	SOUTHERN FOX VALLEY EMERGENCY MEDICAL SERVICES SYSTEM POLICY & PROCEDURES
TITLE: QUALITY ASSURANCE AND DATA COLLECTION POLICY	
SECTION: QUALITY ASSURANCE/DATA COLLECTION	POLICY NUMBER: F 1.0
APPROVED BY: DR. ARTHUR PROUST EMS MEDICAL DIRECTOR	
EFFECTIVE DATE: 09/01/2023	PAGE NUMBER: 1 OF 8

PURPOSE:

1. Medical records are used to track events and transactions between patients and health care providers. EMS patient care reports (PCRs) provide details of the patient encounter for handoff to other healthcare providers and data necessary for ambulance coders to create a bill to reimburse for care provided. EMS data is also used in legal investigations, trauma, stroke, and CPR registries, state and national databases, research, and quality assurance initiatives. EMS documentation serves an important role as a data repository.

2. This policy establishes the System standard for the collection, handling, storage, use, retrieval, evaluation, reporting, and submission of data within the Southern Fox Valley EMS System.

3. This policy applies to all EMS agencies, Resource, Associate, and Participating Hospitals, and individuals with permission to access the System's electronic patient care record (ePCR) software, written patient care reports, and/or EMS data.

4. IDPH Rules Section 515.330 EMS Program Plan - Data collection and evaluation methods

    a. The process that will facilitate problem identification, evaluation, patient care gaps, disease/injury surveillance, and monitoring in reference to patient care and/or reporting discrepancies from hospital and pre-hospital providers;

    b. A policy identifying any additional required data elements that the EMS provider shall include in their patient care report;

    c. Identified benchmarks or thresholds that should be met;

    d. A copy of the evaluation tool for the short reporting form, if used, pre-hospital reporting form; and

    e. A sample of the required information and data submitted by the provider to be reported to the Department summarizing System activity (see Section 515.350).

5. Per IDPH Rules Section 515.330: The EMS System shall have a quality improvement plan which describes how quality indicators and quality benchmarks are selected and how results and improved processes are communicated to the system participants.

POLICY:

1. Quality Assurance Committee will be established by the System.
    a. Each System participant must identify a representative for this committee.

    b. This committee will correspond on a regular basis through email and mail.

    c. Meetings will be held on an as needed basis.

    d. Quality Assurance findings and information shall be forwarded to all departments and System Education Committee.

2. All Quality issues will be brought to the attention of the EMS System Coordinator, EMS Medical Director or the EMS System CQI Coordinator.

3. All quality issues will be reviewed by the EMS System CQI Coordinator, EMS System Coordinator and either the EMS Medical Director or the Associate EMS Medical Director.

4. Data analysis for quality measurement and improvement; problem identification, evaluation, patient care gaps, disease/injury surveillance, and monitoring in reference to patient care and/or reporting discrepancies by System members:

    a. Quality Assurance (QA) is used to systematically improve care and seeks to standardize processes and structures to reduce variation, achieve predictable results, and improve outcomes for patients, healthcare systems, and organizations. Structure includes technology, culture, leadership, and physical capital. Process includes knowledge capital (e.g., standard operating procedures) or human capital (e.g., education and training).

    b. ePCR Quality Assurance review: The System shall conduct quality measurement and improvement reviews and disease/injury surveillance audits as defined by IDPH and the EMS System Quality Improvement Plan.

    c. Thresholds to be met shall be determined by national measures where they exist and local targets established by the Quality Assurance committee and agreed to by the EMS MD.

    d. Data from Quality Assurance analyses and disease/injury surveillance is reported to governmental entities, system leaders, committees, and providers as appropriate and applicable. Reports are available to EMS System providers on a monthly/quarterly/yearly basis and upon request to IDPH.

Effective Date:	09/01/2023				
Review Date(s):	02/2015	08/17/2023			
Revision Date(S):	07/2015				

e. Quality indicators will include but not be limited to: high risk and/or low frequency events, new medications, procedures, protocols, policies, and issues identified by sentinel events.

   i. Examples of metrics to be monitored include:

      1. Utilization of etCO2
      2. Hemorrhage controlled
      3. Level I TC appropriate destination
      4. Scene times for time sensitive pts
      5. STEMI pts: 12L ECG acquirement and transmission
      6. Cardiac arrest ROSC rates
      7. Pre-arrival alert/notification: sepsis, STEMI, stroke, trauma
      8. Pediatric pts assessed and treated appropriately
      9. Geriatric pts assessed and treated appropriately
      10. Assessed & treated appropriately: allergic reaction, altered mental status, cardiac arrest, dysrhythmias, hypoglycemia, nausea, pain, respiratory distress/failure, seizures, shock, stroke

f. Data acquired from the Quality Assurance will provide continuing education topics that will be taught to the current National EMS Standards and National Scope of Practice approved by the System Medical Director

   i. SFVEMSS policies and procedures may be modified to reflect opportunities identified through this same process.

g. All Quality Assurance and Improvement activity of the Southern Fox Valley EMS System is privileged and confidential under the Medical Studies Act (735 ILCD 5/8-2105 (2017)).

5. Correcting or editing an entry

   a. Apparent nonconformities due to errors or omissions in documentation should be corrected promptly once detected through QI monitoring using proper methodology. A locked report may be unlocked and corrected or edited by approved agency administrators (nonclinical entries) and/or those who were listed as EMS responders on the original record (any entries within their scope of practice).

   b. All changes to the original record after it is locked will be automatically noted on an electronic audit trail. The edited report shall be uploaded to cloud storage via usual and customary processes.

   c. If the edits provide new information that could impact continuity of patient care, the amended report shall be provided to the receiving healthcare facility.

   d. Records involved in any open investigation, audit or litigation should not be modified or destroyed. Each agency shall ensure that they have a “litigation hold” program in place to preserve all evidence and documentation existing at the time in the event of a known investigation or litigation being filed

6. Data submissions to IDPH

   a. EMS Providers will import their data electronically directly to IDPH data collection site.

   b. On or before the 15th of each month, each EMS provider agency shall submit all PCR data from the preceding month to the Illinois Department of Public Health (IDPH) based on the current Illinois State Schematron. This data shall be electronically transmitted via the designated secure, encrypted, transmission medium to Illinois Data Systems.

   c. Data validation by IDPH is required prior to submission to ensure compatibility with their data specifications.

   d. Data reporting elements for IDPH: Starting in 2023, IDPH will accept NEMSIS 3.5 data elements. For information on the Illinois Data Program and NEMSIS specifications see https://dph.illinois.gov/topics-services/emergencypreparedness-response/ems/prehospital-data-program/illinois-nemsisspecifications.html

7. End of year data reporting to the EMS System

   a. The QI Committee shall compile summative yearly data reports for all System ePCRs stored on the ESO site.

   b. The report shall include adult and pediatric demographics; patient dispositions, receiving facilities, primary impressions; medications given; interventions performed; pediatric cardiac arrests; run times; vehicles with highest PCR generation numbers, and the number of PCRs stored by each agency.

8. Security and control relative to ePCR software and hardware

   a. Any person or entity that creates, receives, obtains, maintains, uses, or transmits protected health information (PHI) shall adhere to laws regarding the protection of and confidential access to EMS medical records. These include the Illinois Medical Records Retention laws, the Health Insurance Portability and Accountability Act (HIPAA), and Confidentiality of Patient Records and Code of Ethics. Each EMS agency and its employees are responsible for ensuring that all entered data, and electronic resources are appropriately protected against preventable or foreseeable mistakes in data entry, processing, intentional or inadvertent losses, and purposeful malfeasance.

b. Each EMS agency is responsible for ensuring that devices running ePCR software are maintained with all manufacturer mandated updates that prevent breaches in data security and integrity.

c. Usernames and passwords used to access ePCR software or hardware shall not be transmitted through unencrypted email or other unsecure communications mediums.

d. Personal Health Information (PHI), printed PCRs, or other ePCR data that contains patient identities shall not be transmitted through unencrypted email or other unsecure communications mediums.

e. EMS Agencies may specify a limited number of users to have agency level administrator access to the ePCR software. The System reserves the right to limit the number of users with administrative permissions to maintain system security.

f. No individual shall make any unauthorized changes, additions, deletions, or corrections to any hospital or provider templates, ESO files, or PCRs.

g. Each ePCR software user is responsible for maintaining the security of ePCR and associated data when using agency software and hardware. These actions include, but are not limited to:

   i. Logging out of the ePCR software when not in use.
   ii. Securing, locking out, or logging out of the ePCR device when not in use.
   iii. Creating passwords that meet agency, ePCR software vendor, and/orsystem complexity requirements.
   iv. Keeping hardware and software login credentials (username/password) strictly confidential.
   v. Changing passwords if breeched or suspected to have been breached.
   vi. Maintaining physical control of ePCR hardware at all times.

h. EMS agencies are encouraged to enhance the security of ePCR software by implementing additional security measures, including:
   i. Configuring automatic lockout/sleep when a user/device has been idle
   ii. Require a password, pin, or other credentials to access hardware after lockout or sleep periods
   iii. Require complex passwords that include combinations of upper case, lower case, numbers, symbols, etc.

i. ePCR Software user management

   i. User management of ePCR software is primarily the responsibility of the EMS agency and their designated administrators.

ii. Only the EMS System and System level administrators are permitted to permanently inactivate a user account from the ePCR software.

iii. Creating users: Once an EMS clinician is approved to work in the System, the EMS agency must create a user account that contains the individual's name and license number, along with a username and password.

iv. User account permissions: Users of the ePCR software must be assigned the most appropriate level of access for their role in the agency. These permission levels include:

    1. EHR User; QM User; Personnel Management User; Personnel Management Admin
    2. QM Billing | EHR Administrator

v. Inactivating users: EMS agencies shall inactivate an employee's account at the time they leave the System or have practice privileges suspended. The EMS System shall inactivate a Provider Agency's account at the time they leave the System or are suspended from operation.

vi. Only EMS System and System level administrators are permitted to reactivate a user account.

vii. Agency administrators may have to perform additional user account maintenance that includes:

    1. Resetting passwords
    2. Restoring locked-out accounts
    3. Updating license expiration dates
    4. Updating demographics

9. Security and control of printed PCRs

    a. Security of printed PCRs shall be maintained at all times by EMS agencies, their employees, and receiving facilities.

    b. Monitor print queues for failed or inadvertent ePCR print requests that may be cached from a failed printing attempt.

    c. Securely dispose of inadvertently printed PCRs in compliance with privacy policies.

    d. Printed ePCRs should not be routinely transported between facilities, agencies, stations, or offices. If additional ePCRs are needed for records, billing, QI, or other approved reasons, they should be printed upon arrival to the next secure location.

    e. ePCRs should not be sent to remotely located printers unless they are under the control of the provider or another authorized party.

    f. PHI, printed PCRs, or other ePCR data that contains patient identities shall not be transmitted through unencrypted email or other unsecure communications mediums.

   g. When faxing PCRs to a receiving facility, or other authorized recipient, a secure means must be used and the device approved by the facility to receive PHI.

   h. The system provides a PCR print option with identifiable information redacted to be used by paramedic students, QI reviewers, and other authorized parties.

10. Appropriate uses of hospital computers

    a. Use of all electronic systems and devices must be compliant with hospital policies and not in violation of any legal regulations.

    b. Users must not deliberately act in a manner that would negatively impact the operation of electronic devices or systems. This includes, but is not limited to:

       i. tampering with components of the hospital computers or network
       ii. Installing or uninstalling applications that affect system operability

    c. Users must not unfairly monopolize a computer or system resources that prevents others from completing their assigned duties.

    d. Users shall not use hospital equipment to access, store or publish materials which are pornographic, sexual, racist, sexist, or otherwise offensive.

    e. Hospitals reserve the right to monitor, filter, or track communications on their networks or systems. Hospitals will audit system and application logs and processes as required by HIPAA and other applicable regulations.

    f. All network traffic is subject to the acceptable use policies of the network through which it flows.

11. Policy distribution: All current SFVEMSS members, students, and other users of SFVEMSS ePCR software will be given access to a copy of this policy via the System website. The SFVEMSS reserves the right to change this policy at any time.

12. Violation of policy: All allegations of misconduct relative to this policy shall be investigated in compliance with the System Just Culture framework. Any person found to have willfully or grossly violated this policy shall be in noncompliance with the System's Ethics Policy, and shall be subject to the provisions of System Policy Due Process: Corrective coaching/Disciplinary action.

13. Immunity provisions

    a. All information contained in or relating to any medical record audit performed by an authorized party and/or by the EMS MD shall be afforded the same status as information concerning medical studies in Article VIII, Part 21 of the Code of Civil Procedure. Disclosure of such information to IDPH shall not be considered a violation of that Code.

b. Hospitals and individuals that perform or participate in medical audits pursuant to the EMS Act shall be immune from civil liability to the same extent as provided in Section 10.2 of the Hospital Licensing Act.

14. Medical records retention period in Illinois: The System and its members shall preserve EMS-related medical records in a format and for a duration established Illinois law and by policy and for not less than 10 years, unless notified in writing by an attorney before the expiration of the 10-year retention period that there is litigation pending involving the record of a particular patient. In such case, follow direction from the Agency's legal counsel.

Effective Date:	09/01/2023				
Review Date(s):	02/2015	08/17/2023			
Revision Date(S):	07/2015				