ARIZONA DEPARTMENT OF HEALTH SERVICES

Bureau of Emergency Medical Services & Trauma System

Data Quality Assurance Section Manual

Contact: Rogelio Martinez, Section Chief

7/6/2015

"Health and Wellness for all Arizonans"

Table of Contents

A. Introduction

The purpose of this manual is to set the written standards and criteria that the Data and Quality Assurance (ADHS-DQA) Section uses in the development of the Bureau of Emergency Medical Services and Trauma System (BEMSTS) Quality Assurance (QA) process. The Arizona Department of Health Services (ADHS) QA process includes activities that evaluate and analyze the systemic trends of public safety, patient care, professional practices, trainings, and proper utilization of health care services and facilities in the EMS and trauma system.

The collection of Arizona EMS and Trauma data currently occurs through two systems: the Arizona Prehospital Information & EMS Registry System (AZ-PIERS) and the Arizona State Trauma Registry (ASTR). AZ-PIERS collects prehospital information from participating EMS agencies comprised of air and ground ambulances, fire department and districts, and tribal partners around the state. ASTR collects trauma patient information from participating hospitals; these are mostly comprised of designated trauma centers.

As the ADHS-DQA staff progresses in linking and managing EMS data from internal, external, local, state and national sources the capability for integrating information into state QA initiatives will exponentially increase. Policy effects and required updates from data linkages will be updated through this manual on a regular basis. These linkage projects are essential to understanding the complete continuum of care in EMS and trauma patients, validating information, and systematically addressing opportunities that optimize public safety and patient care.

B. AZ-PIERS

AZ-PIERS was established to measure and optimize performance of EMS care in Arizona. The inclusion criteria for AZ-PIERS are all EMS calls which include but are not limited to inter-facility transfers, cancelled, stand-by, 911-emergency, and mass casualty events. All identifiable data collected by an agency belongs to that agency. Approval shall be received from the agency representative prior to the access or release of data. All data shall remain protected and accessible only to the specific agency approved personnel and ADHS-DQA staff, unless otherwise noted in the manual. Data elements are available to the public unless it contains Protected Health Information

(PHI) that may identify a patient, provider, or an organization. This includes information that may be potentially identifiable or is intended for use in the BEMSTS Quality Assurance process.

Provider access to AZ-PIERS:

To gain access to the AZ-PIERS, agencies must fill out the required AZ-PIERS EMS Agency Application. All applications are submitted for processing to the AZ-PIERS data manager. After initial setup by the data manager, the person named on the application as the EMS representative position will be responsible for granting and denying agency employees access to that agency's data. Agencies are responsible for adding or removing users as required. ADHS-DQA recommends that agencies have at least two (2) administrators to ensure access is not the responsibility of one individual. The liability of maintaining compliance with HIPAA and any other regulations on an agency level is the responsibility of the submitting agency. Participation in the registry is in agreement with the policies outlined in this manual.

Hospitals access to AZ-PIERS:

To gain access to AZ-PIERS, hospitals must fill out the required AZ-PIERS Hospital Application. All applications are submitted for processing to the AZ-PIERS data manager. After initial setup by the data manager, hospitals will be responsible for granting and denying hospital employees access to the data. The EMS coordinator position is responsible for granting their base hospital access to the electronic patient care reports (ePCRs). Agencies will be able to grant access to hospitals that are not basing them by filling out the "destination hospital" variable in the ePCR. Hospitals are urged to avoid using general usernames (i.e. EDNurse) to track access among staff. ADHS-DQA recommends that hospitals have at least two (2) administrators to ensure access is not the responsibility of one individual. Hospitals have the additional requirement that an HR representative attach additional documentation on access.

Maintenance of AZ-PIERS records:

Agencies have the ability to modify their records one month after the incident date of the record. AZ-PIERS records are locked down yearly on February 15th of the following year. These policies are put in place in conjunction with the recommendations of the EMS Registry Users Group (EMSRUG) and the availability of ADHS resources. Per ARS 39-101, state law requires that ADHS to maintain all records permanently. ADHS regularly maintains and backs up all records to comply with state law.

Agencies will always have the ability to access their data. Notices shall be given to participating agencies in the event of record loss.

AZ-PIERS Data Process:

Prehospital care data are transmitted to dedicated servers secured via encrypted electronic patient care reporting (ePCR) through the software applications of Field Bridge® and State Bridge® owned by ImageTrend, Inc., a State of Arizona approved vendor. Servers are hosted by ImageTrend in a state-of-the-art data center with maximum level security accessible only by authorized personnel. The data center is monitored electronically and server room access is monitored and recorded. The databases are on a private network with access managed through the firewall permitting only authorized administrators or approved virtual private networks (VPN). The server and network safeguards comply with HIPAA privacy and security rules standards.

C. ASTR

The ASTR was established to provide quarterly trauma reports to submitting hospitals, study the effects and causes of trauma, and evaluate the services and programs related to trauma. The ASTR inclusion criteria and data elements were established in rule through R9-25-1402 and approved by the State Trauma Advisory Board (STAB) and the Trauma and EMS Performance Improvement committee (TEPI). Data elements are available to the public unless it contains Protected Health Information (PHI) that may identify a patient, provider, or an organization. This includes information that may be potentially identifiable or is intended for use in the BEMSTS Quality Assurance process.

Hospital access to ASTR:

To gain access to the ASTR system, hospitals must contact the Arizona State Trauma Registrar. After initial granting of access the hospital's liaison will be responsible for informing the ASTR data manager of changes in user status. Hospitals may access all of their identifiable data through the state but are limited to guidelines established by Health Insurance Portability and Accountability Act (HIPAA) regarding data from other participating hospitals.

Hospitals must keep up to date with adding or removing users as required. It is recommended that hospitals have at least two (2) administrators to ensure access is not the responsibility of one individual. The liability of maintaining HIPAA and other statutes on a hospital level is the responsibility

of the submitting hospital. Participation in the ASTR is in agreement with the policies outlined in this manual.

Maintenance of ASTR records:

ASTR records are locked down yearly on April 1 and considered completed after hospitals turn in their 4th quarter results. All corrections should be completed by the end of June. Per ARS 39-101, state law requires that ADHS to maintain all records permanently. In the case of any record loss, ADHS shall notify the affected organization.

ASTR data process:

Trauma data from Arizona's trauma centers containing confidential information (provider or individual level) are transmitted to ADHS via an encrypted SFTP. Hospitals not participating in the SFTP process have the ability to send their data through a secure email. ADHS makes every effort to provide hospitals with a secure method to send data. Hospitals that wish to send data through a secure email must first request one by contacting ADHS-DQA staff. Trauma data are stored in the ASTR and maintained on a secure in-house server safeguarded by the HIPAA-compliant privacy and security measures described above.

D. Data presentation

Reports to data contributors:

Reports are regularly provided to participants on a quarterly basis to assist in an agency's quality improvement initiatives. The reports are scheduled to be sent to participants in the months of March, June, October, and December. Participating hospitals and EMS agencies are compared to state aggregate measures. The reports are sent by encrypted email to the contacts of the listed on file as they are completed. Participating hospitals and EMS agencies are entitled to their own submitted data upon request. Agencies or hospitals may not receive another organization's quarterly report unless authorized by that organization. The agency representative will receive the AZ-PIERS quarterly report. The trauma medical director and trauma program manager will receive the ASTR quarterly report. Additional recipients may be added through written approval from the organization's representatives.

Reports to the public:

Individuals can access reports related to EMS or traumatic injury on the Bureau's website. All patient, provider, and organization identifiable information have been removed from all reports that are distributed to the public. The public may request additional analysis by contacting the DQA section chief. An annual state trauma report is posted on the website in October after the director's approval. Additionally, quarterly aggregate reports for EMS and trauma centers are posted on the website. Examples of the current reports can be found on the quality assurance reports portion of the DQA website.

National datasets:

ASTR is currently unable to submit directly to the National Trauma Data Bank (NTDB) due to difference in inclusion criteria. Hospitals that participate in ASTR and NTDB have to submit their data separately to each.

AZ-PIERS submits national data elements to NEMSIS as of June 3, 2013 on behalf of those agencies that have indicated in writing they wish to do. Data will not be submitted to NEMSIS unless BEMSTS has prior written approval from a participating EMS agency.

Third Party State Agencies:

BEMSTS regularly works with other Bureaus and Offices within the ADHS. The additional level of protections on the EMS and Trauma Center registries must be considered with collaborative efforts. Data is de-identified outside of ADHS-DQA and is protected per ADHS policy and the policies outlined in this manual.

Grant data requests:

As part of the daily functions of the Bureau, utilization of data from the AZ-PIERS and ASTR may be requested for grants. The ADHS-DQA sections works closely with the other sections/bureaus for grant funding on projects. Care in protecting individual level data is maintained and is not reported on grant applications. Data is de-identified outside of ADHS-DQA staff and is protected per ADHS policy and the policies as outlined in this manual.

Research data requests:

ADHS-DQA distinguishes between the public and researchers. Research is an important component of both registries and follows the framework established by the Council of State and Territorial Epidemiologists (CSTE). As such, the ASTR is available for research purposes. Restrictions placed on AZ-PIERS prevent its use for outside researchers. Data that is requested from registries that are not from AZ-PIERS or ASTR are unable to be processed by ADHS-DQA staff; these requests must go to the appropriate data owner.

Entities requesting data for research purposes that require record-level PHI must obtain approval from the Human Subject Review Board (HSRB) either in their own institution and/or the Arizona Department of Health. There must be a valid reason to receive requested data. Approval from the HSRB does not determine the release of the data, the DQA section must determine if the request is feasible. Feasibility is dependent on size of the requests, staff availability, and prioritization of other projects. Information on the HSRB review process can be found here. The data elements that are available from the individual registries can be found on Data and Quality Assurance Policy webpage.

All requests for ASTR or AZ-PIERS data, whether aggregate or PHI, must be submitted to the ADHS-DQA Section using BEMSTS approved data request forms. The DQA section chief will respond with a confirmation that the request was received.

E. Ongoing Quality Assurance Projects

1) *Arizona Department of Transportation (ADOT):*

As part of its ongoing QA initiative, ADHS-DQA works closely with the Arizona Department of Transportation (ADOT) to reduce the incidence and severity of motor vehicle injuries. The ADOT and ADHS-DQA collaborate on data analysis initiatives, quality assurance, system development, surveillance, and effectiveness of crash prevention strategies. For this reason, ADOT and ADHS-DQA staff exchange crash data that jointly contributes to QA efforts in both agencies. ADOT data remains the property of ADOT; ADHS-DQA is unable to be released any of this data without approval. EMS agencies and hospitals that would like to be excluded in these efforts must contact the Bureau in writing.

1A.Fatal Accident Reporting System (FARS) access to AZ-PIERS:

FARS analysts must fill out the required AZ-PIERS FARS Permission Group Application in order to gain access to the AZ-PIERS. The FARS permission group is limited to retrieving EMS notification time, EMS on scene date/time, and EMS arrival at destination for fatal injuries of motor vehicle traffic. The FARS Data Permission Group module in AZ-PIERS allows the ADOT FARS Analyst to login to AZ-PIERS and generate a basic report containing the three EMS-related times. Strict confidentially and surveillance of activities will be ensured by the AZ-PIERS data manager. Agencies that would like to be excluded must contact the Bureau in writing.

1B. *Crash Outcome Data Evaluation System (CODES) inspired linkage:*

From 1992 to 2013 the National Highway Traffic Safety Administration (NHTSA) began integration efforts to understand the full financial and medical implications of motor vehicle crashes. The goal was to develop prevention and mitigation factors that can be implemented into communities. In 2013, NHTSA turned the data linkage efforts to the states in 2013.

DQA staff completed a database merger in early 2015. Current projects are being developed and will be documented, tracked, and protected to the fullest extent possible.

F. Public health partners

ADHS may develop public health partnership as part of its ongoing initiatives and efforts. All public health partnership will have the following:

- Clearly specified, realistic, and shared goals,
- Clearly delineated and agreed roles and responsibilities,
- Distinct benefits stated for all parties and stakeholders,
- The perception of transparency for all parties and stakeholders,
- Active maintenance of the partnership,
- Equality of participation for all parties and stakeholders,
- Meeting of agreed obligations.

All active Memorandum of Understandings with current Public Health Partners will be displayed on the website as they are formed and updated. It is the responsibility of the DQA section chief, Deputy Bureau Chief, and Bureau Chief to approve public health partners. EMS agencies and hospitals that would like to be excluded in these efforts must contact the Bureau in writing. Developing partnerships will be communicated to members through the list serves, EMS Registry User Group, Trauma Registry Users Group, and the statutory and standing committees.

G. Additional data protection information

All data, application software and operating system software generated by ADHS's electronic systems are safeguarded through administrative, technical, and physical measures compliant with state and federal (HIPAA) privacy and security standards for electronic protected health information. ADHS data security and privacy measures are consistent with generally accepted security best practices and industry requirements. ADHS complies with legal requirements established by Federal and State statutes pertaining to the confidentiality, privacy, accessibility, availability, and integrity of information resources. ADHS Information Security framework is based on Health Information Trust Alliance's (HITRUST's) Common Security Framework standards with 13 security control categories comprised of 42 control objectives and 135 control specifications mapped to HIPAA Security Rule standards and other compliance requirements. All data transmitted over ADHS networks, secure file transfer protocol (SFTP), and email are encrypted and mathematically protected against disclosure. ADHS performs proactive security assessments and tests to identify potential risks and methods of effectively securing ADHS information resources from unauthorized access, misuse and destruction. Security and privacy assessments include continuous monitoring and annual security assessments. Continuous monitoring includes reviewing security controls in each system to ensure that management, operational and technical controls function effectively. Continuous monitoring maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Annual security assessment includes penetration tests, vulnerability scans, and application tests to verify compliance with the ADHS security framework.

H. Provider legal protections

Information that identifies a patient, provider, or organization are subject to the HIPAA guidelines and state statutes. Pursuant to A.R.S. § 12-2291, materials prepared in connection with quality assurance

activities are not medical records. As AZPIERS and ASTR are part of a ADHS-DQA program, the ADHS cannot release or utilize ASTR or AZ-PIERS data (elements, reports) for enforcement or other related scenarios.