



# Columbia-Richland Fire Department

## Standard Operating Guideline OPS – 3.03

### *Health Insurance Portability and Accountability (HIPAA)*

Effective: 2/6/2012

Issued by: Aubrey D. Jenkins, Fire Chief

**Rescinds:** No previous department guideline

**Purpose:**

HIPAA is the Health Insurance Portability and Accountability Act of 1996. It requires all agencies that deal with medical records to keep protected health information (PHI) confidential.

**Scope:**

This policy will be applicable for all personnel (career and volunteer) and each division in the Columbia-Richland Fire Department who have access to patient information understand the organization's concern for the respect of patient privacy and are trained in CRFD's policies and procedures regarding PHI.

**I. Definitions:**

- a. HIPAA is the Health Insurance Portability and Accountability Act of 1996. It requires all agencies that deal with medical records to keep protected health information (PHI) confidential.
- b. PHI is defined as “individually identifiable health information” that is transmitted by electronic media, maintained in any medium that is defined as electronic media, or transmitted or maintained in any other form or medium. In effect, this includes all health information, whether electronic, paper or oral.
- c. “Health information” means: any information, whether oral or recorded in any form or medium that:
  - i. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
  - ii. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.
  - iii. Health information becomes “individually identifiable” if it identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

## **II. Guideline:**

- a. All current personnel will be required to undergo privacy training in accordance with the HIPAA Privacy Rule prior to the implementation date of the HIPAA Privacy Rule, which is December 1, 2011.
- b. All new personnel will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time upon association with the organization, as scheduled by the Medical training officer/Privacy Officer.
- c. All personnel will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time after there is a material change to CRFD's policies and procedures on privacy practices.
  - i. The Privacy Training will be conducted by the Medical Training Officer/ Privacy Officer or his designee.
  - ii. All attendees will receive copies of CRFD's guidelines and procedures regarding privacy.
  - iii. All attendees must attend the training in person and verify attendance and agreement to adhere to CRFD's guidelines and procedures on privacy practices.
  - iv. Training will be conducted using some or all the following: Video, Classroom with documentation, PowerPoint, Question and Answer Period.
  - v. Topics of the training will include a complete review of CRFD's Guideline on Privacy Practices and will include other information concerning the HIPAA Privacy Rule, such as, but not limited to, the following topic areas:
    1. Overview of the federal and state laws concerning patient privacy including the Privacy Regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    2. Description of protected health information (PHI)
    3. Patient rights under the HIPAA Privacy Rule
    4. Staff member responsibilities under the Privacy Rule
    5. Role of the Privacy Officer and reporting employee and patient concerns regarding privacy issues
    6. Importance of and benefits of privacy compliance
    7. Consequences of failure to follow established privacy guidelines
    8. Handling of incident reports and patient care forms.
  - vi. Periodic retraining may be conducted using some or all the following: Video, Classroom with documentation, PowerPoint, Question and Answer Period.

## **III. Patient Care Reports (PCRs)**

- a. CRFD maintains strict requirements on the security and access of all PCRs as well as the initial documentation created by the field providers in their preparation of a PCR.
- b. All preliminary documentation used by CRFD personnel to assist in the creation or modification of a PCR is the sole property of CRFD.
- c. Each member will be given a password to use CRFD's computer systems.

- d. No member may disclose his/her password to any other member.
- e. Each member is to access only his/her PCR's unless directed otherwise by the Privacy Officer or as permitted by an authorized supervisor within the direct course of their duties.
- f. No member is to log onto any computer or password protected software under any user name other than his/her own.
- g. A PCR may be amended by a member upon approval by the Privacy Officer or an authorized supervisor. Amendments must be time stamped by the individual completing the amendments.
- h. All scratch paper and/or forms used by a member in the preparation of a PCR must be shredded immediately. It is a violation of this policy to retain PHI used to create PCR's. This includes hand-off documentation, DHEC Forms, and on-scene notes.
- i. PCR's are only to be printed out with the strict permission by the designated Medical Training Officer and/or Privacy Officer. Printed PCR's are to be maintained in a secure place.
- j. Inappropriate access or retention of PHI may result in disciplinary action, up to and including counseling, verbal reprimands, written reprimands, suspension, demotion and/or termination.

#### **IV. Access, Security and Disclosure**

- a. Security of PHI is everyone's responsibility.
- b. CRFD 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, and should be only to the extent that the person needs access to PHI to complete necessary job functions.
- c. When PHI is accessed, disclosed and used, the individuals involved will make every effort, except in patient care situations, to only access, disclose and use PHI to the extent that only the minimum necessary information is used to accomplish the intended purpose. Patients may exercise their rights to access, amend, restrict, and request an accounting, as well as lodge a complaint with either CRFD or DHEC.
- d. Access to PHI will be limited to those who need access to carry out their duties. The following describes the specific categories or types of PHI to which such persons need access is defined and the conditions, as appropriate, that would apply to such access.
  - i. Patient care reports may be accessed only as part of completion of a patient event and post-event activities and only while actually on duty

- ii. Officer –In –Charge may access only as part of completion of a patient event and Officer post-event activities, as well as for quality assurance checks and corrective counseling of staff.
- iii. Dispatcher Intake forms and preplanned CAD information on patient address may be accessed only as part of completion of an incident, from receipt of information necessary to dispatch a call, to the closing out of the incident and only while on duty.
- iv. Administrative Assistant Intake forms from dispatch and patient care reports may be accessed only as a part of record keeping and distribution of information to individuals, insurance companies or lawyers after approved by privacy officer.
- v. Computer Administrators may access only as a part of maintaining the operating system functions.
- vi. Department Managers may access only to the extent necessary to monitor compliance, accomplish appropriate supervision and management of personnel and report to state agencies.
- vii. Access to PHI is limited to the above-identified persons and to the identified PHI only, based on the Department’s reasonable determination of the persons or classes of persons who require PHI, and the nature of the health information they require, consistent with their job responsibilities.
- viii. Access to a patient’s entire file will not be allowed except when expressly permitted by Department guideline or approved by the Privacy Officer.

**V. Disclosures to and Authorizations from the Patient**

- a. Personnel are not required to limit disclosure to the minimum amount of information necessary when disclosing PHI to other health care providers for treatment of the patient. This includes EMT’s, EMT-Intermediates, Paramedics, any mutual aid provider, personnel involved in the call, and any other person involved in the treatment of the patient who has a need to know that patient’s PHI. D
- b. Disclosures authorized by the patient are exempt from the minimum necessary requirements unless the authorization to disclose PHI is requested by the Department. Authorizations received directly from third parties, such as Medicare, or other insurance companies, which direct the release of PHI to those entities, are not subject to the minimum necessary standards.
- c. For example, if a patient authorizes Disclosure of PHI to Medicare, Medicaid or another health insurance plan for claim determination purposes, the Department is permitted to disclose the PHI requested without making any minimum necessary determination.
- d. For all other uses and disclosures of PHI, the minimum necessary rule is likely to apply. A good example of when the minimum necessary rule applies is when the Department conducts quality assurance activities. In most situations it is not necessary to disclose certain patient information such as the patient’s name, address, social security number, all PHI of the treated patient, in order to conduct a call review. This sensitive information must be redacted or blacked out from the PCR being used as a Q/A example.

## VI. Department Requests for PHI

- a. If the Department needs to request PHI from another health care provider on a routine or recurring basis, the requests must be limited to only the reasonably necessary information needed for the intended purpose, as described below. For requests not covered below, consult an authorized supervisor for guidance. For example, if the request is non-recurring or non-routine, like making a request for documents via a subpoena, response to the request must be limited to the minimum necessary PHI to accomplish the purpose of the request.
- b. Patient care reports: determine what information is reasonably necessary for each on an individual basis.
- c. Incidental Disclosures of PHI may occur in the context of caring for a patient. The privacy laws were not intended to impede common health care practices that are essential in providing health care to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversation between health care providers, or when patient care information in written or computer form is left out in the open for others to access or see.
- d. The fundamental principle is that all staff must be Sensitive to the importance of maintaining the confidence and security of all material created or used that contains patient care information. ***Coworkers and other personnel should not access patient information that is not necessary for the staff member to complete his or her job.***
- e. All personnel must be sensitive to avoiding incidental disclosures to other health care providers and others who do not have a need to know the information. Pay attention to who is within earshot when making verbal statements about a patient's health information, and follow common sense procedures for avoiding accidental or inadvertent disclosures. For example:
  - i. Verbal Security
    1. Public Areas: If patients are in public areas to discuss the service provided to them or to have questions answered, make sure that there are no other persons in the area, or if so, bring the patient into a screened area before engaging in discussion.
    2. Conversations about patients and their health care should not take place in areas where those without a need to know are present.
    3. Other Areas: Personnel may only discuss patient care information with those who are involved in the care of the patient, regardless of physical location. Be sensitive to your level of voice and to the fact that others may be in the area when you are speaking. This approach is not meant to impede anyone's ability to speak with other health care providers freely when engaged in the care of the patient.
    4. When it comes to treatment of the patient, you should be free to discuss all aspects of the patient's medical condition, treatment provided, and any of their health information you may have in your possession with others involved in the care of the patient.
  - ii. Physical Security

1. Patient Care and Other Patient Records: Patient care reports must be stored in safe and secure areas. When any records concerning a patient are completed, they must not be left in open bins or on desktops or other surfaces.
2. Only those with a need to have the information for the completion of their job duties may have access to any records. Paper PCR's must be shredded as soon as the data has been entered into Firehouse.
3. Computers and Entry Devices: Computer access terminals and other remote entry devices such as PDAs and laptops must be kept secure. Access to any computer device shall be by password only.
4. 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 remote devices such as laptops and PDAs shall remain in the physical possession of the individual to whom it is assigned at all times.
5. Personnel shall not access patient care reports unless it falls within the direct course of their duties, clearly defined above.

## **VII. Penalties for Violation**

- a. The Department takes its responsibility to safeguard patient information very seriously. Significant legal penalties may arise from adhere to the laws that protect patient privacy.
- b. Personnel who do not follow our guidelines on patient privacy will be subject to disciplinary action up to and including discharge.
- c. The Department will not retaliate against any staff member who expresses a good faith concern or complaint about any guideline or practice related to the safeguarding of patient information.

## **VIII. Privacy Officer**

- a. The Department has appointed a Privacy Officer to oversee guidelines and procedures on patient privacy and to monitor compliance. The Privacy Officer is also available for consultation on any issues or concerns about how our Department deals with protected health information. Feel free to contact the Privacy Officer at any time with your questions or concerns.

## **IX. Patient Complaints**

- a. Patients have the right to complain to the Department about any concerns they may have concerning patient privacy.
- b. Any patient or family member who expresses a concern or complaint to you should be directed to contact the Privacy Officer.
- c. The Privacy Officer is responsible for receiving, investigating, and documenting all complaints from patients concerning patient privacy issues.