in part, by City of Washington EMS to make decisions about individuals. The HIPAA Compliance Officer shall be the party in charge of designating what information is part of a DRS at City of Washington EMS and for ensuring that appropriate information is being maintained by City of Washington EMS in its designated record sets.

#### *The Designated Record Set at City of Washington EMS*

1. The DRS at City of Washington EMS for any requests regarding PHI includes the following records:
  - a. Paper or electronic patient care reports ("PCR" or "ePCR") created or received by City of Washington EMS and supplementary information regarding the patient's condition. This includes any photos, videos, monitor strips, Physician Certification Statements, Refusal of Care forms, Consent forms, Advance Beneficiary Notice of Noncoverage forms, or information from other sources used by City of Washington EMS to treat patients or bill for services;
  - b. The electronic claims records or other paper records of submission of actual claims to Medicare or other insurance companies;
  - c. Any patient-specific claim and billing information, including responses from insurance payers, such as remittance advice statements, Explanation of Medicare Benefits (EOMBs), charge screens, patient account statements, and signature authorization and agreement to pay documents;
  - d. Notices from insurance companies indicating coverage determinations, documentation submitted by the patient, and copies of the patient's insurance card or policy coverage summary, that relate directly to the care of the patient or payment for that care;

- e. Amendments to PHI, or statements of disagreement by the patient requesting the amendment when PHI is not amended upon request, or an accurate summary of the statement of disagreement.
2. The DRS should also include treatment related records created by other parties such as first responder units, assisting ambulance services, air medical services, nursing homes, hospitals, police departments, coroner's offices, etc., that are used by City of Washington EMS for treatment and payment related purposes.
  3. A designated record set should not include:
    - a. Quality assurance data collected and maintained for peer review purposes;
    - b. Accident reports;
    - c. Incident reports;
    - d. Duplicate information maintained in other systems;
    - e. Data collected and maintained for research;
    - f. Information compiled in reasonable anticipation of litigation or administrative action;
    - g. Employment records; or
    - h. Student records.

**PATIENT AUTHORIZATION TO USE AND DISCLOSE PROTECTED HEALTH INFORMATION**

Patient Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Email: \_\_\_\_\_ Date of Birth: \_\_\_\_\_

By signing this Authorization, I hereby direct the use or disclosure by City of Washington EMS of certain protected health information (PHI) pertaining to the patient listed above. This Authorization concerns the following information about the patient:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

This information may be used or disclosed by City of Washington EMS and may be disclosed to:

\_\_\_\_\_  
\_\_\_\_\_

I understand that I have the right to revoke this Authorization at any time, except to the extent that City of Washington EMS has already acted in reliance on the Authorization. To revoke this Authorization, I understand that I must do so by written request to City of Washington EMS's HIPAA Compliance Officer:

Caroline Scoville  
PO Box 296  
301 C Street  
Washington, KS 66968  
785-325-2284  
washems@washingtonks.net

I understand that information used or disclosed pursuant to this Authorization may be subject to redisclosure by the recipient and no longer subject to privacy protections provided by law.

I understand that my written authorization is not required for City of Washington EMS to use my protected health information for treatment, payment and healthcare operations.

I understand that I have the right to inspect and copy the information that is to be used or disclosed as part of this Authorization. The Authorization is being requested by City of Washington EMS for the following purpose(s):

\_\_\_\_\_  
\_\_\_\_\_

The use or disclosure of the requested information will \_\_\_/will not \_\_\_ result in direct or indirect remuneration to City of Washington EMS from a third party.

I acknowledge that I have read the provisions in the Authorization and that I have the right to refuse to sign this Authorization. I understand and agree to its terms.

This authorization expires on: \_\_\_\_\_ (date or event).

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

*Personal Representative Information (if signer is different from patient):*

Name: \_\_\_\_\_

Relationship to Patient (parent, legal guardian, etc.): \_\_\_\_\_

Description of the authority of personal representative:

\_\_\_\_\_  
\_\_\_\_\_

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_



## **PROCEDURE FOR FILING COMPLAINTS ABOUT PRIVACY PRACTICES**

### **YOU MAY MAKE A COMPLAINT DIRECTLY TO CITY OF WASHINGTON EMS**

You have the right to make a complaint directly to the HIPAA Compliance Officer of City of Washington EMS concerning our compliance with any of our established HIPAA policies and procedures, uses or disclosures of your PHI, or about our compliance with HIPAA.

All complaints should be directed to our HIPAA Compliance Officer at the following address, phone number, or email:

City of Washington EMS  
Attn: Caroline Scoville  
PO Box 296  
301 C Street  
Washington, KS 66968  
785-325-2284  
washems@washingtonks.net

### **YOU MAY ALSO MAKE A COMPLAINT TO THE GOVERNMENT**

The Office for Civil Rights ("OCR") enforces HIPAA. If you believe that we are not complying with the applicable requirements of HIPAA, you may file a complaint with OCR. Complaints to OCR must:

- Be filed in writing, either on paper or electronically, by mail, fax, or e-mail;
- Name the covered entity involved and describe the acts or omissions you believe violated the requirements of HIPAA; and
- Be filed within 180 days of when you knew that the act or omission complained of occurred, unless OCR extends the 180-day period for "good cause."

**FOR MORE INFORMATION, GO TO OCR'S WEBSITE AT: [HTTP://WWW.HHS.GOV/OCR/](http://www.hhs.gov/ocr/).**

# LOG FOR PROCESSING COMPLAINTS ABOUT PRIVACY PRACTICES

(To be completed by HIPAA Compliance Officer)

Date Received	Complainant Name	Description of Complaint	Disposition of Complaint

# **USE OF COMPUTER AND INFORMATION SYSTEMS AND EQUIPMENT POLICY**

## **PURPOSE**

The City of Washington EMS is committed to protecting our staff members, the patients we serve and the company from illegal or damaging actions by individuals and the improper release of protected health information and other confidential or proprietary information.

The purpose of this policy is to outline the acceptable use of computer equipment at the City of Washington EMS. These rules are in place to protect the employee and patients of the City of Washington EMS. Inappropriate use exposes the City of Washington EMS to risks including virus attacks, compromise of network systems and services, breach of patient confidentiality and other legal claims.

## **SCOPE**

This policy applies to employees, volunteers, contractors, consultants, temporary employees, students, and others at the City of Washington EMS who have access to computer equipment, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City of Washington EMS.

## **PROCEDURE**

### *Use and Ownership of Computer Equipment*

1. All data created or recorded using any computer equipment owned, controlled or used for the benefit of the City of Washington EMS is at all times the property of the City of Washington EMS. Because of the need to protect the City of Washington EMS computer network, the company cannot guarantee the confidentiality of information stored on any network device belonging to the City of Washington EMS, except that it will take all steps necessary to secure the privacy of all protected health information in accordance with all applicable laws.
2. Staff members are responsible for exercising good judgment regarding the reasonableness of personal use and must follow operational guidelines for personal use of Internet/Intranet/Extranet systems and any computer equipment.
3. At no time may any pornographic or sexually offensive materials be viewed, downloaded, saved, or forwarded using any Company computer equipment.
4. For security and network maintenance purposes, authorized individuals within the City of Washington EMS may monitor equipment, systems and network traffic at any time, to ensure compliance with all Company policies.

### *Security and Proprietary Information*

1. Confidential information should be protected at all times, regardless of the medium by which it is stored. Examples of confidential information include but are not limited to: individually identifiable health information concerning patients, company financial and business information, patient lists and reports, and research data. Staff members should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, and user level passwords should be changed every 30 days.
3. All PCs, laptops, workstations and remote devices should be secured with a password-protected screensaver, wherever possible, and set to deactivate after being left unattended for 10 minutes or more, or by logging-off when the equipment will be unattended for an extended period.
4. All computer equipment used by staff, whether owned by the individual staff member or City of Washington EMS, shall regularly run approved virus-scanning software with a current virus database.
5. Staff members must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.

#### *Unacceptable Use*

Under no circumstances is a staff member of the City of Washington EMS authorized to engage in any activity that is illegal under local, state, or federal law while utilizing City of Washington EMS computer resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

#### *System and Network Activities*

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Washington.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City of Washington or the end user does not have an active license is strictly prohibited.
3. Exporting system or other computer software is strictly prohibited and may only be done with express permission of management.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a City of Washington EMS computer device to actively engage in procuring or transmitting material that is in violation of the Company's prohibition on sexual and other harassment.

7. Making fraudulent statements or transmitting fraudulent information when dealing with patient or billing information and documentation, accounts or other patient information, including the facsimile or electronic transmission of patient care reports and billing reports and claims.
8. Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the staff member is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
9. Providing information about, or lists of, the City of Washington EMS staff members or patients to parties outside the City of Washington EMS.

*E-mail and Communications Activities*

1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
2. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of e-mail header information.
4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited e-mail originating from within the City of Washington's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by City of Washington or connected via City of Washington's network.

*Use of Remote Devices*

The appropriate use of Laptop Computers, Personal Digital Assistants (PDAs), and remote data entry devices is of utmost concern to City of Washington EMS. These devices collectively referred to as "remote devices" pose a unique and significant patient privacy risk because they may contain confidential patient, staff member or company information and these devices can be easily misplaced, lost, stolen or accessed by unauthorized individuals.

1. Remote devices will not be purchased or used without prior Company approval.
2. The Company must approve the installation and use of any software used on the remote device.
3. Remote devices containing confidential or patient information must not be left unattended.
4. If confidential or patient information is stored on a remote device, access controls must be employed to protect improper access. This includes, where possible, the use of passwords and other security mechanisms.
5. Remote devices should be configured to automatically power off following a maximum of 10 minutes of inactivity.

6. Remote device users will not permit anyone else, including but not limited to user's family and/or associates, patients, patient families, or unauthorized staff members, to use company-owned remote devices for any purpose.
7. Remote device users will not install any software onto any PDA owned by City of Washington EMS except as authorized by the Company.
8. Users of company-owned remote devices will immediately report the loss of a remote device to a supervisor or the HIPAA Compliance Officer.

*Enforcement*

Any staff members found to have violated this policy may be subject to disciplinary action, up to and including suspension and termination.

## **RELEASING PHI TO FAMILY MEMBERS AND OTHERS POLICY**

### **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") permits City of Washington EMS to release protected health information ("PHI") about patients to family members, friends and others involved in the treatment of the patient or payment for that treatment. This policy outlines our procedures for releasing PHI to family members and others involved in our patients' care.

### **SCOPE**

This policy applies to all City of Washington EMS staff members who receive requests from family members, friends and others for PHI of patients of City of Washington EMS. This policy does not apply to formal requests from patients or their personal representatives for: access to PHI; amendment of PHI; restriction of PHI; accounting of disclosures of PHI; or confidential communications. This policy shall apply to requests for PHI from family members of the patient or others who do not qualify as the patient's personal representative, but who are involved in the patient's care or payment for that care.

### **PROCEDURE**

#### *General Procedure for Releasing PHI to Family Members and Others*

1. HIPAA permits City of Washington EMS staff members to release PHI that is directly relevant to the patient's care or payment for care to family members, friends and others involved in a patient's care, or payment for that care, whenever releasing PHI to that individual would be in the best interest of a patient. City of Washington EMS may also use or disclose PHI to notify family members or others about a patient's location, general condition, or death.
2. If an individual other than the patient or the patient's personal representative makes a request for PHI from a City of Washington EMS staff member, the staff member shall first determine whether the patient about whom the request pertains to is present, competent and able to make healthcare decisions.
3. If the patient is present, competent and able to make healthcare decisions, the staff member should obtain the patient's agreement to share the requested PHI with the individual, or give the patient an opportunity to object. The staff member may ask the patient whether it is okay to talk to the individual and release PHI to them. Or, the staff member can simply infer from the circumstances that the patient does not object to sharing the information with the individual. For example, if the patient's neighbor asks to ride along in the ambulance and the patient smiles, the staff member could infer that the patient is fine with the neighbor riding along and overhearing any PHI that is discussed. Or, if the staff member starts asking the patient about his or her medical history and the patient motions for a family member to come over, the staff member can infer that the patient wants the staff member to speak with the family member about his or her medical history.
4. If the patient is unavailable or unable to make medical decisions because of a physical or mental reason at the time of the request, then the staff member may only disclose PHI to the requestor if the requestor is involved with the patient's treatment or payment for the patient's treatment and the staff member believes that releasing PHI to the requestor is in the best interests of the patient. First, the staff member should ask the requestor what his or her relationship is to the patient. Then, the staff member should determine whether disclosure of

PHI to the requestor would be in the best interest of the patient. In making this determination, the staff member should consider things such as:

- a. Who the requestor is and what the requestor's relationship is to the patient;
  - b. Whether the requestor appears to have a legitimate interest in the patient's care or payment for that care;
  - c. Whether the staff member believes that the patient would want that requestor to know the PHI or whether the patient would benefit from the requestor knowing the PHI.
5. If the patient is deceased, a staff member may release relevant PHI to family members and others who were involved in the deceased patient's care prior to death or payment for care, unless doing so would be inconsistent with any prior expressed preference of the patient. The staff member should only disclose PHI that is relevant to the requestor's involvement with the patient's care prior to death or payment for that care.



# **RELEASE OF PROTECTED HEALTH INFORMATION PURSUANT TO LEGAL PROCESS POLICY**

## **PURPOSE**

Protected health information ("PHI") may be released pursuant to valid legal process under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This policy provides guidelines for City of Washington EMS regarding the release of PHI pursuant to court orders, summonses, subpoenas, warrants, administrative requests, and discovery requests (collectively referred to in this policy as "legal process"), so that City of Washington EMS only releases PHI in accordance with HIPAA and as required by state law. This policy will work in conjunction with City of Washington EMS's HIPAA Compliance Officer Action Plans on "Requests for PHI from Attorneys," "Administrative Requests for PHI from Government Agencies," and "Court-Ordered Requests for PHI."

## **SCOPE**

This policy applies to all City of Washington EMS staff members who may receive or respond to requests for PHI accompanied by legal process. These requests typically occur after a call is completed and are generally served on staff at City of Washington EMS's station in person or through the mail. Generally, all such requests will be directed to and handled by the HIPAA Compliance Officer.

## **PROCEDURE**

### *General Procedure for Handling Requests*

1. City of Washington EMS is permitted by HIPAA, and may be required by Kansas law and federal law, to furnish requested PHI to certain parties pursuant to a valid legal process.
2. If City of Washington EMS receives a request for PHI accompanied by legal process, the request shall be directed to the HIPAA Compliance Officer.
3. The HIPAA Compliance Officer shall first determine whether the request is: (a) a court order or a court-ordered subpoena, summons or warrant ("SSW"); (b) an administrative request; or (c) a subpoena, discovery request, or other legal process issued by an attorney. When determining what type of request has been received, the HIPAA Compliance Officer shall look to the issuer of the request (*i.e.*, who the requesting party is) and keep in mind the following guidelines:
  - a. Court orders and court-ordered SSWs are issued by courts, grand juries, and administrative tribunals and signed by a judge or other judicial officer.
  - b. Administrative requests are issued by a federal, state, or local administrative agency such as a department of health, a law enforcement agency, or other similar type of agency. Administrative agencies are permitted to issue "administrative" warrants, subpoenas, summonses or other similar type requests for information. These documents are likely to be signed by a high level official from the requesting administrative agency.
  - c. Attorneys may issue subpoenas and discovery requests. These requests can usually be distinguished from other types of "official" court-ordered or administrative requests because they are signed by an attorney, not a judge, judicial officer or administrative official.

When in doubt, the HIPAA Compliance Officer should solicit the assistance of legal counsel in determining what type of request was received.

4. Patient authorization is not required when releasing PHI pursuant to a request for PHI accompanied by legal process. However, patients may need to be notified about certain requests in accordance with this policy before PHI is released.
5. All disclosures of PHI pursuant to requests accompanied by legal process must be documented by the HIPAA Compliance Officer in City of Washington EMS's "Accounting Log for Disclosures of PHI" and a copy of the request shall be maintained with that log in the patient file, along with other information required by this policy.

#### *Responding to Court-Ordered Requests*

1. If the HIPAA Compliance Officer determines that the request is a court order or a court-ordered SSW, the HIPAA Compliance Officer shall first verify that the request has been signed by a judge or other judicial officer of a court, grand jury, or administrative tribunal. If the request has not been signed by a judge or judicial officer, the HIPAA Compliance Officer shall send the requestor a letter stating that City of Washington EMS will not disclose any PHI until City of Washington EMS receives a court order or court-ordered SSW that is signed by the appropriate party.
2. If the request is signed by a judge or judicial officer, City of Washington EMS may disclose ONLY the information that is specifically requested by the court order or court-ordered SSW. For example, the HIPAA Compliance Officer should not simply turn over a copy of all records (including records relating to prior transports and billing records) if the request asks City of Washington EMS to "provide any treatment records about John Smith from April 15, 2013." However, if the request asks City of Washington EMS to provide "any and all records pertaining to John Smith," then City of Washington EMS must generally provide all PCR's, all billing records, and any other information maintained about the patient. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI City of Washington EMS is required to disclose. If necessary, the HIPAA Compliance Officer shall ask that the requester re-issue a more specific request.
3. The HIPAA Compliance Officer shall retain a copy of the court-ordered request and document the name of the requesting party, the date of the request, the date of disclosure, and the PHI that was disclosed.

#### *Responding to Administrative Requests from Government Agencies*

1. If the HIPAA Compliance Officer determines that a request for PHI qualifies as an administrative request (including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process) issued by a federal, state, or local government agency, the HIPAA Compliance Officer should first determine whether the agency has the authority to make the request and to receive the PHI requested. The HIPAA Compliance Officer should look to any statutory or regulatory authority cited in the request and consult with legal counsel when making this determination. If the HIPAA Compliance Officer determines that the agency does not have the legal authority to request and receive the PHI requested, the HIPAA Compliance Officer shall send the requestor a letter stating that City of Washington EMS will not disclose any PHI until the agency provides City of Washington EMS with a statement citing appropriate legal authority to request and receive the PHI requested.

2. If the HIPAA Compliance Officer determines that the agency is authorized by law to make the request, the HIPAA Compliance Officer must then verify that:
  - a. The PHI sought by the request is relevant and material to a legitimate law enforcement inquiry;
  - b. The request is specific and limited in scope to the extent reasonable and practicable in light of the purpose for which the PHI is sought; and
  - c. De-identified information could not reasonably be used.

The HIPAA Compliance Officer should look to the administrative request to determine whether these conditions are clearly met. If it is not clear from the administrative request that all three of the above-listed conditions are met, then the HIPAA Compliance Officer shall contact the administrative agency who issued the request and inform the agency that PHI will not be released until City of Washington EMS receives written assurances from the requestor that the conditions are met.

3. If the HIPAA Compliance Officer determines that the above-listed conditions are met, the HIPAA Compliance Officer may release ONLY the PHI that the administrative request asks for. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI City of Washington EMS is required to disclose. If necessary, the HIPAA Compliance Officer shall ask that the requester re-issue a more specific request.
4. The HIPAA Compliance Officer shall retain a copy of the administrative request as well as any assurances, and document: the name of requesting party; the date of the request; the date of disclosure; and the PHI that was disclosed.

#### *Responding to Requests from Attorneys*

1. If the HIPAA Compliance Officer determines that the request is a subpoena, discovery request, or other legal process from an attorney (that is not accompanied by an official order from a court, grand jury or administrative tribunal), the HIPAA Compliance Officer shall first verify that the original subpoena, discovery request, or other legal process is enclosed with the request. References to a subpoena or other document in the request are not sufficient. If the original legal process has not been provided to City of Washington EMS, the HIPAA Compliance Officer shall send the requestor a letter stating that City of Washington EMS will not disclose any PHI until the original process has been provided.
2. Then, the HIPAA Compliance Officer shall verify that "satisfactory written assurances" have been provided to City of Washington EMS by the requestor. This means that City of Washington EMS must receive written documentation from the attorney requesting the PHI that demonstrates either of the following:
  - a. The attorney requesting the PHI made a good faith attempt to provide written notice to the patient that included information about the litigation or proceeding and the PHI request and such notice was sufficient to permit the individual the opportunity to raise an objection to the court or administrative tribunal. Additionally, the time for the patient to raise objections to the court or administrative tribunal has elapsed, and either: (i) no objections were filed; or (ii) all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution. Documentation may include, for example, a copy of the notice mailed to the individual that includes instructions for raising an objection with the court and the deadline for doing so, and a written statement or

other documentation demonstrating that no objections were raised or all objections raised were resolved and the request is consistent with the resolution. To the extent that the subpoena or other request itself demonstrates the above elements, no additional documentation is required;

OR

- b. The parties to the dispute giving rise to the request for PHI have agreed to a "qualified protective order" and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or the attorney seeking the PHI has requested a qualified protective order from such court or administrative tribunal. A "qualified protective order" is an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (i) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and (ii) requires the return of the PHI or destruction of the PHI (including all copies made) at the end of the litigation or proceeding. Documentation may include, for example, a copy of the qualified protective order that the parties have agreed to and documentation or a statement that the order was presented to the court, or a copy of the motion to the court requesting a qualified protective order.

If all written assurances have not been provided to City of Washington EMS, the HIPAA Compliance Officer shall send the requestor a letter stating that City of Washington EMS will not disclose any PHI until the proper written assurances have been provided.

3. If the required satisfactory written assurances have been provided to City of Washington EMS, then the HIPAA Compliance Officer may disclose PHI as requested in the subpoena or other legal process. The HIPAA Compliance Officer shall ONLY disclose the PHI that has been requested in the document. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI City of Washington EMS is required to disclose. If necessary, the HIPAA Compliance Officer shall ask that the requester re-issue a more specific request.
4. The HIPAA Compliance Officer shall retain a copy of the request from the attorney as well as the satisfactory written assurances from the attorney in the patient file. The HIPAA Compliance Officer shall also document the name of requesting party, the date of the request, the date of disclosure, and the PHI that was disclosed.

# **RELEASE OF PROTECTED HEALTH INFORMATION TO LAW ENFORCEMENT WITHOUT LEGAL PROCESS POLICY**

## **PURPOSE**

Protected health information ("PHI") may only be released to law enforcement officials under specific and limited circumstances under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This policy provides consistent guidelines for City of Washington EMS staff members to follow regarding the release of PHI to law enforcement when the law enforcement official does not serve some type of legal process, such as a summons, subpoena, or warrant, so that staff only release PHI in accordance with HIPAA. This policy will work in conjunction with City of Washington EMS's "Staff Member Action Plan for Release of PHI to Law Enforcement Without Legal Process."

## **SCOPE**

This policy applies to all City of Washington EMS staff members who may come in contact with law enforcement including field personnel who may encounter law enforcement officials at the scene of an incident and other staff who may be approached by law enforcement directly after an incident. This policy applies to situations where law enforcement is seeking PHI from a staff member and the law enforcement official does not present City of Washington EMS with legal process, such as a subpoena, summons or warrant. City of Washington EMS's Policy on Release of Protected Information Pursuant to Warrant, Subpoena, Summons or Administrative Request applies to situations where law enforcement or other parties are seeking information pursuant to legal process.

## **PROCEDURE**

### *General Procedure for Handling Requests*

1. If a staff member of City of Washington EMS is approached by a law enforcement official and the official makes requests a request for PHI about a patient from the staff member, the staff member should verify the identity of the law enforcement official and ask the official what is the purpose for which the request is being made.
2. If the request is being made for one of the purposes listed in this policy, then the staff member may release the PHI to the law enforcement official, in accordance with this policy. Formal written patient authorization is not required when releasing PHI pursuant to one of the purposes listed in this policy; however, where the patient is readily available and able to consent to the disclosure, verbal consent should be obtained and documented by the staff member before disclosure of PHI is made to the law enforcement official.
3. If the staff member is unsure about whether the release of PHI is proper, the staff member should contact City of Washington EMS's HIPAA Compliance Officer or an immediate supervisor for guidance. Under no circumstance should any staff member release PHI to law enforcement if the staff member is unsure about the appropriateness of the disclosure.
4. If the request for PHI does not fall under one of the purposes listed in this policy, the staff member should inform the law enforcement officer that s/he is not permitted under HIPAA to release the information. The staff member may inform the law enforcement official of the following two options:
  - a. The law enforcement official may obtain legal process, such as a warrant, summons, or subpoena, to obtain the information from City of Washington EMS.

- b. The law enforcement official may obtain the information directly from the patient if the patient is stable and willing to speak with the official. Staff members should only provide this option to a law enforcement official when doing so would not impede patient care and where the patient is willing to speak with the official. For a stable patient, the staff member should first consult with the patient to determine whether the patient is willing to speak with the official. If the patient declines to speak with the official, the staff member should inform the enforcement official.
5. Staff members should record, at a minimum, the following information about all law enforcement requests that are unaccompanied by legal process:
    - a. The name of the law enforcement official;
    - b. The date and time of the request;
    - c. The purposes for which the request was made (if provided);
    - d. What information the law enforcement official requested;
    - e. Whether the patient was consulted about the request and the patient's response;
    - f. Whether the HIPAA Compliance Officer or other individual at City of Washington EMS was consulted about the request;
    - g. Whether the law enforcement official made any representations to City of Washington EMS;
    - h. Whether PHI was released and what PHI was released; and
    - i. The reason(s) why the PHI was released.

## **PURPOSES FOR WHICH DISCLOSURE CAN BE MADE TO LAW ENFORCEMENT WITHOUT LEGAL PROCESS**

### *Disclosures of PHI Required by State Reporting Law*

1. Kansas law requires that City of Washington EMS staff members report the following types of incidents to law enforcement agencies in Kansas: PER KANSAS BOARD OF EMS, EMERGENCY MEDICAL SERVICES IN KANSAS HAVE NO REGULATORY REQUIREMENT FOR REPORTING TO LAW ENFORCEMENT AGENCIES.
2. If there is any doubt regarding whether or not Kansas requires reporting of a particular injury or incident, the staff member should contact a supervisor for a list of incidents that must reported under Kansas law.

### *Disclosures of PHI to Locate or Identify a Suspect, Material Witness, Fugitive or Missing Person*

1. PHI may be disclosed to law enforcement for purpose of locating or identifying a **suspect, material witness, fugitive** or **missing person** only upon request of a law enforcement official. The disclosure may not be initiated by City of Washington EMS.
2. If a law enforcement official indicates to a staff member that they need PHI about an individual to identify or locate a **suspect, material witness, fugitive** or **missing person**, the staff member should ask the law enforcement official to confirm that the *sole* purpose of the request is to locate or identify one of the listed individuals. If the law enforcement official already knows who the individual is and where the individual is located, then the staff member should not proceed to disclose PHI for this purpose.

3. Although no formal written request is required from law enforcement, the staff member should ask that the PHI request be documented in writing, preferably on the law enforcement department's letterhead. In the absence of a written request from the law enforcement agency, the staff member should, at a minimum, document that the law enforcement officer verified that the PHI was needed to identify or locate a **suspect, material witness, fugitive** or **missing person**.
4. If the staff member is satisfied that law enforcement has made a good faith representation that the information requested is needed to locate or identify a **suspect, fugitive, material witness, or missing person**, then the staff member may disclose only the following PHI about that individual to the official:
  - Name
  - Address
  - Date of birth
  - Place of birth
  - Social Security Number
  - Blood type
  - Type of injury
  - Date of treatment
  - Time of treatment
  - Description of distinguishing physical characteristics (i.e. weight, hair color, eye color, gender, facial hair, scars and tattoos).

#### *Disclosing PHI About Crime Victims*

1. PHI about crime victims may be disclosed to law enforcement only upon request of a law enforcement official. The disclosure may not be initiated by City of Washington EMS.
2. If a law enforcement officer requests PHI about an individual who may be the victim of a crime, City of Washington EMS staff members should first discern whether the individual is in fact a victim of a crime. Victims of a crime may include motor accident victims because often a summary or misdemeanor offense is involved (like when the accident is the result of the driver of another vehicle violating traffic laws). In many cases, the determination that a patient is or may be a crime victim can be inferred from the circumstances and the presence of law enforcement at the scene.
3. City of Washington EMS may disclose PHI about a crime victim to a law enforcement official if the individual agrees to the disclosure. If the patient is conscious and alert, and it would not impede the provision of care, the staff member should ask the patient if it is acceptable to disclose the PHI to law enforcement. If the patient does not consent to the disclosure, then PHI should not be disclosed and law enforcement should be informed of that fact. If the victim does consent to the disclosure, the PHI may be released in accordance with the patient's wishes. The consent may be verbal, but it should be documented on a patient care report or other document.
4. If the patient is unable to consent, due to incapacity or other reason, the staff member should ask law enforcement if they can wait until the patient is able to consent to the release of the PHI. If the law enforcement official represents that waiting until the patient is capable of agreeing to the disclosure would compromise an immediate law enforcement activity, then PHI may be disclosed to law enforcement provided the following conditions are met:



- a. The staff member, in the exercise of professional judgment, determines that disclosure would be in the best interests of the crime victim;
- b. The law enforcement officer needs the information to determine whether a violation of law has occurred; and
- c. The law enforcement officer represents that the information requested is not intended to be used against the crime victim.
- d. Representations from law enforcement may be verbal and should be documented in a patient care report or other document.

*Disclosing PHI Regarding Victims of Abuse, Neglect, or Domestic Violence*

1. If law enforcement makes a request for PHI regarding someone who a City of Washington EMS staff member reasonably believes to be the victim of violence or abuse, City of Washington EMS may release PHI to law enforcement if the patient agrees to the disclosures. The staff member should first ask the patient for his/her consent to release the information. If the patient does not consent to the disclosure, no PHI should be provided to law enforcement and law enforcement should be informed of this fact. If the individual agrees to the disclosure of PHI, the staff member may give the PHI to law enforcement in accordance with the patient's consent. This consent can be verbal but it should be documented on the patient care report.
2. If the individual is unable to consent to the disclosures due to incapacity, mental condition, etc., and the laws of Kansas expressly authorize reporting of this type of information to law enforcement, City of Washington EMS staff members may release PHI to law enforcement provided that either of the following conditions are met:
  - a. The staff member, in the exercise of professional judgment, believes that the disclosure is necessary to prevent serious harm to the patient or other potential victims; or
  - b. Law enforcement assures the staff member that the PHI will not be used against the victim and represents that an immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
3. Representations from law enforcement may be verbal and should be documented in a patient care report by the staff member along with all details regarding the disclosure including the identity of the requestor, the purpose of the request, the date and time of the request, and the PHI released about the victim.
4. If City of Washington EMS discloses PHI without the patient's consent because the patient was unable to consent, the HIPAA Compliance Officer must contact the patient and alert them of the disclosure, unless City of Washington EMS believes contacting the patient will only put the patient at greater risk.

*Disclosing PHI Regarding Decedents*

1. PHI can be released to law enforcement about decedents without a request for PHI from a law enforcement official (*i.e.*, City of Washington EMS may initiate this type of disclosure).
2. City of Washington EMS staff members may disclose limited PHI to law enforcement about an individual who has died when staff members have a reasonable, good faith belief that the death may have resulted from



criminal conduct. The staff member does not necessarily have to come to a legal conclusion, or know with complete certainty, that the death resulted from a crime. This includes any type of crime.

3. Disclosure regarding suspected victims of a crime should be limited to basic facts about the victim and the circumstances of the death.

#### *Disclosing PHI to Report a Crime on City of Washington EMS's Premises*

1. City of Washington EMS may initiate this type of disclosure to law enforcement absent a request from a law enforcement official.
2. City of Washington EMS staff members may disclose to law enforcement any PHI that staff members in good faith believe constitutes evidence of a crime committed on City of Washington EMS's premises. City of Washington EMS's premises include the station house, headquarters, parking lot, the ambulance, etc.
3. Disclosure of PHI to report a crime on the premises should be limited to information that is necessary to alert law enforcement about the crime and to describe the crime to law enforcement.

#### *Disclosing PHI to Report a Crime in an Emergency*

1. City of Washington EMS may initiate this type of disclosure to law enforcement absent a request from a law enforcement official.
2. City of Washington EMS staff members may disclose PHI to law enforcement when they believe it is necessary to alert law enforcement to:
  - The commission of a crime
  - The nature of a crime
  - The location of the crime
  - The location of a crime victim
  - The identity, description, and location of the perpetrator of a crime
3. Disclosures of PHI to report a crime in an emergency should be limited to necessary information about the nature of the crime and information about the suspect(s).

#### *Disclosure of PHI to Avert a Serious Threat to Health or Safety*

1. City of Washington EMS may initiate this type of disclosure to law enforcement absent a request from a law enforcement official.
2. City of Washington EMS staff members may disclose PHI to avert a serious threat to health or safety so long as a staff member believes that the disclosure is necessary to:
  - a. Avert a serious and imminent threat to a person's safety or the public at large;
  - b. Identify or apprehend an individual because that individual admitted to participating in a violent crime that may have caused serious harm to someone; or

- c. Identify or apprehend someone who escaped from a correctional institution or from lawful custody.
- 3. Disclosures of PHI to prevent or lessen a serious and imminent threat to the health or safety should only be made to alert persons who are reasonably able to prevent or lessen the threat.
- 4. Disclosures of PHI to prevent or lessen a serious threat to health or safety should be limited to necessary information to prevent or lessen the threat, and necessary information about the individual who poses the threat.

## ACTION PLAN: RELEASE OF PHI TO LAW ENFORCEMENT WITHOUT LEGAL PROCESS

**Step 1:** If the request comes from law enforcement, verify the identity of the law enforcement official and ask the official what is the purpose for which the request is being made.

<p><b>Step 2:</b> Is the law enforcement officer requesting information for one of the law enforcement purposes listed in this action plan?</p>	<p style="text-align: center;">NO</p> <p style="text-align: center;">Go to Step 3</p>	<p style="text-align: center;">YES</p> <p>You may release the PHI in accordance with the corresponding guidance for each purpose, listed in the column directly across from the stated purpose. Formal written patient authorization is not required when releasing PHI pursuant to one of the purposes listed in this policy. But, if the patient is readily available and able to consent to the disclosure, verbal consent should be obtained and documented before disclosure of PHI is made to the law enforcement official. In addition, you should record, at a minimum, the following information about all law enforcement requests that are unaccompanied by legal process:</p> <ul style="list-style-type: none"> <li>• The name of the law enforcement official;</li> <li>• The date and time of the request;</li> <li>• The purposes for which the request was made (if provided);</li> <li>• What information the law enforcement official requested;</li> <li>• Whether the patient was consulted about the request and the patient's response;</li> <li>• Whether the HIPAA Compliance Officer or other individual at City of Washington EMS was consulted about the request;</li> <li>• Whether the law enforcement official made any representations to City of Washington EMS;</li> <li>• Whether PHI was released and what PHI was released; and</li> <li>• The reason(s) why the PHI was released.</li> </ul>
<p style="text-align: center;">Required by State Reporting Law</p> <p>The information that the law enforcement officer is asking for is required to be reported to law enforcement under state law (e.g., animal bites, gunshot wounds, burn injuries, out-of hospital deaths, vehicle accidents, etc.).</p>		<p style="text-align: center;">Required by State Reporting Law</p> <p>You may release any PHI that is necessary to comply with state reporting law and should track the disclosure on a patient care report or other form and inform the patient about the disclosure, whenever possible.</p>
<p>Identify or Locate a Suspect, Material Witness, Fugitive, or Missing Person</p> <p>The information is needed by law enforcement for the sole purpose of identifying or locating a suspect,</p>		<p>Identify or Locate a Suspect, Material Witness, Fugitive, or Missing Person</p> <p>You may release <u>only</u> the following types of PHI about the individual to law enforcement:  <i>Name; Address; Date of Birth; Place of Birth; Social Security Number; Blood Type; Type of Injury; Date of Treatment; Time of Treatment; A Description of</i></p>

<p>material witness, fugitive, or missing person.</p>	<p><i>Distinguishing Physical Characteristics.</i></p>
<p align="center"><b>Crime Victims</b></p> <p>The information is needed by law enforcement about a person who is or who is suspected by the law enforcement officer to be the victim of a crime.</p>	<p align="center"><b>Crime Victims</b></p> <p>You should first ask whether the victim agrees to the disclosure and if the victim refuses, the PHI should not be released and the officer should be informed that s/he may speak with the victim directly. If the patient agrees, information may be disclosed pursuant to the patient's wishes and the agreement should be documented along with the disclosure. If the patient is unable to agree to the disclosure because he/she is incapacitated or some other reason and the law enforcement official represents that waiting until the patient is capable of agreeing to the disclosure would compromise an immediate law enforcement activity, then you may release the PHI requested provided all the following conditions are met:</p> <ul style="list-style-type: none"> <li>• You determine that disclosure would be in the best interests of the victim;</li> <li>• The officer needs the information to determine whether a violation of law has occurred; and</li> <li>• The law enforcement officer represents that the information requested is not intended to be used against the crime victim and you document that representation.</li> </ul>
<p align="center"><b>Death from Criminal Activity</b></p> <p>You need to disclose PHI to law enforcement regarding a decedent because it appears that the decedent died as a result of criminal conduct.</p>	<p align="center"><b>Death from Criminal Activity</b></p> <p>You must first have a reasonable, good faith belief that that the individual's death resulted from criminal conduct. This does not require a legal conclusion and the death may have been the result of any criminal conduct. You should only release information that is necessary to alert law enforcement about the death, such as the identity of the patient and basic facts about the circumstances of the death.</p>
<p align="center"><b>Crime on Premises</b></p> <p>You need to disclose PHI to report a crime that occurred on the premises of City of Washington EMS or in one of our vehicles.</p>	<p align="center"><b>Crime on Premises</b></p> <p>You may disclose PHI to law enforcement if you believe in good faith the PHI constitutes evidence of criminal conduct on the premises of City of Washington EMS's station house, headquarters, parking lot, or any vehicle. The information should be limited to basic information about the patient and circumstances about the crime.</p>
<p align="center"><b>Reporting Crime in Emergency</b></p> <p>You need to disclose PHI to report a crime in an emergency.</p>	<p align="center"><b>Reporting Crime in Emergency</b></p> <p>You may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:</p> <ul style="list-style-type: none"> <li>• The commission and nature of a crime;</li> <li>• The location of the crime; and</li> <li>• The identity, description, and location of the perpetrator of such crime.</li> </ul>
<p align="center"><b>To Avert a Serious Threat to Health or Safety</b></p>	<p align="center"><b>To Avert a Serious Threat to Health or Safety</b></p> <p>You may disclose PHI to someone who is able to prevent or lessen a threat to</p>



You need to disclose PHI to someone who is able to prevent or lessen a serious threat to health or safety.

health or safety if you believe it is necessary to do so in order to:

- Avert a serious and imminent threat to a person's safety or the public at large;
- Identify or apprehend an individual because that individual admitted to participating in a violent crime that may have caused serious harm to someone; or
- Identify or apprehend someone who escaped from a correctional institution or from lawful custody.

Disclosures of PHI to prevent or lessen a serious threat to health or safety should be limited to necessary information to prevent or lessen the threat, and necessary information about the individual who poses the threat.

Step 3:

If the request for PHI does not fall under one of the purposes listed in this action plan, you should inform the law enforcement official you are not permitted under HIPAA to release the information. You may inform the law enforcement official of the following two options:

- The law enforcement official may obtain legal process, such as a warrant, summons, subpoena or administrative request to obtain the information from City of Washington EMS.
- The law enforcement official may obtain the information directly from the patient if the patient is stable and willing to speak with the official. You should only provide this option to a law enforcement official when doing so would not impede patient care and where the patient is willing to speak with the official. You should first consult with the patient to determine whether the patient is willing to speak with the official. If the patient declines to speak with the official, you should inform the enforcement official.

**ACTION PLAN: COURT-ORDERED REQUESTS FOR PHI**

<p><u>Step 1:</u> Is the court order or a court-ordered subpoena, summons or warrant ("SSW") signed by a judge or other judicial officer of a court, grand jury or administrative tribunal?</p>	<p>YES  Go to Step 2</p>	<p>NO  The HIPAA Compliance Officer should deny the request in writing stating that a court order or court-ordered SSW signed by a judge or judicial officer must be provided to City of Washington EMS before the request will be considered.</p>
<p><u>Step 2:</u> If the request is signed by a judge or judicial officer, City of Washington EMS may disclose ONLY the information that is specifically requested by the court order or court-ordered SSW. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI City of Washington EMS is required to disclose. If necessary, the HIPAA Compliance Officer shall ask that the court, grand jury or administrative tribunal re-issue a more specific request. The HIPAA Compliance Officer shall retain a copy of the court-ordered request in the patient file, track the disclosure in an accounting log, and document: the name of requesting entity; the date of the request; the date of disclosure and the PHI that was disclosed.</p>		

## ACTION PLAN: ADMINISTRATIVE REQUESTS FOR PHI FROM GOVERNMENT AGENCIES

<p><u>Step 1:</u> Does the federal, state, or local government agency have the authority to make the administrative request (an administrative request can include an administrative subpoena, summons, civil or other authorized investigative demand or similar process)? The HIPAA Compliance Officer should look to any statutory or regulatory authority cited in the request and consult with legal counsel when making this determination.</p>	<p>YES  Go to Step 2</p>	<p>NO The HIPAA Compliance Officer should deny the request in writing stating that proper legal authority, demonstrating that the agency has the right to request and receive the PHI, must be provided to City of Washington EMS by the administrative agency before the request will be considered.</p>
<p><u>Step 2:</u> Is it clear from the request that all 3 conditions below are satisfied?</p> <ol style="list-style-type: none"> <li>1. The PHI sought by the request is relevant and material to a legitimate law enforcement inquiry;</li> <li>2. The request is specific and limited in scope to the extent reasonable practicable in light of the purpose for which the PHI is sought; and</li> <li>3. De-identified information could not reasonably be used?</li> </ol>	<p>YES  Go to Step 3</p>	<p>NO The HIPAA Compliance Officer should send the requestor a letter stating that City of Washington EMS will not disclose any PHI until the administrative agency certifies in writing that the three conditions have been met.</p>
<p><u>Step 3:</u> The HIPAA Compliance Officer shall ONLY disclose the PHI that has been requested in the administrative request. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI City of Washington EMS is required to disclose. If necessary, the HIPAA Compliance Officer shall ask the requesting agency to re-issue a more specific request. The HIPAA Compliance Officer shall retain a copy of the administrative request as well as any written assurances in the patient file. The HIPAA Compliance Officer shall also track the disclosure in an accounting log and document: the name of requesting agency; the date of the request; the date of disclosure and the PHI that was disclosed.</p>		



## ACTION PLAN: ATTORNEY-ISSUED SUBPOENAS AND DISCOVERY REQUESTS

<p><u>Step 1:</u> Does the request contain the original subpoena, discovery request, or other legal process? References to a subpoena or other document in the request letter are not sufficient.</p>	<p>YES  Go to Step 2</p>	<p>NO The HIPAA Compliance Officer should deny the request in writing stating that the original subpoena, discovery request, or other legal process must be provided to City of Washington EMS before City of Washington EMS will consider the request.</p>
<p><u>Step 2:</u> Does the request seeking PHI also contain "satisfactory written assurances?" In order to contain satisfactory written assurances, the request must include documentation that demonstrates <u>either</u> of the following:</p> <ul style="list-style-type: none"> <li>• The attorney requesting the PHI made a good faith attempt to provide written notice to the patient that included information about the litigation or proceeding <u>and</u> the PHI request, and such notice was sufficient to permit the individual the opportunity to raise an objection to the court or administrative tribunal. Additionally, the time for the patient to raise objections to the court or administrative tribunal has elapsed, and either: (i) no objections were filed; or (ii) all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution. Documentation may include, for example, a copy of the notice mailed to the individual that includes instructions for raising an objection with the court and the deadline for doing so, and a written statement or other documentation demonstrating that no objections were raised or all objections raised were resolved and the request is consistent with the resolution. To the extent that the subpoena or other request itself demonstrates the above elements, no additional documentation is required;</li> <li>OR</li> <li>• The parties to the dispute giving rise to the request for PHI have agreed to a "qualified protective order" and have presented it to the court or administrative tribunal with jurisdiction over the dispute; <u>or</u> the attorney seeking the PHI has requested a qualified protective order</li> </ul>	<p>YES  Go to Step 3</p>	<p>NO The HIPAA Compliance Officer should send the requestor a letter stating that City of Washington EMS will not disclose any PHI until the proper satisfactory written assurances have been provided to City of Washington EMS.</p>



from such court or administrative tribunal. A "qualified protective order" is an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (i) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and (ii) requires the return of the PHI or destruction of the PHI (including all copies made) at the end of the litigation or proceeding. Documentation may include, for example, a copy of the qualified protective order that the parties have agreed to and documentation or a statement that the order was presented to the court, or a copy of the motion to the court requesting a qualified protective order.

Step 3:

The HIPAA Compliance Officer shall ONLY disclose the PHI that has been requested in the subpoena. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI City of Washington EMS is required to disclose. If necessary, the HIPAA Compliance Officer shall ask the requesting agency to re-issue a more specific request. The HIPAA Compliance Officer shall retain a copy of the request from the attorney as well as the satisfactory written assurances in the patient file. The HIPAA Compliance Officer shall also track the disclosure in an accounting log and document: the name of requesting party; the date of the request; the date of disclosure and the PHI that was disclosed.

## **NEWS MEDIA INTERACTION POLICY**

### **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") establishes the circumstances under which individuals' protected health information ("PHI") can be disclosed. Generally, City of Washington EMS may not disclose PHI to the news media without the patient's written express authorization. In addition, state laws may also grant patients additional privacy protections and may enable parties to bring legal action for invasion of privacy or other related causes of action for improper releases of patient information to the news media – sometimes even information that might not qualify as PHI under HIPAA.

This policy establishes consistent guidelines for City of Washington EMS to follow when dealing with requests from the media so that City of Washington EMS respects individual privacy rights and complies with applicable federal and state law. This policy is meant to work in conjunction with City of Washington EMS's "Action Plan on News Media Interaction." City of Washington EMS fully respects the right of the public to know about events, but we will provide information to the news media only to the extent that the law allows us and only when it would not infringe on the privacy rights of our patients.

### **SCOPE**

This policy applies to all City of Washington EMS staff members who might come into contact with or who may be contacted by various media outlets. Generally, all requests from the media for any information about an incident involving City of Washington EMS will be directed to our Public Information Officer to handle. Or, if City of Washington EMS does not have a designated Public Information Officer, all requests should be directed to our HIPAA Compliance Officer.

### **PROCEDURE**

#### *Requests from the News Media*

1. City of Washington EMS staff members will at all times treat members of the media in a professional manner when a request for information is made.
2. All information requests from the news media received by any City of Washington EMS staff members shall be directed to the Public Information Officer. Or, if City of Washington EMS does not have a designated Public Information Officer, all requests from the news media shall be directed to the HIPAA Compliance Officer. Upon receipt of a request for information from the news media, staff members should inform the news media requestor that it is the policy of City of Washington EMS that all media requests be handled by one official and staff members should provide the media requestor contact information for the Public Information Officer or HIPAA Compliance Officer, as appropriate. Or, the staff member may contact the Public Information Officer or HIPAA Compliance Officer to inform the Officer of the request and request authorization to release information to the media.
3. Staff members other than City of Washington EMS's Public Information Officer or HIPAA Compliance Officer are not permitted to release information to the news media, unless authorized or directed by the appropriate Officer to do so.

4. The Public Information Officer or HIPAA Compliance Officer shall use discretion in handling requests from the news media and when deciding whether to release (or permit the release) of information to the media. The Public Information Officer or HIPAA Compliance Officer should only release information to the media when such release would not violate federal or state laws and when release would not infringe a patient's reasonable expectation to privacy. For example, if City of Washington EMS transported a high profile member of the community, City of Washington EMS should probably decline to disclose even general information that does identify the individual to the media since it is likely the patient's identity would be known to anyone hearing the report.

#### *Releasing Information to the News Media*

1. City of Washington EMS may not release any PHI to the news media, absent a patient's written, signed authorization. In the event that the patient or the patient's authorized representative signs a HIPAA-compliant authorization form, disclosures of information, including PHI, may be made so long as they are done in accordance with the express terms of the written Authorization. City of Washington EMS's "Authorization to Use and Disclose Protected Health Information" Form should be used for this purpose.
2. If there is no written authorization from the patient, City of Washington EMS may only release information that is "de-identified." De-identified information is information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify a specific individual. City of Washington EMS may only release the following types of "de-identified" information to members of the media where appropriate:
  - a. Name of hospital. City of Washington EMS may provide the name of the hospital to which patients have been transported. (*Example:* The media calls about "the accident at Third and Main earlier this afternoon." City of Washington EMS may inform the media that "a patient was transported from the accident scene to ABC Hospital.")
  - b. Number of patients. City of Washington EMS may provide the total number of patients involved in an incident or transported to a facility. City of Washington EMS may not indicate specifics, such as the type of vehicle a patient was driving or which patient went to a particular facility. (*Example:* City of Washington EMS may inform the media that "four patients were transported from the fire at the Chemical Factory. Two were taken to County General and two were taken to the Regional Medical Center.")
  - c. Age & Gender. City of Washington EMS may provide the age of a patient and the gender of the patient, unless it could reasonably be used to identify the patient. (*Example:* City of Washington EMS may inform the media that "a 39 y/o male was transported from the accident on the Interstate.")
  - d. Designation of crew members. City of Washington EMS may state, for example, that one paramedic and two EMTs were involved in caring for the patients involved in a motor vehicle accident. City of Washington EMS may identify the names of the personnel who responded. (*Example:* City of Washington EMS may inform the media that "City of Washington EMS personnel on the scene of the incident included two paramedics and a supervisor and advanced life support was administered.")
  - e. Type of Transport. City of Washington EMS may indicate that a particular call was an emergency and that transportation was facilitated by ambulance or helicopter. (*Example:* "Of the 3 patients on the scene of the incident, one was transported by helicopter to the Trauma Center and two were transported as non-emergency patients to the local hospital emergency department.")

## **ACTION PLAN: NEWS MEDIA INTERACTION**

<p><u>Step 1:</u> Is the request asking City of Washington EMS to disclose PHI? Upon receipt of a request for information from the news media, the Public Information Officer or HIPAA Compliance Officer shall determine whether the request is asking City of Washington EMS to disclose PHI.</p>	<p>YES Go to Step 2</p>	<p>NO Go to Step 3</p>
<p><u>Step 2:</u> City of Washington EMS will not release any PHI to the news media absent a patient's written, signed authorization. The Public Information Officer or HIPAA Compliance Officer may consider asking the patient, or the patient's personal representative, whether they would agree to allow City of Washington EMS to release the requested PHI to the news media. In the event that the patient or the patient's authorized representative does agree to permit City of Washington EMS to make the disclosure, the Public Information Officer or HIPAA Compliance Officer shall require the individual to complete and sign City of Washington EMS's "Authorization to Use and Disclose Protected Health Information" Form to permit the disclosure. City of Washington EMS may only disclose PHI to the media in strict compliance with what the Authorization states.</p>		
<p><u>Step 3:</u> City of Washington EMS may release the following types of "de-identified" information to members of the media in accordance with City of Washington EMS's "Policy on News Media Interaction":</p> <ul style="list-style-type: none"> <li>• Name of hospital</li> <li>• Number of patients</li> <li>• Age and gender of patients</li> <li>• Designation of crew members</li> <li>• Type of transport</li> </ul>		

## **STAFF MEMBER MEDICAL RECORDS POLICY**

### **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires City of Washington EMS to treat protected health information ("PHI") contained in the medical records of our staff members with the same degree of protection as the PHI of our other patients. This policy provides guidance to management and staff concerning the privacy and security of City of Washington EMS staff member medical records.

### **SCOPE**

This policy applies to PHI of all staff members and it applies equally to management and non-management staff members.

### **PROCEDURE**

#### *Distinguishing PHI and Employment Records*

1. Health information that is obtained about staff members in the course of providing ambulance or other medical services directly to them is considered to be PHI under HIPAA.
2. Health information that City of Washington EMS receives in its role as an employer is not considered to be PHI. Rather, the information is an employment record to which City of Washington EMS does not have an obligation to extend HIPAA protections. For example, if a staff member submits a doctor's statement to a supervisor to document an absence or tardiness from work, City of Washington EMS does not need to treat that statement as PHI. Other health information that could be treated as an employment record, and not PHI, includes:
  - a. Medical information that is needed for City of Washington EMS to carry out its obligations under the FMLA, ADA and similar laws;
  - b. Information related to occupational injury, disability insurance eligibility, drug screening results, workplace medical surveillance, and fitness-for-duty-tests of employees.

#### *General Policy Regarding Staff Member's PHI*

1. City of Washington EMS will, to the extent required by law, protect, use and disclose PHI it receives about staff members in accordance with HIPAA and our HIPAA Policies and Procedures.
2. Only those with a legitimate need to use or disclose PHI about staff members will have access to that information.
3. In accordance laws concerning disability discrimination, all medical records of staff will be kept in separate files apart from the employee's general employment file. These records will be secured, used and disclosed in accordance with applicable laws.

#### *General Policy Regarding Employment Records*

1. Employment records are not considered to be PHI. As such, City of Washington EMS is not required to protect, use and disclose employment records in accordance with HIPAA.
2. Employment records that are not covered under HIPAA include, but are not limited to:

- a. Information obtained to determine suitability to perform the job duties (such as physical examination reports);
  - b. Drug and alcohol tests obtained in the course of employment;
  - c. Doctor's excuses provided in accordance with the attendance policy;
  - d. Work-related injury and occupational exposure reports; and
  - e. Medical and laboratory reports related to such injuries or exposures, especially to the extent necessary to determine workers' compensation coverage.
3. Despite the fact that City of Washington EMS is not required to protect, use and disclose employment records in accordance with HIPAA, City of Washington EMS will limit the use and disclosure of these records to only those necessary to perform business-related functions authorized by law. City of Washington EMS will also secure all employment records of staff members and ensure that only staff members with a legitimate need to have access to them, such as certain management staff, City of Washington EMS's designated physician and state agencies pursuant to state law, have access to employment records.

## **PHYSICAL SECURITY OF PHI AND E-PHI POLICY**

### **PURPOSE**

City of Washington EMS is obligated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to establish physical safeguards to protect electronic protected health information ("e-PHI") and other PHI. This policy establishes our security measures to protect our electronic information systems, networks and applications and as well as buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

### **SCOPE**

This policy applies to all City of Washington EMS staff members. All staff members should be on the lookout for any potential problems that could jeopardize the security of electronically stored information, especially e-PHI. This policy describes our general approach to facility security and the steps necessary to prevent a breach in the physical security system in place. It also describes our general procedures to limit physical access to electronic information systems and the buildings and rooms in which they are housed and our general procedures on disposal or reissuance of equipment containing e-PHI.

### **PROCEDURE**

#### *Facility Access Controls*

1. Access to areas of our facility that contain our information system with e-PHI will be granted only to those with a verifiable and approved business need to have access.
2. Access control will be established with physical hardware that prevents improper or inadvertent entry into a secure area. This hardware may include keyed locks, combination locks, swipe cards, smart cards and other devices on all doors housing our information system equipment.
3. Any space in a building that we share with another entity that contains PHI that we create, receive, maintain or transmit will be maintained at the same level of security as if we owned the space. Specifically, we will protect that area from access by others in the building who are not part of City of Washington EMS.
4. Disabling or circumventing any of the physical security protections is strictly prohibited. Any problems with physical security measures must be reported to the HIPAA Compliance Officer immediately.

#### *Facility Security Plan*

1. The HIPAA Compliance Officer will be responsible for developing a facility security plan that protects our buildings from unauthorized physical access, tampering, and theft.
2. The plan will incorporate hardware to limit access to our buildings to only those persons with proper keys and/or access codes.
3. City of Washington EMS will maintain a current list of all staff members who have authorization to access our facilities with PHI.

### *Access Control and Validation Procedures*

1. City of Washington EMS has established procedures for controlling and validating a staff member's access to our facilities. Access to various areas of the facilities will be based on the role of the staff person and their need to access a particular area.
2. Access to locations that house our systems, networks or applications with PHI that we create, receive, maintain or transmit will have the greatest limitations on access, and access to these critical areas will be reviewed frequently by management and the HIPAA Compliance Officer.

### *Maintenance Records*

1. To help ensure that our physical security systems are in continuous operation, City of Washington EMS has developed a maintenance program for all security devices, including locks, keypads, and other access devices.
2. Any repairs or change outs of any security devices will be recorded.

### *Workstation Security and Use*

1. A "workstation" is defined as any electronic computing device, such as a desktop computer, laptop computer, mobile electronic device or any other device that is used to create, receive, maintain or transmit PHI.
2. All workstations (including fixed locations such as in our billing or business office and mobile workstations such as with portable electronic devices for field use) should be password protected so that they may not be accessed without authentication by an authorized user.
3. All workstations are set up to lock out after a set time period so that if the staff member is no longer using the workstation for a set period of time, access will not be permitted without the proper password.
4. Procedures are established for each work area, depending on the nature of the work area to limit viewing of workstation device screens to only those operating the workstation wherever possible.
  - a. In office areas, all screens should be pointed away from hallways and open areas. The screens should be pointed away from chairs or other locations where non staff members, such as patients, may be.
  - b. In field operations, ambulance personnel will need to follow procedures to ensure that the devices are not left in an open area, such as a countertop in the Emergency Department.
5. Workstations will be set so that staff members may not inadvertently change or disable security settings, or access areas of the information system they are not authorized to access.
6. Only those authorized to access and use the workstation will be permitted to use the workstation.
7. No software may be downloaded or installed on the workstation in any manner without prior authorization. (This prohibition includes computer games, screen savers, and anti-virus or anti-spam programs).



8. All staff members will log out or lock workstations whenever they are left unattended or will not be in use for an extended period of time.
9. All portable workstation devices will be physically secured wherever possible when not in use. Laptops will be locked with security cables and other mobile devices will be locked physical locations or in an appropriate storage compartment when not in use.
10. Remote access to access e-PHI on our information system must be approved by City of Washington EMS.

*Disposal of Hardware and Electronic Media Devices and Media Controls*

1. City of Washington EMS carefully monitors and regulates the receipt and removal of hardware and electronic media that contain PHI and other patient and business information into and out of our stations and other facilities.
2. As a general rule, simple deletion of files or folders is not sufficient to ensure removal of the file or data. This simply removes the directional "pointers" that allow a user to find the file or folder more readily. Deleted files are usually completely retrievable with special software and computer system expertise.
3. City of Washington EMS has in place the following procedures governing the disposal of hardware, electronic media, and e-PHI stored on hardware and other electronic media:

- **Sanitizing Hard Disk Drives.** All hard disk drives that have been approved by the HIPAA Compliance Officer for removal and disposal (or taken out of active use) shall be sanitized so that all programs and data have been removed from the drive. City of Washington EMS will follow industry best practices (such as the U.S. Department of Defense clearing and sanitizing standard – DoD 5220.22-M) when cleaning off hard drives.

Proper sanitizing usually involves a reformatting of the hard drive in a secure manner with an approved wipeout utility program. Degaussing software may need to be used to ensure total removal of files.

No hard drive will be reissued, sold or otherwise discarded until the drive has been sanitized.

- **Media Re-Use.** All e-PHI and other patient and business information shall be removed from any media devices before they are made available for reuse.
- **Accountability.** City of Washington EMS tracks the movement of all computer hardware, workstations, and data storage devices. Movement both within the organization and outside the organization is tracked.
- **Data Backup and Storage.** Each information system area will create an exact copy of all e-PHI when necessary immediately prior to any movement or disposal. This procedure is in addition to the standard routine backup protocol to ensure that all e-PHI is preserved before potential compromise.
- **Destruction of Paper and electronic PHI.** When destroying and/or permanently removing PHI from electronic media for any purpose, City of Washington EMS shall adhere to HHS's "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals." In accordance with that Guidance, paper, film, or other

hard copy media shall be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. Electronic PHI is considered to be destroyed or permanently removed from electronic media when the media that contain the PHI have been cleared, purged, or destroyed consistent with "NIST **Special Publication 800-88**, *Guidelines for Media Sanitization*," such that the electronic PHI cannot be retrieved. (NIST Special Publication available at: [www.nist.gov](http://www.nist.gov)).

# **GENERAL SECURITY OF ELECTRONIC AND OTHER PATIENT AND BUSINESS INFORMATION**

## **PURPOSE**

City of Washington EMS is committed to providing all aspects of our service and in conducting our business operations in compliance with all applicable laws and regulations. This policy set forth our commitment to compliance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the use and disclosure of Protected Health Information ("PHI") under the Privacy Regulations ("Privacy Rule") and the security of Electronic Protected Health Information ("e-PHI") under the Security Regulations (the "Security Rule").

This policy and our procedures as to the creation, use, disclosure, and security of PHI and e-PHI also applies to other essential patient information, billing and business information, and confidential information that is stored electronically or in any other manner, including paper or hard copy form.

## **SCOPE**

This Policy addresses our general approach to compliance with the Security Rule. As a covered entity under the Security Rule, City of Washington EMS is required to:

1. Ensure the confidentiality, integrity and availability of all PHI and e-PHI City of Washington EMS creates, receives, maintains or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and
4. Ensure compliance with the Privacy and Security Rule by our staff.

Compliance with the Privacy and Security Rules will require City of Washington EMS to implement:

- Administrative Safeguards—actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect PHI and e-PHI and to manage the conduct of our staff in relation to the protection of and authorized access to patient information.
- Physical Safeguards—physical measures, policies and procedures to protect our electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
- Technical Safeguards—the technologies and the policies and procedures for its use that protect PHI and e-PHI and control access.

## **PROCEDURE**

*HIPAA Compliance Officer*

City of Washington EMS has designated a HIPAA Compliance Officer with overall responsibility for the development and implementation of policies that conform to the Privacy Rule ("Privacy Policies") and the Security Rule ("Security Policies"). The HIPAA Compliance Officer is Caroline Scoville. The HIPAA Compliance Officer is responsible for ensuring that City of Washington EMS: (i) complies with the HIPAA Security Policies, (ii) develops and implements HIPAA security procedures ("Security Procedures") for each Security Policy, (iii) maintains the confidentiality of all e-PHI created or received by City of Washington EMS (as well as other essential patient information, billing and business information, and confidential information that is stored electronically) from the date the information is created or received until it is destroyed, and (iv) trains all staff members of City of Washington EMS at the appropriate level of HIPAA training as determined by the HIPAA Compliance Officer.

#### *Implementation of Security Measures*

City of Washington EMS will implement any security measure that allows it to reasonably and appropriately comply with a specific security standard in the Security Rule. In determining which security measures to implement, City of Washington EMS will take into account its size, complexity and capabilities; technical infrastructure; hardware and software security capabilities; the costs of the security measures; and the probability and criticality of potential risks to e-PHI.

City of Washington EMS will determine what security measures *must* be implemented and will determine those measures that we have *discretion* to implement. The determination as to what security measures are required or discretionary will be reviewed by the Privacy/HIPAA Compliance Officer to ensure compliance with the Security Rule.

#### *Security Complaints*

The HIPAA Compliance Officer shall be responsible for facilitating a process for individuals (including staff members) to file a complaint regarding our Security Policies or the manner in which e-PHI and other confidential information is handled. The HIPAA Compliance Officer is responsible for ensuring that the complaint and its disposition are appropriately documented and handled.

#### *Mitigation, Sanctions and Non-Retaliation*

City of Washington EMS will ensure it mitigates damages that may occur as a result of any violation of the Security Rule or our Security Policies or specific Security Procedures.

Any staff members who violate the Security Rule or City of Washington EMS policies with respect to e-PHI and other protected and confidential information will be disciplined accordingly. This may include verbal or written counseling, suspension, or even termination, depending upon the seriousness of the infraction.

City of Washington EMS will not intimidate or retaliate against any person for exercising his or her rights under the Security Rule or for reporting any concern, issue or practice that the person believes in good faith to be in violation of the Security Rule or our Security Policies or specific Security Procedures.

City of Washington EMS will not require any person to inappropriately waive any rights that person may have to file a complaint with the Department of Health and Human Services.

#### *Security Policies and Procedures*

The City of Washington EMS Security Policies and Security Procedures are designed to ensure compliance with the Security Rule. These Security Policies and Security Procedures will be kept current and in compliance with any changes in the law or regulations. There will be periodic evaluation of our Security Policies and Procedures whenever there are significant changes in the law or regulations or at least on an annual basis when there are no such changes.

#### *Responsibility of All Staff Members*

City of Washington EMS takes privacy issues very seriously, especially in light of the unique work that we do in EMS and medical transportation. We will only recruit, hire, or accept staff members who are sensitive to patient privacy and who demonstrate a commitment to the principles of protecting our patient information and our business and other confidential information.

Every member of the City of Washington EMS staff is responsible for being aware of, and complying with, the Privacy Rule, the Security Rule, and our Privacy and Security Policies and Procedures. This is an essential requirement of all positions within the organization.

#### *Supervision of Staff Members Who Work With e-PHI*

All staff members who use, access or work with e-PHI shall be supervised by appropriate members of management in accordance with their level of e-PHI access. For instance, the use of e-PHI by staff members in the billing department will be supervised by the billing department manager or other appropriate member of management who oversees that function. The use of e-PHI by field providers will be supervised by the appropriate field/operations supervisory personnel and/or line officers as appropriate.

## **FACILITY AND COMPUTER ACCESS POINT CONTROLS**

### **PURPOSE**

City of Washington EMS is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Due to its critical importance to City of Washington EMS, it is our obligation to control access to our physical locations, such as stations, buildings, garages and offices, as well as the rooms, vehicles, and secured areas where our electronic information system hardware, software, or other peripheral devices are stored or maintained. It is our policy to limit access to our electronic information system while at the same time, permit authorized access in the event of an emergency, or other events that require contingency plans to be placed in operation.

The contingency operations, facility security plan, and access and control and validation procedures are all part of facility and access point controls to preserve, protect, restore and limit or permit access to e-PHI. This policy describes our general approach to facility access under the Security Rule.

### **SCOPE**

This policy applies to all City of Washington EMS staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It is intended to cover all facilities that house our information system hardware, software and related devices and equipment.

### **PROCEDURE**

#### *Contingency Operations*

1. The HIPAA Compliance Officer will work with managers of the electronic information system to determine contingency plans and procedures that should be implemented in the event of the need to restore lost data and to maintain uninterrupted access to e-PHI.
2. Working with management of the Company, the HIPAA Compliance Officer will develop a list of persons who have permission to access computer systems and secured areas in the event that restoration and preservation of data is necessary.
3. The HIPAA Compliance Officer, as part of the contingency plan, will develop and maintain a list of persons authorized to have access to the facility when the contingency plan is in operation.
4. The HIPAA Compliance Officer will work with management to develop a "call list" of persons who need immediate notification when the contingency plan is in operation.
5. The HIPAA Compliance Officer will work with the communications center and other points of access to the facility to determine their role and procedures to follow in the event the contingency plan is in operation.

#### *Facility Security*

- a. The HIPAA Compliance Officer will work with management to determine who should have access to e-PHI and the electronic information system and determine the extent of that access.
- b. Care will be taken to ensure that limitation of access does not hinder our ability to provide essential information needed for treatment and transport of patients, billing for our services, and health care operations.
- c. An inventory of all software and hardware will be developed and maintained by the Privacy/HIPAA Compliance Officer to include:
  - a. Use of make, model and/or serial numbers as identification numbers to hardware and other devices that are part of the electronic information system.
  - b. A separate and independent inventory list will be maintained to catalog all software and hardware, with their respective identification numbers. The inventory will be conducted on at least an annual basis.
  - c. Any discrepancies in the current inventory of software and hardware in comparison to the last inventory will be reported to management and will be investigated to ensure that there is a proper accounting of all City of Washington EMS software and hardware.
  - d. A central storage area for all original/licensed copies of software, source codes, etc. shall be created that is secure and environmentally safe so that the software is protected from destruction or damage as best as possible. These items shall be stored in the vault at City Hall.
- d. All City of Washington EMS staff members who are approved for access to e-PHI sources and the electronic information system shall be assigned unique passwords where appropriate to ensure secure access to the system.
- e. There will be a list of all keys and passport devices issued to personnel who have access to the electronic information system to ensure accountability. The keys will be returned upon termination with the Company, and the Staff Member Termination Checklist will be completed to ensure that all necessary means of access have been revoked or returned. The list will be developed and maintained by the HIPAA Compliance Officer and updated as needed.
- f. There will be sign-in logs on the main server, which is maintained on the server, so that the person who accessed the server can be readily traced. The information in these logs should include:
  - a. Name of the person;
  - b. Time in;
  - c. Time out;
  - d. Description of purpose for access.
- g. All logs and checkpoint records will be reviewed periodically to ensure only authorized persons with a legitimate purpose for access actually have access to the facility or secured area.

### *Access Control and Validation*

1. Lists of persons with approved access to e-PHI and the electronic information system will be maintained to include lists of approved vendors and other outside parties who have permission to access our facilities and secure areas.
2. Software testing and other maintenance or service of the electronic information system will be carefully monitored by the HIPAA Compliance Officer.
3. All guests and others with temporary access to the electronic information system that contains e-PHI shall sign or log in to the facility or access point. Access will be granted only upon presentation of verification of identity (such as a driver's license) and authorization to have access to the facility or access point.
4. The staff member permitting access to anyone other than an authorized City of Washington EMS staff member will document their name so as to be able to track who gave the person access.

### *Maintenance Records*

1. The HIPAA Compliance Officer will ensure that all repairs and maintenance to the electronic information system hardware or software is properly logged and documented.
2. The repair or maintenance records will contain, at a minimum:
  - a. Name of person completing the maintenance or repair;
  - b. Purpose of the maintenance or repair;
  - c. Name of person authorizing it;
  - d. Date and time the work started and ended;
  - e. Brief description of the work completed and the outcome of it (more work required, alternative procedure to put in place, etc.).
3. The HIPAA Compliance Officer will periodically review the documentation of maintenance and repairs to determine trends or change in procedures to e-PHI security that should be made.

### *Accountability*

1. The HIPAA Compliance Officer will develop a procedure to maintain and record the actions of any staff member or other person who adds hardware or software to our electronic information system.
2. Any hardware or software removed from the electronic information system will be signed in and signed out, with the signature of the person removing the hardware or software, and a corresponding signature of the HIPAA Compliance Officer or other approved manager to acknowledge approval for the removal and responsibility for it.



3. No hardware or software will be added to the electronic information system without consultation with the HIPAA Compliance Officer.
4. To maintain security and to help prevent viruses from attacking our information system, no downloads or software additions are permitted without approval of management and only after consultation with the HIPAA Compliance Officer.

## **THIRD PARTY ACCESS TO E-PHI POLICY**

### **PURPOSE**

City of Washington EMS is required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to control access to our physical locations, such as stations, buildings, garages and offices, vehicles, and secured areas where our electronic protected health information ("e-PHI") is stored as well as system hardware, software, or other mobile electronic devices that are used to create, receive, maintain or transmit e-PHI. This policy outlines our approach to limiting third party access to our e-PHI while at the same time, permitting authorized access in the event that our contingency plan is operation.

### **SCOPE**

This policy applies to all City of Washington EMS staff members who control third party access to our e-PHI and systems, hardware and mobile electronic devices used to create, receive, maintain or transmit e-PHI. It is intended to cover all physical locations that house our information system hardware, software and related devices and equipment that are utilized to create, receive, maintain or transmit e-PHI at City of Washington EMS.

### **PROCEDURE**

#### *Access During Contingency Operations*

1. The HIPAA Compliance Officer will work with individuals who manage electronic information systems to determine contingency plans and procedures that should be implemented in the event of the need to restore lost data and to maintain uninterrupted access to e-PHI.
2. The HIPAA Compliance Officer will identify outside parties who have permission to access our electronic systems and secured areas in the event that restoration and preservation of data is necessary.
3. The HIPAA Compliance Officer will work with management to develop a "call list" of persons who need immediate notification when the contingency plan is in operation.

#### *Facility Security*

1. The HIPAA Compliance Officer will work with management to determine what outside parties, in general, should have access to e-PHI and the electronic information system and determine the extent of that access.
2. The HIPAA Compliance Officer will maintain an inventory of all software, hardware and mobile electronic devices used to create, receive, maintain or transmit e-PHI at City of Washington EMS. That inventory should include:
  - a. Use of make, model and/or serial numbers as identification numbers to hardware and other devices that are part of the electronic information system.
  - b. A file to catalog all software, hardware and mobile electronic devices with their unique identification numbers.

3. Any discrepancies in the current inventory of software, hardware and mobile electronic devices will be reported to management and will be investigated to ensure that there is a proper accounting of all items and to determine whether further action may need to be taken in response to the loss of an item (e.g., breach notification in the event of a breach of unsecured PHI).
4. If City of Washington EMS implements keypad access to physical facilities, the HIPAA Compliance Officer will ensure that access codes are changed or disabled when staff members leave.
5. There will be measures at the entrance to City of Washington EMS's facility and at key access points that require personal identification, so that only authorized parties gain access to areas where e-PHI can be accessed. These procedures will be reviewed periodically to ensure only authorized persons with a legitimate purpose for access actually have access to the facility or secured area.

#### *Access Control and Validation*

1. The HIPAA Compliance Officer will maintain a list of all third parties with approved access to e-PHI and the electronic information system. This list will include names of approved vendors and other outside parties who have permission to access our facilities and secure areas.
2. Software testing and other maintenance or service of the electronic information system will be carefully monitored by the HIPAA Compliance Officer to ensure that only necessary e-PHI is accessed and that e-PHI is not being improperly used or disclosed.
3. City of Washington EMS will ensure that only approved parties with a legitimate need to access our electronic information system are granted access. If outside parties need physical access to an area with e-PHI, they must present valid credentials (such as a driver's license and business card or badge).

#### *Maintenance Records*

1. The HIPAA Compliance Officer will ensure that all repairs and maintenance to the electronic information system hardware, software and mobile electronic devices is properly logged and documented.
2. The repair or maintenance records will contain, at a minimum:
  - a. Name of person completing the maintenance or repair;
  - b. Purpose of the maintenance or repair;
  - c. Name of person at City of Washington EMS authorizing the maintenance or repair;
  - d. Date and time the work started and ended; and
  - e. Brief description of the work completed and the outcome of it (more work required, alternative procedure to put in place, etc.)
3. The HIPAA Compliance Officer will periodically review the documentation of maintenance and repairs to determine trends or changes in procedures to e-PHI security that should be made.

*Accountability*

1. City of Washington EMS shall have a way to record the addition or removal of any hardware, software or mobile electronic devices to or from our electronic information system.
2. No hardware, software or mobile electronic devices will be added to the electronic information system without notifying the HIPAA Compliance Officer. The HIPAA Compliance Officer shall review any additions and ensure that any addition will comply with City of Washington EMS's HIPAA Policies and Procedures.
3. To maintain security and to help prevent viruses from attacking our information system, no downloads or software additions are permitted without approval of management and only after consultation with the HIPAA Compliance Officer.

## **PERSONS WHO MAY ACCESS COMPUTER SYSTEMS AND SECURED AREAS IN THE EVENT OF AN EMERGENCY**

As part of the City of Washington EMS HIPAA Compliance Plan, the Company is required to have a list on file of those persons authorized to access the City of Washington EMS computer systems in the event of an emergency.

The following persons may have access to the City of Washington EMS computer information systems and secured areas in the Event of an Emergency:

- City Administrator, City Clerk, City Treasurer and Full Time EMT;
- Computer Information Concepts personnel;
- Dague Computers personnel;
- Computer Solutions, Inc personnel.
- Other assigned/hired/contracted personnel as needed to correct/maintain normal business operations.

If other individuals are allowed access, they shall first enter into a Business Associate agreement with the City of Washington EMS.

## **PERSONS WITH KEYS TO CITY OF WASHINGTON EMS BUSINESS OFFICE**

As required in the City of Washington EMS HIPAA Compliance Plan, a list of individuals who are in possession of keys to the office must be kept and updated regularly. Keys shall be returned and documented in the event of an employee's termination of employment with the City of Washington.

Only the following individuals shall possess a key to the City of Washington EMS:

City Administrator Carl D. Chalfant, Cell phone: 785-220-4175

City Clerk Denise Powell, Home: 785-325-2400 Cell phone: 785-747-8534

City Treasurer Colleen Hillyer, Home: 785-325-2157 Cell phone: 785-541-0075

HIPAA Compliance Officer/Full Time EMT Caroline Scoville, Cell phone: 785-822-4591

## **INVENTORY OF HARDWARE & MOBILE ELECTRONIC DEVICES**

All City of Washington EMS computer hardware and mobile electronic devices assigned to the use of each staff member are to be inventoried and tracked using this form. Supervisors must review this form with each staff member and the staff member must acknowledge assignment of the hardware or device.

The form should be maintained in the staff member's personnel file with a copy to be kept by the HIPAA Compliance Officer. When the staff member leaves the organization, there must be verification that all computer equipment, software and mobile electronic devices have been returned.

Name of Staff Member: \_\_\_\_\_  
 Position Title: \_\_\_\_\_  
 Department: \_\_\_\_\_

Hardware

Device	Description	Serial #	Date Assigned	Date Returned	Staff Initials
Computer					
Laptop					
Printer					

Mobile Electronic Devices

Device	Description	Serial #	Date Assigned	Date Returned	Staff Initials
Cell phone					
Digital camera					
Storage device (USB, external hard drive etc.)					
[Insert additional items as necessary]					



## **COMPUTER HARDWARE/PERIPHERALS/SOFTWARE INVENTORY**

All City of Washington EMS computer hardware, peripheral devices, and software assigned to the use of each staff member are to be inventoried and tracked. The City Administrator must review this form with each staff member upon completion, with the staff member acknowledging assignment of the device/software.

The form should be maintained in the staff member's personnel file. When the staff member leaves the organization, there must be verification that all computer equipment and software has been returned.

### **Name of Staff Member: Denise Powell**

Position Title: City Clerk

#### Hardware

Nobilis Notebook S/N 1098332 mfg date 1/2009 N4040

HP Laserjet P4014N S/N CNDX331958

### **Name of Staff Member: Carl D. Chalfant**

Position Title: City Administrator

Printer - Hewlett Packard DeskJet 970cxi Model C6429A S/N MX9B11B118

Nobilis N4022 908789 Laptop Mfg date 3/2007 S/N 6AN0AC027349 M/N Z84F

### **Name of Staff Member: Colleen Hillyer**

Position Title: City Treasurer

Nobilis i265G Pro - 17" monitor-flat panel M/N FP767 (BenQ)  
SN 99L537201133901038TAB011 Mfg date 9/2003

Keyboard S/N 5167712613037 Mouse P/N X08-70400 Tower Nobilis 1098333 Mfg date 1/2009

Battery Backup - S/N G30904777 M/N KIN2200AP

Logitech cordless Mouse & Receiver S/N LZC25051865

Receipt Printer - Ithaca M/N 94PL P/N ITH94CX S/N HR002377302

HP Laserjet 1000 CNBJ198336

#### **SERVER**

HP ML310G5 S/N 470065-052hp S/N MX200200M7



**PASSWORD AUTHORIZATION FORM**

Name: \_\_\_\_\_ Date: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Employee ID: \_\_\_\_\_

New Password  Replacement Password

Organizational Software \_\_\_\_\_

Employee Sign-on \_\_\_\_\_

Password \_\_\_\_\_

I agree that I will comply with all privacy, security and confidentiality policies and procedures set in place by City of Washington EMS during my entire employment or association with City of Washington EMS. If I, at any time, knowingly or inadvertently breach privacy, security and/or patient confidentiality policies and procedures, I agree to notify the HIPAA Compliance Officer of City of Washington EMS immediately. In addition, I understand that a breach of privacy, security or patient confidentiality policies may result in suspension or termination of my employment or position at City of Washington EMS. Upon termination of my employment or association with City of Washington EMS for any reason, or at any time upon request, I agree to return any and all patient confidential information in my possession. This agreement is not a contract for continued employment.

*Employee Signature* \_\_\_\_\_

*HIPAA Compliance Officer Signature* \_\_\_\_\_

## **STAFF MEMBER ACCESS TO E-PHI POLICY**

### **PURPOSE**

Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") City of Washington EMS is required to ensure that all staff members have appropriate access to e-PHI, and that his or her identity is properly verified before access to City of Washington EMS's networks, systems and applications containing e-PHI can be obtained. This policy establishes procedures to prevent staff members (including former staff members) who should not have access to e-PHI from obtaining it, and ensures that those who are authorized to have access to e-PHI obtain access in a secure fashion.

### **SCOPE**

This policy applies to all City of Washington EMS staff members who have access to any e-PHI that is created, received, maintained or transmitted by City of Washington EMS. The HIPAA Compliance Officer shall be responsible for ensuring proper administration of this policy.

### **PROCEDURE**

#### *Authority to Access e-PHI*

1. Staff members seeking access to any network, system, or application that contains e-PHI must satisfy a user authentication mechanism such as unique user identification and password, biometric input, or a user identification smart card to verify their identity and authority to access e-PHI.
2. Staff members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and password, or other authentication information.
3. Staff members should take reasonable steps to ensure that they verify the identity and correct address (digital or physical) of the receiving person or entity prior to transmitting e-PHI. This might include sending a "test email" or calling a party before a fax is sent.

#### *Unique User Identification*

1. Any staff member or authorized user that requires access to any network, system, or application that creates, receives, maintains or transmits e-PHI at City of Washington EMS must be provided with a Unique User Identification Number.
2. When requesting access to any network, system, or application that creates, receives, maintains or transmits e-PHI at City of Washington EMS, a staff member or authorized user must supply their assigned Unique User Identification in conjunction with a secure password.
3. If a staff member or authorized user believes their User Identification has been comprised, they must report that incident to the appropriate supervisor or the HIPAA Compliance Officer immediately.

#### *Security Password Management*

1. All staff members must create a password in conjunction with their Unique User Identification to gain access to any network, system or application used to create, receive, maintain or transmit e-PHI at City of Washington EMS.
2. A generic User Identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to e-PHI. An additional Unique User Identification and password must be supplied to access networks, systems applications and database systems containing e-PHI at City of Washington EMS.
3. Managers of networks, systems, or applications used to create, receive, maintain or transmit e-PHI at City of Washington EMS must ensure that passwords set by staff members meet the minimum level of complexity described in this policy.
4. Managers of networks, systems, or applications used to create, receive, maintain or e-PHI are responsible for educating staff members about all password related policies and procedures, and any changes to those policies and procedures.
5. Password "aging times" (i.e., the period of time a password may be used before it must be changed) must be implemented in a manner commensurate with the criticality and sensitivity of the e-PHI contained within each network, system, application or database.
6. Staff members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:
  - a. Passwords are only to be used for legitimate access to networks, systems, or applications.
  - b. Passwords must not be disclosed to other staff members or individuals.
  - c. Staff members must not allow other staff members or individuals to use their password.
  - d. Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
  - e. All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store e-PHI must be of sufficient complexity to ensure that it is not easily guessable.
7. Passwords should be a minimum of eight characters in length.
8. Passwords should incorporate three of the following characteristics:
  - a. Any lower case letters (a-z)
  - b. Any upper case letters (A-Z)
  - c. Any numbers (0-9)
  - d. Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @ # \$ % ^ & \* ( ) \_ - + = { } [ ] ; : " ' | \ / ? < > , . ~ `).
  - e. Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.

- f. Passwords must not be words found in a dictionary.

#### *Emergency Access to e-PHI and PHI*

If a system, network or application contains e-PHI used to provide patient treatment, and the denial or strict access to that e-PHI could inhibit or negatively affect patient care, staff members responsible for electronic information systems must ensure that access to that system is made available to any caregiver in case of an emergency.

#### *Termination of Access*

1. All supervisors will immediately notify the HIPAA Compliance Officer when a staff member has been separated from service with City of Washington EMS or when the person no longer is permitted to access e-PHI on City of Washington EMS's systems, networks, or applications.
2. Staff members' access to City of Washington EMS's systems, networks and applications containing e-PHI will immediately be disabled on the effective date of the separation or, if still on the staff, the effective date when authorization for access to e-PHI has ended.
3. The staff member will be removed from all information system access lists.
4. The staff member will be removed from all user accounts.
5. The staff member will turn in all keys, tokens, or access cards that allow access to the information system.
6. The "Staff Member Termination Checklist" will be completed by the supervisor the last day of the staff member's authorized access.

## **STAFF MEMBER ELECTRONIC COMMUNICATIONS**

### **PURPOSE**

City of Washington EMS is required under the Health Information Portability and Accountability Act of 1996 ("HIPAA") to ensure that protected health information ("PHI") that we create, receive, maintain or transmit is not improperly disclosed through any means, including electronic means. The purpose of this policy is to prevent the improper use or disclosure of PHI through electronic means, while staff members are on and off-duty.

### **SCOPE**

This policy covers any and all electronic communications of City of Washington EMS staff members when those communications involve the use or disclosure of PHI created, received, maintained or transmitted by City of Washington EMS. This policy applies to all staff members both on and off duty, whether using company or personal equipment.

### **PROCEDURE**

#### *General Rules Regarding Company Equipment*

1. All PHI created, received, maintained or transmitted using any "Company Equipment" is at all times the property of City of Washington EMS and may be considered to be part of the official records of City of Washington EMS. "Company Equipment" is any electronic device that is owned, leased, controlled, or used for the benefit of City of Washington EMS. This includes, but is not limited to: computers, cell phones, cameras, USB drives, and other devices that are capable of creating, capturing, storing, and/or transmitting electronic information.
2. All Company Equipment shall remain at all times the property of City of Washington EMS, even if being used for personal use.
3. City of Washington EMS cannot guarantee the confidentiality of information stored on any Company Equipment, except that it will take all steps necessary to secure the privacy of all PHI in accordance with all applicable laws. Information stored on Company Equipment is subject to disclosure to law enforcement or other third parties at the sole discretion of City of Washington EMS.
4. City of Washington EMS may monitor activity on Company Equipment, our information systems and our network(s) at any time for the purpose of ensuring that PHI is not being improperly used or disclosed. This includes the ability to monitor internet activity and email, as permitted by law.
5. All internet activity (browsing, email, etc.) using Company Equipment must comply with City of Washington EMS's HIPAA Policies and Procedures and staff members may not disclose PHI on the internet using Company Equipment unless the disclosure is authorized by City of Washington EMS, would not violate HIPAA or other applicable federal and state laws, and the disclosure is for a legitimate, business-related purpose. For example, emailing demographic information about a patient to a patient's insurer for purposes of billing may be a permissible use.

#### *General Rules Regarding Personal Equipment*

1. Staff members must comply with City of Washington EMS's HIPAA Policies and Procedures when engaging in internet activity on "Personal Equipment," both on and off-duty. "Personal Equipment" includes any internet-capable device that is not owned, leased or otherwise controlled or used for the benefit of City of Washington EMS.
2. Where permitted by law to do so, City of Washington EMS will investigate internet activity, whether on or off-duty, and take appropriate disciplinary action against staff members whenever City of Washington EMS learns about a possible or actual violation of our HIPAA Policies and Procedures.
3. Staff members should consult with the HIPAA Compliance Officer whenever there is a question regarding whether an internet posting or internet activity might violate our HIPAA Policies and Procedures.
4. The following types of activities are prohibited at all times and can result in disciplinary action:
  - a. Posting, sharing, or otherwise disseminating any PHI relating to City of Washington EMS patients without authorization from City of Washington EMS.
  - b. Posting, sharing or otherwise disseminating information that could potentially identify a patient, including: photos, videos or other images of a scene or patient; a description of patient injuries; or other scene activities that could be identified with a specific scene without authorization from City of Washington EMS.

#### *Use of Company Electronic Mail*

1. City of Washington EMS's email is intended to be used as a tool to facilitate communications on behalf of City of Washington EMS.
2. All email transmissions that originate from City of Washington EMS staff members on Company email must contain, at a minimum, a signature section that contains the following information:
  - a. The sender's full name;
  - b. City of Washington EMS's name;
  - c. The telephone number of City of Washington EMS; and
  - d. An approved notice and disclaimer.
3. Below the signature section, the following notice and disclaimer must appear on all transmissions from City of Washington EMS staff members in at least 10 point font:

**CONFIDENTIALITY NOTICE:** This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, and/or privileged information protected by law. If you are not the intended recipient, you may not use, copy, or distribute this e-mail message or its attachments. If you believe you have received this e-mail message in error, please contact the sender by reply e-mail and telephone immediately and destroy all copies of the original message.

#### *Facsimile Transmissions Using Company Fax Machine*



1. City of Washington EMS's fax machine is intended to be used as a tool to facilitate communications and the exchange of information, including patient information that is needed to perform our services.
2. All outgoing facsimile transmissions using the Company fax machine must contain a cover sheet that includes at a minimum, the following information:
  - a. The name of City of Washington;
  - b. The name of the intended recipient;
  - c. The name of the sender;
  - d. Facsimile number of the recipient;
  - e. Telephone number of the sender;
  - f. Date of the transmission;
  - g. The number of pages in the transmission; and
  - h. An approved notice and disclaimer.
3. At the bottom of the facsimile cover sheet, the following notice and disclaimer must appear in at least 10 point font:

Confidentiality Notice: This facsimile transmission is confidential and is intended only for the review of the party to whom it is addressed. It may contain proprietary and/or privileged information protected by law. If you are not the intended recipient, you may not use, copy or distribute this facsimile message or its attachments. If you have received this transmission in error, please immediately telephone the sender above to arrange for its return.

*Images and Videos That May Contain PHI*

1. Staff members are strictly prohibited from capturing any images or videos that could potentially identify a patient PHI while on duty without the express permission of a supervisor. Staff members may carry a personal electronic device (such as a cell phone) that is capable of capturing images; but, staff members must adhere to our HIPAA Policies and Procedures when using the device and the device may never be used to capture PHI (unless expressly permitted by a supervisor). No other personal electronic devices that function as a camera and/or video recorder shall be carried by staff members while engaged in any work activities.
2. Staff members may only capture images or video while on-duty with a company-issued device and only for legitimate business-related purposes. Staff members must be authorized by City of Washington EMS to capture images or video while on duty.
3. Images or videos taken with Company Equipment may only be disseminated in accordance with City of Washington EMS's HIPAA Policies and Procedures and City of Washington EMS Protocols & Standard Operating Procedures and all such images and videos are the sole property of City of Washington EMS.

4. Any images or videos that might identify a patient may not be posted on the internet without the express approval of City of Washington EMS.

## **USE OF ELECTRONIC MAIL AND FACSIMILE TRANSMISSIONS**

### **PURPOSE**

City of Washington EMS is responsible for ensuring the privacy and security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Electronic mail and facsimile transmissions are common methods for general communication and sending and receiving patient information. We need to ensure that e-mail and faxes are sent to the proper person and are received by the proper person.

In the event that e-mail and faxes are sent to or received by a person not designated to receive the information, it is important to provide notices and disclaimers on these transmissions to alert the receiving party that the transmission may be confidential and to give them steps they should take to alert us and to return the transmitted information.

### **SCOPE**

This policy applies to all City of Washington EMS staff members who use the electronic mail system or send documents by facsimile transmission.

### **PROCEDURE**

#### *Electronic Mail*

1. The intended use of electronic mail is as a tool to facilitate communications and the exchange of information that is needed to perform our services.
2. It shall be the policy of our company to avoid sending any PHI or e-PHI via electronic mail for any reason if at all possible, or unless specifically requested by patient or patient's family.
3. Occasional personal use is permissible so long as:
  - a. it does not consume more than a trivial amount of resources;
  - b. does not interfere with staff member productivity;
  - c. does not take priority over Company business;
  - d. and complies with our e-mail use and harassment policies.
4. In all cases, users of our electronic mail system have an obligation to use it appropriately, effectively, and efficiently.
5. Staff members must be aware that e-mail can be forwarded, intercepted, printed and stored by others. Therefore, users must utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.
6. E-mail accounts and passwords should not be shared or revealed to anyone else besides the authorized user(s).

7. All electronic mail transmissions that originate from City of Washington EMS staff members must contain, at a minimum, a signature section that contains the following information:

- a. The sender's full name;
- b. The name of the Company or Service;
- c. The telephone number of the Company or Service;
- d. An approved notice and disclaimer.

8. Below the signature section, the following notice and disclaimer must appear on all transmissions from City of Washington EMS staff members in at least 10 point font:

**CONFIDENTIALITY NOTICE:** This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, and/or privileged information protected by law. If you are not the intended recipient, you may not use, copy, or distribute this e-mail message or its attachments. If you believe you have received this e-mail message in error, please contact the sender by reply e-mail and telephone immediately and destroy all copies of the

### **FACSIMILE TRANSMISSIONS**

1. As with e-mail transmissions, the transmission of documents by facsimile machine requires similar protections and safeguards.

2. All facsimile transmissions must contain a cover sheet that includes at a minimum, the following information:

- a. Name of the Company or Service;
- b. Name of the intended recipient;
- c. Name of the sender;
- d. Facsimile number of the recipient;
- e. Telephone number of the sender;
- f. Date of the transmission;
- g. The number of pages in the transmission;
- h. An approved notice and disclaimer.

3. At the bottom of the facsimile cover sheet, the following notice and disclaimer must appear in at least 10 point font:

**Confidentiality Notice:** This facsimile transmission is confidential and is intended only for the review of the party to whom it is addressed. It may contain proprietary and/or privileged information protected by law. If you are not the intended recipient, you may not use, copy or distribute this facsimile message or its attachments. If you have received this transmission in error, please immediately telephone the sender above to arrange for its return.

# **CREATING BACKUPS OF E-PHI POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires City of Washington EMS to back up and preserve all e-PHI created, received, used, and stored by City of Washington EMS in the event of an emergency or disaster. This policy outlines the procedures for preserving and protecting e-PHI and other important business information from tampering, theft, fire, flood, and other physical damage. Key to this process is the proper replication of exact copies of data in a secondary system so that if the primary system fails, the data will be completely preserved and accessible.

## **SCOPE**

This policy applies to all e-PHI created, received, maintained or transmitted by City of Washington EMS. Creating backups will be the responsibility of the manager in charge of the particular electronic equipment for his/her area of responsibility, in close coordination with the HIPAA Compliance Officer. This policy applies to all electronic equipment and devices that are used to create, receive, maintain or transmit e-PHI at City of Washington EMS. This policy applies to all staff members and vendors or contracted parties who are responsible for completing backups of City of Washington EMS's e-PHI.

## **PROCEDURE**

### *Physical Access Controls*

1. All backup systems will be located in a secure area, with limited access so that only those with responsibility for the backup system will have access to it.
2. Servers, backup drives and other data and information saving hardware will be located in a locked room.
3. Only authorized parties will have access to a physical location where backup devices are stored.

### *Backup Schedule*

1. Data and information stored on any computers or electronic devices will, at a minimum, be backed up at sufficient intervals to ensure that critical data (especially PHI) can be restored and recovered immediately. A full system backup will be completed at least monthly.
2. City of Washington EMS will verify that the backups are successfully completed at the end of each backup process to ensure that a complete replication of the data and information backed up has actually been created.

### *Backup Schedule Logs*

1. The backup software will capture a list of all files and directories encountered and saved. Logs will be maintained and will contain information about successful backups, unsuccessful backups, backup media that was left in place and overwritten, when and where the media was sent or transmitted off-site, the success or failure of restore tests and bad media encountered which may affect our ability to obtain files from a previous backup.

2. A primary and secondary staff member will be assigned to rotate the media used for backups if City of Washington EMS backs up e-PHI with physical media. This staff member will track the following information:
  - a. Whether the backup was successful;
  - b. Date and time the backup began and the date and time it was completed;
  - c. Description of any problems encountered during the backup; and
  - d. Verification that a check was made to ensure that the backup was complete.

#### *Marking and Storage of Backup Media*

1. All backup disks, drives, tapes or other physical backup media will be legibly and clearly marked with #'s 1, 2 and 3, and are rotated daily. The backups store the date and time they are created on the disks themselves.
2. All backup tapes, drives and other physical storage media will be stored in a secure vault to ensure the preservation of all but the most recent data and information in the event of a catastrophic fire, flood, or other damage to the primary backup location. City of Washington EMS may choose to contract with a reputable vendor to manage its backup process and media storage. In the event that a vendor is chosen, the vendor must execute a business associate agreement with City of Washington EMS to ensure that the vendor will, among other things, protect the integrity of the data stored and protect it from improper use or disclosure. Security access controls implemented at the off-site backup and storage location must meet or exceed the security access controls of the source systems. In other words, information security at any backup storage location must equal or exceed the security where the primary computers and servers are located.
3. City of Washington EMS may electronically backup PHI to a cloud server if City of Washington EMS obtains a business associate agreement from the server agency and all PHI is maintained in a manner that enables City of Washington EMS to meet its HIPAA compliance obligations.

#### *Data Retention*

1. Full system backups will be copied and/or archived.
2. Archived backups must be periodically tested to ensure that they are recoverable.

#### *Documentation*

The backup restore and recovery processes must be documented by the HIPAA Compliance Officer.

#### *Storage of Media Other Than Backups*

Old hard drives or other media storage devices that have been removed from the information system will be handled as follows:

1. If the device is to retain PHI, it will be stored in the same fashion as the backup devices.

2. If the device is to be taken out of service and no longer used to store PHI, it shall be "sanitized" and erased prior to disposal in accordance with City of Washington EMS's "Policy on Physical Security of PHI and e-PHI."

*Emergency Contact information*

City of Washington EMS will maintain a list of designated staff to be contacted in an emergency. A copy of this list will be kept in a secure location at the main facility and the off-site backup location (if applicable). The list must be kept up to date and readily accessible in case of an emergency. The list will also include vendor contact and support information and contacts for the off-site media storage location.

**EMERGENCY CONTACT LIST**

City Administrator Carl D. Chalfant, Cell phone: 785-220-4175

City Clerk Denise Powell, Home: 785-325-2400 Cell phone: 785-747-8534

City Treasurer Colleen Hillyer, Home: 785-325-2157 Cell phone: 785-541-0075

HIPAA Compliance Officer/Full Time EMT Caroline Scoville, Cell phone: 785-822-4591

Dague Computers & Engraving, Jennifer Dague Phone: 785-325-2858

CIC, Inc. 800-437-7457

Computer Solutions, Inc. 785-243-2621

# **ELECTRONIC INFORMATION SYSTEM ACTIVITY REVIEW AND AUDITING POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires City of Washington EMS to monitor and audit its electronic information system used to create, receive, maintain or transmit electronic protected health information ("e-PHI") so that quality assurance procedures will detect and address problems with the system. City of Washington EMS needs to identify the specific actions that have taken place such as timing and completion of back-up procedures, tracking server file access, and tracking power interruptions and other unusual events that could compromise our system and threaten the integrity of e-PHI.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who are responsible for monitoring and maintaining our electronic information system or are responsible for its security. The policy also applies to staff members assisting with the audit and review process. The HIPAA Compliance Officer shall have overall responsibility for monitoring, maintaining, and overseeing the security of our electronic information system and conducting audits.

## **PROCEDURE**

1. The HIPAA Compliance Officer will develop procedures to document the creation, receipt, maintenance and transmission of e-PHI within the information system.
2. The HIPAA Compliance Officer will review the records of information system activities, including a review of audit logs, security incident tracking reports, back-up records, etc., as necessary.
3. Uses and disclosures need not be documented for purposes of an audit trail if the use is made entirely within the internal information system and the use did not involve any outside parties.
4. Disclosures that are required to be accounted for under HIPAA shall be recorded and tracked. Generally all non-patient authorized disclosures that are not related to treatment, payment and healthcare operations will be accounted for. An accounting of these disclosures must include:
  - a. The date of the disclosure;
  - b. The name and address of the organization or person receiving the disclosure (if known);
  - c. A brief description of the PHI disclosed; and
  - d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.



# **ENCRYPTION OF E-PHI POLICY**

## **PURPOSE**

City of Washington EMS is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Security involves protection of e-PHI, PHI and other important Company information during its transmission and receipt via electronic means such as electronic mail and file, information, or software transfers. Encrypting and decrypting electronic information and files during their "transit" is a technical means of ensuring that if the information or files are intercepted or end up in the wrong hands, they cannot be deciphered or interpreted.

In effect, encryption turns the transmission into unique "gibberish" that transforms the electronic information or files into something that cannot be viewed in their original form unless it is decrypted at the receiving end. It is like attaching a unique "code" to that information so that it can only be accessed by those with the "de-coder."

While we are not legally required to "encrypt" electronic information or files in most cases, we are obligated to ensure that e-PHI, PHI, and other important patient or Company information does not fall into the wrong hands or is viewed or used by those who should not have access to it. Thus, it is the policy of City of Washington EMS to use encryption or decryption techniques wherever possible.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who are responsible for the manner in which e-PHI and other important Company information is transmitted or received by the Company.

## **PROCEDURE**

1. The HIPAA Compliance Officer will as part of a risk assessment identify all transmission and reception points for electronic information to determine:
  - a. Where the information is sent;
  - b. The type of information that is sent;
  - c. The general content of the information to determine if it contains e-PHI or other important or confidential information.
2. The HIPAA Compliance Officer in conjunction with management will then determine:
  - a. If the encryption and decryption of the information should be implemented based on the type of information, its destination (internal or external) and the risk of improper interception;
  - b. If it is feasible to implement encryption and decryption of the information after a review of the costs of implementation;
  - c. If implementation is not feasible, to document why it is not feasible;

- d. Establish other reasonable means to prevent the risk of improper access and use of e-PHI, PHI and other important confidential and company information if it should be intercepted by persons not authorized to receive it.
3. If encryption/decryption is implemented, a careful review of all available options will be completed by the Privacy/Information Security Officer, including a review of available technology, its features, and the ability to maintain and upgrade the software in the future.
4. As of the adoption of this policy, the information system network within the City of Washington EMS is password-protected; has access controls; facility controls; and very limited transmission of e-PHI on the network. E-PHI is transmitted directly through WPS Medicare bulletin board; through ASK's secure website, and through Medicaid's secure website.
  - a. Only the Full-Time EMT's pc in the City of Washington EMS business office actually stores e-PHI on it. The other computers on the network only have access to billing information which includes:
    - i. Patient name;
    - ii. Responsible party (if other than patient);
    - iii. Address;
    - iv. Invoice information which includes point of origin/dropoff, and loaded mileage.
  - b. A backup copy of the e-PHI is stored on the server, but is not accessible by any other machine on the network without the proper software installed.
5. At this point, encryption technology is not cost-effective.

## **ACCESS TO SERVER/TAPE BACKUP INFORMATION & EMERGENCY CONTACT INFORMATION**

Only the following individuals shall have access to the server containing City of Washington EMS proprietary, confidential and secure information:

1. City Clerk;
2. City Administrator.

Only the following individuals shall have access to and be responsible for ensuring the backup tape on the main server is changed daily to ensure proper back-up procedures:

1. City Treasurer;
2. City Clerk;
3. Full-Time EMT;
4. City Administrator.

Only the following individuals shall have access to the back-up disks for the electronic billing software containing City of Washington EMS proprietary, confidential and secure information:

1. Full-Time EMT;
2. City Clerk;
3. Full-Time EMT;
4. HIPAA Compliance Officer.

The following individuals shall be contacted in the event of emergency concerning computer information systems:

1. City Administrator Carl D. Chalfant Cell phone: 785-220-4175
2. City Clerk Denise Powell Home 785-325-2284 Cell phone: 785-747-8534
3. City Treasurer Colleen Hillyer Home: 785-325-2157 Cell phone: 785-541-0075
4. HIPAA Compliance Officer Caroline Scoville Home: 785-325-2407 Cell phone: 785-822-4591
5. Computer Information Concepts (Software vendor/support for backups) 800-437-7457
6. Dague Computers, computer support/professionals 785-325-2858
7. Computer Solutions, Inc. (Server support) 785-243-2621

# **ELECTRONIC INFORMATION SYSTEM ACTIVITY REVIEW AND AUDITING POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires City of Washington EMS to monitor and audit its electronic information system used to create, receive, maintain or transmit electronic protected health information ("e-PHI") so that quality assurance procedures will detect and address problems with the system. City of Washington EMS needs to identify the specific actions that have taken place such as timing and completion of back-up procedures, tracking server file access, and tracking power interruptions and other unusual events that could compromise our system and threaten the integrity of e-PHI.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who are responsible for monitoring and maintaining our electronic information system or are responsible for its security. The policy also applies to staff members assisting with the audit and review process. The HIPAA Compliance Officer shall have overall responsibility for monitoring, maintaining, and overseeing the security of our electronic information system and conducting audits.

## **PROCEDURE**

1. The HIPAA Compliance Officer will develop procedures to document the creation, receipt, maintenance and transmission of e-PHI within the information system.
2. The HIPAA Compliance Officer will review the records of information system activities, including a review of audit logs, security incident tracking reports, back-up records, etc., as necessary.
3. Uses and disclosures need not be documented for purposes of an audit trail if the use is made entirely within the internal information system and the use did not involve any outside parties.
4. Disclosures that are required to be accounted for under HIPAA shall be recorded and tracked. Generally all non-patient authorized disclosures that are not related to treatment, payment and healthcare operations will be accounted for. An accounting of these disclosures must include:
  - a. The date of the disclosure;
  - b. The name and address of the organization or person receiving the disclosure (if known);
  - c. A brief description of the PHI disclosed; and
    - i. brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

# **CONTINGENCY PLANNING POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires City of Washington EMS to implement a policy to ensure that we effectively protect the integrity of protected health information ("PHI") that we hold in the event of an emergency. This policy ensures that our response to an emergency or other occurrence that threatens or damages our computer, electronic, or other information systems is appropriate and provides for the contingencies necessary to protect and preserve PHI in accordance with HIPAA.

## **SCOPE**

This policy contains procedures for protecting the integrity of PHI (including e-PHI) and other essential patient information, billing and business information, and confidential information in the event of an emergency or other occurrence (i.e., fire, vandalism, system failure and natural disaster). The HIPAA Compliance Officer shall oversee the implementation of these procedures.

## **PROCEDURE**

### *Applications and Data Criticality Analysis*

1. City of Washington EMS will assess the relative criticality of specific applications and data within the company for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.
2. The assessment of data and application criticality should be conducted periodically and at least annually as part of the Security Risk Analysis to ensure that appropriate procedures are in place for data and applications at each level of risk.

### *Data Backup Plan*

1. The City of Washington EMS will establish and implement a Data Backup Plan that ensures that City of Washington EMS will create and maintain retrievable exact copies of all PHI and other essential business information that is at a medium to high risk for destruction or disruption.
2. The Data Backup Plan must apply to all medium and high risk files, records, images, voice or video files that may contain PHI and other essential business information.
3. The Data Backup Plan must require that all media used for backing up PHI and other essential business information be stored in a physically secure environment. Where backup media remains on site, it will be kept in a physically secure location, different from the location of the computer systems which have been backed up.
4. If an off-site storage facility or backup service is used, a written Business Associate Agreement must be entered into with the outside party maintaining the data to ensure that the Business Associate will safeguard any PHI and other essential business information in an appropriate manner.
5. Data backup procedures and contingency plan shall be tested on a periodic basis to ensure that exact copies of PHI and other essential business information can be retrieved and made available whenever it is needed.

6. The HIPAA Compliance Officer will ensure that each functional area of the Company with medium and high risk to PHI has an appropriate Data Backup Plan in place.

#### *Disaster Recovery Plan*

1. To ensure that each functional area of City of Washington EMS can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting information systems containing PHI or other essential business information, each functional area will establish and implement a Disaster Recovery Plan.
2. The Plan must ensure that each area can restore or recover any loss of this information and the systems needed to make that information available in a timely manner.
3. The Disaster Recovery Plan will include procedures to restore PHI and other essential business information from data backups in the case of a disaster causing data loss.
4. The Disaster Recovery Plan will include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.
5. The Disaster Recovery Plan must be documented and easily available to the necessary personnel at all time, who should be trained to implement the Disaster Recovery Plan.
6. The disaster recovery procedures outlined in the Disaster Recovery Plan must be tested on a periodic basis to ensure that PHI and other essential business information and the systems needed to make e-PHI available can be fully restored or recovered.
7. The HIPAA Compliance Officer will ensure that each functional area of the Company with medium and high risk to PHI has an appropriate Disaster Recovery Plan in place.

#### *Emergency Mode Operation Plan*

1. Each functional area of City of Washington EMS must establish and implement (as needed) procedures to enable continuation of administrative, patient care, and billing and business processes for protection of the security of PHI and other essential business information while operating in emergency mode.
2. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan must be tested periodically to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.
3. The HIPAA Compliance Officer will ensure that each functional area of the Company with medium and high risk to PHI has an appropriate Emergency Mode Operation Plan in place.

# **DISASTER MANAGEMENT AND RECOVERY OF E-PHI POLICY**

## **PURPOSE**

City of Washington EMS is responsible under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") for ensuring that we have a process in place to ensure that we can recover from the catastrophic disruption of our information system and loss of any data or information, especially electronic protected health information ("e-PHI"), which may be stored on that system. This policy will be followed in an emergency situation such as or disaster such as fire, vandalism, terrorism, system failure, or natural disaster.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It is intended to cover all information system hardware, software and operational procedures. The HIPAA Compliance Officer shall be the primary party in charge of disaster management and recovery.

## **PROCEDURE**

To ensure that City of Washington EMS will be able to recover from a serious information system disruption, including situations that could lead to the loss of data in the event of an emergency or disaster (such as fire, vandalism, terrorism, system failure, or natural disaster) the following procedures are established:

1. A disaster recovery plan will be established and implemented to restore or recover any loss of e-PHI and any loss or disruption to the systems required to make e-PHI available.
2. The disaster recovery plan will be developed by staff members responsible for the maintenance of the security and integrity of the information system and will be reviewed and approved by the HIPAA Compliance Officer and senior management.
3. The disaster recovery plan must include:
  - a. A data backup plan including the storage location of backup media;
  - b. Procedures to restore e-PHI from data backups in the case of an emergency or disaster that results in a loss of critical data;
  - c. Procedures to ensure the continuation of business critical functions and processes for the protection of e-PHI during emergency or disaster situations;
  - d. Procedures to periodically test data backup and disaster recovery plans;
  - e. Procedures to periodically perform an application and data criticality analysis establishing the specific applications and e-PHI that is necessary to maintain operation in an emergency mode;
  - f. Procedures to log system outages, failures, and data loss to critical systems;
  - g. Procedures to train the appropriate personnel to implement the disaster recovery plan;
  - h. The disaster recovery plan must be documented and easily available to the necessary personnel at all times.

## ACCESS LOG TO SECURE AREAS

NAME (PRINT)	TIME IN	TIME OUT	PURPOSE FOR ACCESS	SIGNATURE



# **SECURITY INCIDENT MANAGEMENT POLICY**

## **PURPOSE**

The Health Insurance Portability and Accountability Act ("HIPAA") requires City of Washington EMS to track and appropriately respond to all incidents that could compromise our electronic protected health information ("e-PHI"). This policy establishes City of Washington EMS's procedures for reporting a security incident and the steps that will be taken by City of Washington EMS to investigate and take action when a potential or actual security incident occurs.

## **SCOPE**

This policy applies to all City of Washington EMS staff members who utilize the electronic information system. Everyone at City of Washington EMS is responsible to know what to do when confronted with a security incident. The Security/Breach Incident Reporting Form should be used in conjunction with this policy.

## **PROCEDURE**

### *Security Incident Defined*

A "security incident" is an attempted or successful unauthorized entry, breach or attack on the electronic information system that we use to create, receive, maintain or transmit e-PHI. Security incidents include unauthorized probing and browsing of the files, a disruption of service in our information system and incidents where e-PHI has been improperly altered or destroyed. Security incidents also include things such as a virus, hacking attempt or incident, "phishing" incident, malware installation, corrupt data or other similar incident involving City of Washington EMS's information system.

### *Reporting a Security Incident*

1. All staff members are responsible for immediately reporting a suspected security incident to the HIPAA Compliance Officer or an immediate supervisor.
2. When a suspected security incident occurs, the HIPAA Compliance Officer shall have the reporting staff member and other members with knowledge of the incident complete City of Washington EMS's "Internal Breach/Security Incident Reporting Form."
3. The HIPAA Compliance Officer will be responsible for initiating an immediate investigation to isolate the problem and take whatever action is necessary to protect the information system and e-PHI and other vital electronic information.
4. The HIPAA Compliance Officer will notify management immediately in the event the incident cannot be immediately corrected, or if any e-PHI or other vital information is altered or destroyed. Management will also be notified of any completed investigation and the outcome of the investigation.
5. In the event of unlawful activity via the use of City of Washington EMS's information system, local, state, or federal law enforcement may be notified. That determination will be made by management with recommendation from the HIPAA Compliance Officer. The HIPAA Compliance Officer is responsible for coordinating communications with outside organizations and law enforcement.

6. Whenever a security incident is suspected or confirmed to have occurred, remedial action will be taken, including action against any individual staff members when it has been confirmed that they caused or contributed to the incident.

#### *HIPAA Compliance Officer Responsibility*

The HIPAA Compliance Officer is responsible for the following:

1. Initiating the appropriate incident management action, including restoration.
2. Determining the physical and electronic evidence to be gathered as part of the incident investigation.
3. Monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
4. Determining if a widespread communication is required, the content of the communication, and how best to distribute the communication.
5. Communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
6. Initiating, completing, and documenting the incident investigation.
7. Determining whether the incident may qualify as a breach of unsecured PHI requiring breach notification under City of Washington EMS's "Policy on Breaches of Unsecured Protected Health Information."

# **BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION POLICY**

## **PURPOSE**

Under the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") City of Washington EMS has an obligation, following the discovery of a breach of unsecured protected health information ("PHI"), to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed. City of Washington EMS also has an obligation to notify the Department of Health and Human Services ("HHS") of all breaches. In some cases, City of Washington EMS must notify media outlets about breaches of unsecured PHI. This policy details how City of Washington EMS will handle and respond to suspected and actual breaches of unsecured PHI.

## **SCOPE**

This Policy applies to all City of Washington EMS staff members who come into contact with PHI. All suspected breach incidents shall be brought to the attention of the HIPAA Compliance Officer and the HIPAA Compliance Officer shall investigate each incident and initiate the appropriate response to the incident.

## **PROCEDURE**

### *Breach Defined*

1. A breach is 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 the PHI.
  - a. An acquisition, access, use, or disclosure of PHI created, received, maintained or transmitted by City of Washington EMS that is not permitted by HIPAA is presumed to be a breach unless City of Washington EMS demonstrates that there is a low probability that the PHI has been compromised based on a "risk assessment" of at least the following factors:
    - i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    - ii. The unauthorized person who used the PHI or to whom the disclosure was made;
    - iii. Whether the PHI was actually acquired or viewed; and
    - iv. The extent to which the risk to the PHI has been mitigated.
  - b. "Unsecured protected health Information" is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS for securing PHI - available on HHS's website at: <http://www.hhs.gov/ocr/privacy>. Generally, PHI is "unsecured" if it is not encrypted by strong encryption technology or if it has not been properly destroyed. If the PHI is able to be used, read, or deciphered it is "unsecured."
2. A breach does not include any of the following:

- a. Unintentional acquisition, access, or use of unsecured PHI by a staff member at City of Washington EMS or someone acting under the authority of City of Washington EMS if the acquisition, access, or use was made in good faith and within that individual's scope of authority, so long as the information was not further used or disclosed in violation of HIPAA.
- b. Any inadvertent disclosure of PHI by a City of Washington EMS staff member who is generally authorized to access PHI to another person at City of Washington EMS who is generally authorized to access PHI, so long as the information received as a result of such disclosure was not further used or disclosed in violation of HIPAA.
- c. A disclosure of PHI where City of Washington EMS has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

#### *Reporting a Suspected Breach Incident*

1. All City of Washington EMS staff members are responsible for immediately reporting a suspected breach incident to a supervisor or the HIPAA Compliance Officer. City of Washington EMS staff members shall report all known and suspected HIPAA violations.
2. The HIPAA Compliance Officer will notify management about the suspected incident.
3. The HIPAA Compliance Officer shall document the date that the suspected breach of unsecured PHI occurred (if known) and the date(s) on which the supervisor and the HIPAA Compliance Officer were notified about the incident.

#### *Investigating a Suspected Breach Incident*

1. The HIPAA Compliance Officer shall then initiate an investigation to determine whether an actual breach has occurred and what actions, if any, are necessary.
2. The HIPAA Compliance Officer shall interview all necessary parties who may have information about the incident. The staff member who reported the suspected incident and other members with knowledge of the incident should be asked to complete City of Washington EMS's "Internal Breach Incident Reporting Form." Staff members should be required to convey all information that they know about the incident and to cooperate in any subsequent investigation regarding the incident.
3. After gathering all available information about the incident, the HIPAA Compliance Officer shall conduct an analysis to determine whether an actual breach of unsecured PHI occurred. City of Washington EMS shall consult with legal counsel whenever necessary in making this determination. The HIPAA Compliance Officer shall utilize City of Washington EMS's "HIPAA Compliance Officer Action Plan: Breach Analysis Steps" in making this determination.
4. If the Compliance Officer determines that a breach of unsecured PHI has **not** occurred, the reasons behind that conclusion shall be thoroughly documented.

5. If the HIPAA Compliance Officer determines that a breach of unsecured PHI has occurred, the reasons behind that conclusion shall be thoroughly documented and the HIPAA Compliance Officer shall proceed to notify all necessary parties in accordance with this policy.

*Breach Notification to Affected Individuals*

1. Following the discovery of a breach of unsecured PHI, City of Washington EMS will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach. The HIPAA Compliance Officer shall be the party who is primarily responsible to make proper notice, in consultation with City of Washington EMS management.
2. A breach shall be treated as discovered by City of Washington EMS as of the first day on which the breach is known, or, by exercising reasonable diligence would have been known to City of Washington EMS or any person, other than the person committing the breach, who is a staff member or agent of City of Washington EMS.
3. City of Washington EMS shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
4. If a law enforcement official states to City of Washington EMS that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, City of Washington EMS shall:
  - a. Delay notification for the time period specified by the official if the statement is in writing and specifies the time for which a delay is required; or
  - b. If the notice is a verbal statement, delay notification temporarily, and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time. If the statement is made orally, the HIPAA Compliance Officer shall document the statement, including the identity of the official making the statement.
5. City of Washington EMS shall provide written notification, in plain language, by first-class mail to each affected individual at the last known address of each individual. If the affected individual agreed to receive electronic notice of breaches, City of Washington EMS may provide notice by electronic mail. The notification may be provided in one or more mailings as information becomes available.
6. The HIPAA Compliance Officer shall utilize City of Washington EMS's "Individual Notice of Breach of Unsecured PHI" when sending notice to affected parties. The Notice shall include, to the extent possible:
  - 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 types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, or other types of information were involved);
  - c. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

- d. A brief description of what City of Washington EMS is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
  - e. Contact procedures for individuals to ask questions or learn additional information about the incident from City of Washington EMS. These contract procedures shall include a toll-free telephone number and an e-mail address to reach City of Washington EMS's HIPAA Compliance Officer.
7. If the HIPAA Compliance Officer determines that affected individuals need to be contacted immediately to protect them from potential harm, the HIPAA Compliance Officer shall contact those individuals by telephone or other means as soon as possible. City of Washington EMS shall still send written notice to these individuals about the incident.
  8. If City of Washington EMS knows that any affected individual is deceased and City of Washington EMS has the address of the next of kin or personal representative of the individual, City of Washington EMS shall provide written notification by first class mail to either the next of kin or personal representative.
  9. If City of Washington EMS has insufficient or out-of-date contact information for any affected individuals, City of Washington EMS shall use a substitute form of notice that, in the informed opinion of the HIPAA Compliance Officer, will reach the individual. Substitute notice is not required in cases where there is insufficient or out-of-date contact information for the next of kin or personal representative of a deceased individual. Substitute notice will be provided in the following manner:
    - a. If there is insufficient or out-of-date contact information for fewer than 10 affected individuals, then substitute notice may be provided by an alternative form of written notice such as placing a notice in the newspaper, calling the patient, or other means.
    - b. If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall: (i) be conspicuously posted on City of Washington EMS's home page of its website for 90 days, or conspicuous notice in major print or broadcast media in geographic areas where each affected individual likely resides; and (ii) include a toll-free phone number for City of Washington EMS that remains active for at least 90 days where individuals can learn whether their unsecured PHI may be included in the breach.

#### *Breach Notification to the Media*

1. For a breach of unsecured PHI involving more than 500 residents of a single state or jurisdiction, City of Washington EMS shall notify prominent media outlets serving the state or jurisdiction about the breach. The HIPAA Compliance Officer shall be the party in charge of making such notice and shall make such notification in consultation with City of Washington EMS management and legal counsel.
2. Notification to the media shall be made without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.
3. Notification to the media shall include all information that must be included in individual notice.

#### *Breach Notification to HHS*

1. City of Washington EMS shall notify HHS of all breaches of unsecured PHI in accordance with this policy.
  - a. For breaches of unsecured PHI involving 500 or more individuals, City of Washington EMS shall provide notice to HHS when it provides notice to affected individuals. Notice must be provided in the manner specified on the HHS Website at: <http://www.hhs.gov/ocr/privacy/HIPAA/administrative/breachnotificationrule/>. The HIPAA Compliance Officer shall be responsible for ensuring that such notice is submitted to HHS and must consult management before submitting the information to HHS.
  - b. For breaches of unsecured PHI involving less than 500 individuals, City of Washington EMS shall maintain a log of such breaches and report them to HHS on an annual basis. The HIPAA Compliance Officer shall track these breaches on City of Washington EMS's "Log for Tracking Breach Incidents." The HIPAA Compliance Officer shall report these breaches to HHS annually, no later than 60 days after the end of the calendar year in which these breaches were discovered. This shall be done in the manner specified on the HHS Website at: <http://www.hhs.gov/ocr/privacy/HIPAA/administrative/breachnotificationrule/>. The HIPAA Compliance Officer shall ensure that the information is submitted to HHS by March 1 of each year and must consult with management before submitting the information to HHS.

*Breach Notification in Accordance with State Law*

1. The HIPAA Compliance Officer shall also determine, in consultation with legal counsel, whether City of Washington EMS has any additional breach notification obligations under applicable Kansas laws or other state laws.
2. City of Washington EMS must look to each state in which an affected individual resides when making this determination and shall consult legal counsel licensed to practice in those states.

*Administrative Requirements*

1. The HIPAA Compliance Officer shall record and maintain thorough records of all activities related to suspected and actual breach incidents.
2. In the event of a suspected crime, or other unlawful activity, local, state, or federal law enforcement may need to be notified. That determination will be made by management with recommendation from the HIPAA Compliance Officer. The HIPAA Compliance Officer shall coordinate communications with outside organizations and law enforcement.
3. City of Washington EMS will train all members of its staff so that they are able to identify suspected breaches of unsecured PHI and know to report all suspected breaches to the appropriate party immediately.
4. Staff members who violate this policy will be subject to disciplinary action, up to and including termination.

**INTERNAL BREACH/SECURITY INCIDENT REPORTING FORM**

All personnel must report all known and suspected breaches of unsecured PHI and all security incidents immediately to the HIPAA Compliance Officer. If an incident occurs, or is suspected to have occurred, the staff member with knowledge of the incident must complete this form to the best of his/her knowledge and provide as much detail about the incident as possible. The staff member will also be expected to participate in any subsequent investigation of the incident and to provide additional details as they become available.

Date of Discovery of Incident: \_\_\_\_\_ Date of Report: \_\_\_\_\_

Complete Description of Incident (please include date, time, patients affected, parties involved, whether any hardware or devices were involved and any other details):

---

---

---

---

---

---

---

Your Name and Title: \_\_\_\_\_

Signature: \_\_\_\_\_



# LOG FOR TRACKING BREACH INCIDENTS

(To be completed by HIPAA Compliance Officer)

Date of Incident	Date of Discovery	Description of Breach Incident	Type of Unsecured PHI Involved in Breach (SSN, DOB, etc.)	Names of Affected Individuals	Date of Individual Notice	Date of Notice to HHS	Date of Media Notice (if Applicable)

## INDIVIDUAL NOTICE OF BREACH OF UNSECURED PHI

Date:

Via First Class Mail

[INSERT NAME OF AFFECTED INDIVIDUAL]

[INSERT LAST KNOWN ADDRESS FOR AFFECTED INDIVIDUAL]

Re: [Suspected] Breach of Your Protected Health Information

Dear [INSERT NAME OF AFFECTED PARTY]:

City of Washington EMS is committed to patient privacy and we strive to protect the confidentiality of our patients' healthcare information. We take steps to quickly identify and immediately address all known or suspected breaches of your healthcare information.

City of Washington EMS [believes] [has information] that your health information [may have been] [was] improperly [accessed, used, disclosed]. Therefore, we are providing this notice to you so that you are aware of and informed about the incident, and so that you can take any further steps that may be necessary to protect your health information.

**Provide a brief description of what happened, including the date of the breach and the date City of Washington EMS discovered the breach.** *Example:* It was brought to our attention that on April 3, 2014 one of our employees accessed your electronic patient file for non business-related reasons and without authorization. We discovered this on April 5, 2014.]

**[Give a brief, generic description of the types of unsecured PHI that were involved in the incident such as: full name, SSN, DOB, home address, account number, condition, etc.** *Example:* The file that was breached contained your home address, your Medicare identification number, your healthcare condition, and your date of birth.]

**[Explain any steps that the individual should take to protect themselves from potential harm from the breach.** *Example:* We recommend that you carefully monitor explanations of benefits (EOBs) or other remittance advice or account statements received from your health insurer to determine if any other person has used your identity to obtain health care. If you receive an EOB or bill for health care services that you believe you did not receive, immediately contact your insurer and the health care provider who furnished the services.]

**[Briefly explain what City of Washington EMS is doing or has done to investigate the breach, to mitigate harm to the individual, and to protect against further breaches.** *Example:* City of Washington EMS has spoken with the employee to ascertain what information was accessed and retained while viewing your file. We also audited access and download logs for that computer to determine whether other unauthorized parties could have gained access to your information and whether any patient information was extracted from the computer. We found no activity that indicates that any other party accessed your information.]

**[Provide contact procedures for the individual to ask questions or learn additional information, including either: a toll-free telephone number, an email address, website, or postal address.** *Example:* We encourage

you to contact us at 785-325-2284 and ask to speak with our HIPAA Compliance Officer, Caroline Scoville, for more information about this incident. We are happy to answer your questions or to provide you with any additional information that you might require.

We sincerely regret any inconvenience that this incident has caused and we have taken all appropriate steps to ensure that your health information is protected and that a similar incident does not happen in the future. We value your trust in City of Washington EMS and we consider patient privacy a top priority. If there is anything we can do to assist you, please contact us at the toll-free number above.

Sincerely,

Caroline Scoville  
HIPAA Compliance Officer  
City of Washington EMS

## ACTION PLAN: BREACH ANALYSIS STEPS

<p><u>Step 1:</u> Was there an acquisition, access, use or disclosure of PHI that was created, received, maintained, or transmitted by City of Washington EMS? The HIPAA Compliance Officer shall determine whether PHI was actually involved in the incident, keeping in mind that PHI only includes individually identifiable information that relates to an individual's healthcare or payment for healthcare.</p>	<p>YES  Go to Step 2</p>	<p>NO  There has been no breach of unsecured PHI and breach notification is unnecessary.</p>				
<p><u>Step 2:</u> Was the PHI involved in the incident "unsecured?" PHI involved in an incident will be considered to be "unsecured" when it is in electronic form and it is <u>not</u> encrypted in accordance with City of Washington EMS's "Policy on Encryption and Decryption of e-PHI."</p>	<p>YES  Go to Step 3</p>	<p>NO If the HIPAA Compliance Officer determines that the PHI involved in the incident was secured in accordance with City of Washington EMS's policies on securing hard copy and electronic PHI, then there has been no breach of unsecured PHI and breach notification is unnecessary.</p>				
<p><u>Step 3:</u> Was there a HIPAA violation? The HIPAA Compliance Officer must make a determination that there was a violation of the HIPAA Privacy Rule. The incident must involve a use or disclosure that is not permitted by HIPAA.</p>	<p>YES  Go to Step 4</p>	<p>NO  There has been no breach of unsecured PHI and breach notification is unnecessary.</p>				
<p><u>Step 4:</u> Did the incident compromise the security or privacy of the PHI involved? To determine whether the incident compromised the security or privacy of the PHI that was potentially breached, the HIPAA Compliance Officer must look to the 4-factors outlined below:</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; border-bottom: 1px solid black; width: 15%;"><u>Factor</u></th> <th style="text-align: left; border-bottom: 1px solid black;"><u>Explanation</u></th> </tr> </thead> <tbody> <tr> <td style="vertical-align: top;">1. The nature and extent of the PHI involved</td> <td style="vertical-align: top;">Consider the type and amount of involved and whether the inci the PHI involved sensitive information. example, credit card numbers, s security numbers, or other informa that could be used for identity the financial fraud more I compromises the security information. The same is true clinical information, especially det clinical information (e.g., treatn</td> </tr> </tbody> </table>	<u>Factor</u>	<u>Explanation</u>	1. The nature and extent of the PHI involved	Consider the type and amount of involved and whether the inci the PHI involved sensitive information. example, credit card numbers, s security numbers, or other informa that could be used for identity the financial fraud more I compromises the security information. The same is true clinical information, especially det clinical information (e.g., treatn	<p>Yes  Go to Step 5</p>	<p>NO  There has been no breach of unsecured PHI and breach notification is unnecessary.</p>
<u>Factor</u>	<u>Explanation</u>					
1. The nature and extent of the PHI involved	Consider the type and amount of involved and whether the inci the PHI involved sensitive information. example, credit card numbers, s security numbers, or other informa that could be used for identity the financial fraud more I compromises the security information. The same is true clinical information, especially det clinical information (e.g., treatn					

<p>medication, medical his information, etc.).</p> <p>2. The person who used the PHI or to whom the disclosure was made</p> <p>3. Whether the PHI was actually acquired or viewed</p> <p>4. The extent to which the risk to the PHI has been mitigated</p>	<p>Consider whether the person received the information obligations to protect the informa For example, other covered entities obligated to protect PHI that receive in the same manner as Ci Washington EMS.</p> <p>Determine whether the improv disclosed PHI was returned be being accessed for an impr purpose.</p> <p>Consider whether immediate s were taken to mitigate the pote harm from the improper use disclosure of the PHI.</p>	
<p><u>Step Five:</u> Does a breach exception apply? The HIPAA Compliance Officer must also determine whether one of the breach exceptions outlined in the Breach Notification Rule applies to the incident. If so, there is no reportable breach. The three breach exceptions are:</p> <ul style="list-style-type: none"> <li>• Unintentional Access, Acquisition or Use of PHI. The incident involved <i>unintentional</i> access, acquisition or use of PHI by a workforce member of City of Washington EMS or someone acting under the authority of City of Washington EMS. The unintentional incident must: (1) be made in good faith; (2) made within the scope of employment; and (3) not result in further improper use or disclosure of PHI.</li> <li>• Inadvertent Disclosure to an Authorized Party. Inadvertent disclosure between parties at City of Washington EMS who are authorized to access PHI is <u>not</u> a breach if the PHI is not further used or disclosed in violation of HIPAA. "Authorized to access PHI" means that the two parties involved in the incident are authorized to access PHI <i>in general</i> - not necessarily that they are authorized to access the same type of PHI.</li> </ul>	<p>Yes</p> <p>City of Washingt on EMS does not have to make breach notificatio n.</p>	<p>NO</p> <p>City of Washington EMS must make breach notification in accordance with City of Washington EMS's "Policy on Breaches of Unsecured Protected Health Information."</p>

<ul style="list-style-type: none"><li>• Disclosure Where Retention Was Not Possible. If the HIPAA Compliance Officer can demonstrate that an unauthorized recipient of the improperly disclosed PHI would not reasonably have been able to retain the PHI, this breach exception applies.</li></ul>		
---	--	--



## **CONTRACTING WITH BUSINESS ASSOCIATES POLICY**

### **PURPOSE**

City of Washington EMS is responsible for ensuring the privacy and security of all protected health information ("PHI") that we create, receive, maintain or transmit under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA requires that City of Washington EMS ensure that those persons and entities that perform services on our behalf using PHI agree to protect that PHI as we would by requiring those parties to sign a "business associate agreement" ("BAA") with City of Washington EMS. This policy describes our approach to entering into business associate agreements with persons and organizations that perform services on our behalf involving the use of PHI.

### **SCOPE**

This policy applies to all City of Washington EMS staff members who are responsible for entering into agreements with outside vendors or persons who might have access to PHI. Generally, the HIPAA Compliance Officer of City of Washington EMS is responsible to initiate a business associate agreement with any person or entity that performs a service on behalf of City of Washington EMS that involves the use or disclosure of PHI.

### **PROCEDURE**

1. The HIPAA Compliance Officer is responsible for identifying persons and organizations that perform services on our behalf and who in any manner create, receive, maintain or transmit PHI about our patients. All such persons or entities are called "business associates" ("BAs") of City of Washington EMS. For example, our business associates include, but are not limited to, our outside billing company, our outside consultants, and our outside attorney. Workforce members are not business associates, nor are organizations that share a direct treatment relationship with patients to whom City of Washington EMS provides services. When in doubt, the HIPAA Compliance Officer should consult qualified legal counsel when determining whether an entity meets the legal definition of a BA.
2. All identified BAs of City of Washington EMS must enter into a BAA if they wish to do business with us. Even if we do not have a written services contract with a party, HIPAA requires that we have a written business associate agreement with all BAs. No disclosures of PHI will be made by City of Washington EMS to a BA until the BAA has been signed.
3. Whenever possible, City of Washington EMS will use its standard business associate agreement. If the BA insists on using its own business associate agreement, the HIPAA Compliance Officer must ensure that the agreement proposed by the BA conforms to HIPAA's requirements.
4. Whenever City of Washington EMS modifies its existing business associate agreement, the HIPAA Compliance Officer shall ensure that we enter into a new business associate agreement with our current BAs.
5. Whenever possible, all contracts and service agreements between City of Washington EMS and any BA should include the relevant business associate language directly in the contract or service agreement. Otherwise, a stand-alone business associate agreement is required. If there is a business associate agreement separate from the main contract or service agreement, then the main agreement must specifically refer to the business associate agreement.

6. The HIPAA Compliance Officer will maintain a current list of business associates.
7. At times, City of Washington EMS may be asked to enter into business associate agreements. The HIPAA Compliance Officer shall evaluate the appropriateness of the business associate agreement under the circumstances and enter into the agreement only when required by law and if the agreement meets the legal requirements under HIPAA.
8. The HIPAA Compliance Officer is responsible for maintaining BA agreements on file for periodic review and inspection.
9. With respect to a person or entity that is not a BA, but which may potentially come into contact with PHI, such as janitorial services or information technology service providers, the HIPAA Compliance Officer should seek to have a "Confidentiality Agreement" in place with the entity.



## **CITY OF WASHINGTON EMS BUSINESS ASSOCIATE LIST**

The City of Washington EMS has Business Associate Agreements in place with the following individuals/companies:

1. Computer Information Concepts. Software vendor/support. *Date signed:* \_\_\_\_\_
2. Clubine & Rettele, Chartered. Accounting & consulting firm/services. *Date signed:* \_\_\_\_\_
3. Dague Computers. Computer sales, service, repairs, maintenance. *Date signed:* \_\_\_\_\_
4. Dr. David K. Hodgson, M.D. Medical Director. *Date signed:* \_\_\_\_\_
5. 911 Communications Center. Dispatch services. *Date signed:* \_\_\_\_\_
6. The Law Office of Elizabeth Baskerville Hiltgen. Law Services. *Date signed:* \_\_\_\_\_
7. Credit Management. Debt collection services. *Date signed:* \_\_\_\_\_
8. Federal Payments. Electronic payments. *Date signed:* \_\_\_\_\_
9. Computer Solutions, Inc. Computer technical/service support. *Date signed:* \_\_\_\_\_
10. Administrative Services of Kansas (ASK), Inc. Software vendor, electronic trading partner. *Date signed:*  
4/16/2003

The City of Washington EMS has included in its HIPAA compliance plan policies and procedures which do not allow for the electronic sharing of or transmitting of any protected health information (PHI) by email or in any electronic form other than with the Administrative Services of Kansas (ASK), Inc, a software vendor which transmits our files to the correct insurance carrier. The Business Associate Agreement (also known as Trading Partner Agreement) that we have on file with this company dated April 16, 2003, details privacy and security measures and how each party shall strive to maintain confidentiality and security of any and all PHI it maintains or receives from the other party. This list shall be reviewed on a regular basis, and in the event that any new vendors or business associates are identified, a business associate agreement shall be prepared and signed with the appropriate applicable language to comply with both the Privacy and Security regulations.

**GUEST/TRAINEE CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT**

I, \_\_\_\_\_, acknowledge that patients provide and City of Washington EMS collects personal, confidential information verbally, in writing, and through digital means. I understand and agree that any information pertaining to patients is strictly confidential and protected by federal and state laws and that I will not use or disclose patient information in any way, unless City of Washington EMS authorizes me to do so.

I agree that I will comply with all HIPAA policies and procedures in place at City of Washington EMS during my experience as a guest/trainee with City of Washington EMS. If at any time I knowingly or inadvertently breach patient confidentiality or violate the HIPAA policies and procedures of City of Washington EMS, I agree to notify City of Washington EMS immediately.

I also understand that I may be exposed to other confidential or proprietary information of City of Washington EMS and I agree not to reveal any of that information to anyone at any time, unless I am authorized by City of Washington EMS to do so. This means that I will not disclose information about City of Washington EMS's business practices or other information that City of Washington EMS might consider to be confidential or proprietary.

Failure to uphold these obligations may result in immediate suspension or termination of the privilege to gain clinical experience or observe the activities of City of Washington EMS. Upon termination of this privilege for any reason, or at any time upon request, I agree to return any and all patient information or confidential or proprietary information in my possession. I understand that any patient or confidential information that I see or hear while a guest/trainee will stay here at City of Washington EMS when I leave.

I have been given an overview of City of Washington EMS's HIPAA policies and procedures and have been given access to review those policies and I agree to abide by them.

*Print Name:* \_\_\_\_\_

*Signature:* \_\_\_\_\_ *Date:* \_\_\_\_\_

**STUDENT/GUEST/TRAINEE ACKNOWLEDGEMENT AND RELEASE FORM**

I hereby acknowledge that I am riding on a City of Washington EMS ambulance voluntarily as part of an educational or observer program. I further acknowledge that City of Washington EMS ambulances respond to emergency situations that could expose me to certain hazards, which I might not otherwise encounter.

I agree to release, and hold harmless, City of Washington, Kansas, from and against any claims for loss which may arise from my participation in this program, whether for property damage, personal injury, or other loss of casualty.

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature

## **STAFF MEMBER HIPAA ASSURANCES**

I agree that I will comply with all of City of Washington EMS's HIPAA policies and procedures during my entire employment or association with City of Washington EMS. If I at any time knowingly or inadvertently breach the policies and procedures, or witness someone else doing so, I agree to notify the HIPAA Compliance Officer of City of Washington EMS immediately.

In addition, I understand that a breach of patient confidentiality, City of Washington EMS's HIPAA policies and procedures, or of these assurances may result in disciplinary action up to and including termination of my employment or association with City of Washington EMS. Upon termination of my employment or association for any reason, or at any time upon request, I agree to return any and all patient confidential information in my possession, as well as any devices, hardware, or software issued to me by City of Washington EMS.

I understand that all hardware, software and other devices owned by City of Washington EMS are the sole property of City of Washington EMS and that I only have the right to use the equipment for legitimate company purposes for which I am authorized. If I utilize a password to access any hardware, software, or other devices owned by City of Washington EMS, I will provide that password to the HIPAA Compliance Officer upon request. With respect to any device issued to me by City of Washington EMS, I agree to:

1. Protect all data on the device in accordance with all company policies and procedures and not permit unauthorized use or access to data on the device;
2. Permit City of Washington EMS to configure and install security software on the device and not modify or delete that software;
3. Permit City of Washington EMS to remotely wipe the device whenever City of Washington EMS deems such action necessary;
4. Permit City of Washington EMS to monitor the device when permitted by law to do so;
5. Allow City of Washington EMS to inspect the device when City of Washington EMS has a legitimate business need to do so;
6. Hold City of Washington EMS harmless if the device is damaged and/or my personal data is viewed or deleted;
7. Immediately report any loss of the device and any improper use or access to data on the device; and
8. Limit storage of data to work-related information, in accordance with City of Washington EMS policies and procedures.

I further understand that upon termination of my employment or association with City of Washington EMS for any reason, City of Washington EMS will terminate my access to its equipment and facilities.

I have read and understand the HIPAA policies and procedures that have been provided to me by City of Washington EMS. I agree to abide by all policies or be subject to disciplinary action up to and including termination of employment or of any membership or association with City of Washington EMS. This is not a contract of employment and does not alter the nature of the existing relationship between City of Washington EMS and me.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Name: \_\_\_\_\_

## STAFF MEMBER TERMINATION CHECKLIST

This checklist shall be completed by the HIPAA Compliance Officer upon the termination of a staff member for any reason – whether voluntary or involuntary.

Name of Staff Member: \_\_\_\_\_

Date of Termination: \_\_\_\_\_ Position: \_\_\_\_\_

Item	Date Completed	Initials
Network access terminated		
Network user account deactivated		
ePCR system access terminated		
Keys to buildings and ambulances returned		
All company hardware and devices returned		
Access codes to building deactivated		
All paper and digital PHI returned		
Remote access terminated		
[Insert additional items as necessary]		

HIPAA Compliance Officer Signature: \_\_\_\_\_

Date: \_\_\_\_\_

<b>SUBJECT IDENTITY THEFT PREVENTION POLICY</b>	<b>ISSUED BY CITY COUNCIL</b>	<b>EFFECTIVE DATE SEPTEMBER 3, 2013</b>
---	-----------------------------------	---

**POLICY STATEMENT:**

**PURPOSE:**

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, measures to respond to such events, and methods to safeguard personal customer information.

**CONTACT INFORMATION:**

The Senior Management Person responsible for this program is:

Name: Carl D. Chalfant  
 Title: City Administrator  
 Phone number: 785-325-2284

**RISK ASSESSMENT**

The City of Washington has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current and/or existing accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information the utility was able to identify red flags that were appropriate to prevent identity theft.

- New accounts opened in person
- New accounts opened via fax upon receipt of payment
- Account information accessed in person
- Account information accessed via telephone (person)

**PROCEDURE:**

**DETECTION (RED FLAGS):**

The City of Washington adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- Identification documents appear to be altered;
- Photo and physical description do not match appearance of applicant;

- Other information is inconsistent with information provided by applicant;
- Other information provided by applicant is inconsistent with information on file;
- Application appears altered or destroyed and reassembled;
- Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased);
- Lack of correlation between the SS# range and date of birth;
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application);
- Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager) ;
- SS#, address, or telephone # is the same as that of other customer at utility;
- Customer fails to provide all information requested;
- Personal information provided is inconsistent with information on file for a customer;
- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet;
- Identity theft is reported or discovered.

## **RESPONSE**

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the City Administrator.

- New accounts:
  - Ask applicant for additional documentation (e.g. valid driver's license, social security card, or military ID card)
  - Notify City Clerk or City Administrator as soon as possible.
  - Notify law enforcement. The utility will notify the Washington County Sheriff's Office of any attempted or actual identity theft.
  - Do not open the account.
- Existing account:
  - Notify City Clerk or City Administrator as soon as possible.
  - Close the account with approval of the City Administrator.
  - Terminate services with approval of the City Administrator.

## **PERSONAL INFORMATION SECURITY PROCEDURES:**

The City of Washington adopts the following security procedures.

1. Paper documents and files containing secure information will be stored in the vault.
2. Only specially identified employees with a legitimate need will have keys to City Hall.



3. Files containing personally identifiable information are kept in the vault except when an employee is working on the file.
4. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
5. Employees store files when leaving their work areas.
6. Any sensitive information shipped using outside carriers or contractors will be encrypted.
7. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
8. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.
9. No visitor will be given any entry codes or allowed unescorted access to the office.
10. Access to sensitive information will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different.
11. Passwords will not be shared or posted near workstations.
12. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
13. Anti-virus and anti-spyware programs will be run on individual computers on a weekly basis and on servers daily.
14. When sensitive data is received or transmitted, secure connections will be used.
15. Computer passwords will be required.
16. User names and passwords will be different.
17. The use of laptops is restricted to those employees who need them to perform their jobs.
18. Laptops are stored in a secure place.
19. Laptop users will not store sensitive information on their laptops.
20. Employees will never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.
21. If a laptop must be left in a vehicle, it will be locked in a trunk.
22. The computer network will have a firewall where your network connects to the Internet.
23. Any wireless network in use is secured.
24. Maintain central log files of security-related information to monitor activity on your network.
25. Monitor incoming traffic for signs of a data breach.
26. Monitor outgoing traffic for signs of a data breach.
27. Implement a breach response plan as described in the HIPAA plan.
28. Check references or do background checks before hiring employees who will have access to sensitive data.

29. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
30. Access to customer's personal identity information is limited to employees with a "need to know."
31. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.
32. Implement a regular schedule of employee training.
33. Employees will be alert to attempts at phone phishing.
34. Employees are required to notify the City Administrator immediately if there is a potential security breach, such as a lost or stolen laptop.
35. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
36. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.
37. Paper records will be shredded before being placed into the trash.
38. Paper shredders will be available in the office.
39. Any data storage media will be disposed of by shredding, punching holes in, or incineration.

#### **IDENTITY THEFT PREVENTION PROGRAM REVIEW AND APPROVAL**

This plan has been reviewed and adopted by the City Council. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

#### **ANNUAL REPORT**

A report will be prepared annually and submitted to the City Council to include matter related to the program, the effectiveness of the policies and procedures, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

---

Ryan W. Kern, Mayor