Patient Medical Record Security and Privacy Policies and Procedures (1003.00)

I. GENERAL PROVISIONS:

A. The intent of these policies and procedures is to define internal requirements for patient medical record security and privacy in accordance with the Health Insurance Portability and Accountability Act (HIPAA) enacted by the U.S. Congress in 1996, defined as Protected Health Information (PHI) requirements through the Privacy Rule and the Security Rule.

B. The Kern County EMS Department, as a local government regulatory agency in accordance with State law, is exempt from chain of custody agreements and other HIPAA requirements applied to private organizations. However, internal medical record security requirements and medical record privacy requirements under the Privacy Rule and Security Rule are applicable.

C. These policies and procedures shall apply to any and all records or data with any patient identification information. All patient medical records managed by the Department, including but not limited to completed or partially completed PCR-Transport forms, EMT-I First Responder forms, MICN forms, Defibrillation or Combitube forms, physician and hospital claims for EMS Fund reimbursement, PCR-Transport data reports, or patient record images with patient identification information (hereinafter referred to as "patient record(s)") shall be applied to these policies and procedures.

D. Kern County EMS Department staff shall continuously comply with these policies and procedures.

II. MEDICAL RECORD SECURITY: (Security - Ensure the security of patient information and associated transactions both from a physical and electronic point of view)

A. All patient records shall be maintained secure by the Department.

B. Patient records shall either be attended by Department staff or stored in a secure or locked area of the Department. Patient records may only be removed from the Department by EMS staff if approved by the Department Privacy Officer (DPO).

C. Patient records shall remain in a secure area or locked storage after office hours. This includes staff offices with patient records. No patient record will be left in an open office area unattended.

D. The data entry office shall remain closed and locked when unoccupied during and after normal office hours.

E. During office hours, any office that contains patient records shall be closed and locked when left unattended by Department staff. EMS staff will continuously monitor secure office areas for unauthorized access. An office is unattended when staff are physically outside the specific office area and unable to maintain record security. This includes breaks, lunch, or meetings outside the specific office space.

F. The Computer Server Room must remain locked after normal business hours, unless occupied by Department Staff.

G. All entrance and exit doors must remain locked after normal business hours, unless the building is occupied by Department staff.

H. Electronic Patient Record Security:

1. All computer workstations and servers within the Department require a user identification and password for login access to electronic documents, including electronically stored patient records, in accordance with the following requirements:

   a. File access is controlled by login identification;

   b. Unique passwords, changed at least annually, shall be maintained secure by each EMS staff member; and

   c. Login identification and passwords will be removed when an employee is no longer employed by the Department.

2. EMS staff shall comply with one of the following when an office area with a computer workstation is unoccupied with the intent to remain unoccupied (i.e. lunch, a break, a meeting, or an appointment):

   a. The office door(s) must be locked; or

   b. Logoff the workstation; or

   c. Shut down the workstation.

3. Upon leaving the office for the day Department staff must shut down their computer workstation, except VPN users as per H- 6.

4. Department Computer Servers are to remain "locked" at the system console, requiring a password login to access the system and data.

5. Patient record data may be referred electronically provided referral is through a secure process that allows end-to-end authentication. Electronic referral consists of e-mail, file transfer protocol, Internet

web posting, and any configurable data stream. End-to-end authentication is met when the electronic referral does not leave a secure network environment and the recipient is known, such as the Kern County Wide Area Network e-mail client, or when encryption and authentication measures are used between sender and recipient thus verifying full receipt by recipient. Any e-mail traveling outside a secure network environment – into the Internet – requires encryption and authentication measures.

6. Remote access to Department workstations and thus the Department Local Area Network and Kern County Wide Area Network require of the remote user:

   a. An account with a reputable Internet Service Provider.

   b. Install and configure VPN software per County specifications. User cannot share his/her VPN password with others.

   c. Install ICSA Labs approved anti-virus software (McAfee or Norton). Anti-virus files must be updated, at minimum, every three months.

   d. Log out once completing current remote session - do not allow the session to remain open and idle on the intent to return at a later time - by logging off the Department workstation and then properly exiting all remote access and VPN software accordingly. The County reserves the right to terminate idle connections exceeding ten (10) minutes.

   e. Take reasonable steps to safeguard data from tampering and unauthorized disclosures at remote locations.

III. INTERNAL PATIENT RECORD MANAGEMENT PROCEDURES:

A. Upon receipt, patient records shall immediately be delivered to the Data Entry office, appropriate EMS staff or must be attended by EMS staff until the patient records can be appropriately secured.

B. Patient records cannot remain in office areas open to the public (i.e. staff boxes, routing trays, training rooms, break rooms, cabinet tops located in passageways) or in plain sight of the public (i.e. copier rooms, fax machines, desktops, and counter tops).

C. Stored patient records shall be maintained in a locked storage area.

D. Upon DPO authorization to release a patient record, an assigned staff member is to retain the requested patient record until pick-up or place the patient record into a sealed envelope for pick-up so the patient record is not in plain sight of the public. A requested patient record cannot be placed in

plain sight on a counter top or an out-box awaiting pick-up from the requestor.

IV. MEDICAL RECORD PRIVACY: *(Privacy - Ensure the confidentiality of the patient record through management of access)*

A. Any patient record request received by Department staff from any other organization or individual shall be referred to the DPO for review and consideration.

B. Patient records may be reviewed by Department staff in group quality improvement activities. However, all patient identification information shall be removed or rendered unreadable for group quality improvement activities involving other organizations or individuals. Such patient records will still not be released unless approved by the DPO.

V. MEDICAL RECORD RELEASE:

A. All patient record release requests shall be referred to the DPO for review, authorization or denial.

B. Patient records are confidential, limited to the possession of the Department, authorized EMS providers involved with response to the patient location or direct patient care that completed the record, authorized medical facilities that receive the patient if transported, and validated service payor sources.

C. Patient record copies can be provided by the DPO to legal sources in accordance with legal and valid subpoena or appropriate patient or legal patient responsible party medical record release.

D. The DPO may release a copy of a patient record directly to the patient or patient responsible party in accordance with the following:

1. Completion of the form "Authorization to Release Records";

2. Verification that the person completing the form is the patient or the legal patient responsible party with appropriate identification and documentation.

E. In each case of patient record release to a legal source, patient or legal patient responsible party, a full copy of the subpoena, medical record release or completed Authorization to Release Records in addition to the patient record copy will be maintained on file. Authorization to Release Records are also patient records in accordance with these policies and procedures.

VI. TRAINING: *(To ensure protection of health information a self-certified training program must be created and implemented for employees and vendors)*

A. All Department staff shall review these policies and procedures and shall sign a verification form that validates competency and compliance. The signed verification form shall be retained in each Department staff member's personnel file at the Department.

B. Any newly employed Department staff person shall review these policies and procedures and shall sign a verification form that validates competency and compliance. The signed verification form shall be retained in each Department staff member's personnel file at the Department.

C. These policies and procedures, as a public record, will be referred to providers or organizations upon request and will be posted on the Department's web site.

Kern County EMS Department

Patient Medical Record Security and Privacy Policies & Procedures

EMS Staff Competency & Compliance Verification Form

With my signature below, I verify that I have reviewed the Kern County EMS Department - Patient Medical Record Security and Privacy Policies & Procedures, that I am competent in the content, and I will comply with the requirements.

_____

(print name)

_____

(signature)

_____

(date signed)

KERN COUNTY EMS DEPARTMENT
AUTHORIZATION TO RELEASE RECORDS

TO: _____

I,_____, D.O.B. _____,

hereby authorize and consent to the release of any medical, psychiatric, drug and/or alcohol abuse records to myself or to representative of patient as signed above.

PATIENT NAME: _____

PATIENT AGE: _____ PATIENT SEX: _____

D.O.B.: _____ CALL DATE: _____

CALL LOCATION: _____

TYPE OF INCIDENT/MEDICAL PROBLEM: _____

HOSPITAL:_____

AMBULANCE SERVICE: _____

EXECUTED THIS _____ DAY OF _____, 20_____.

_____

Signature of Person Requesting Records Date of Request for Records

For Office Use Only:

Records Released By: **Identification Verified**: ___**Yes** ___**No**