Bureau of Emergency Medical Services & Trauma System

Data Quality Assurance Section Manual

Contact: Rogelio Martinez, Section Chief

5/30/2013
# Table of Contents

**Introduction** .............................................................................................................................. 1

**Arizona Pre-hospital Information & EMS Registry System (AZ-PIERS)** ........................................ 2
- Provider access to AZ-PIERS
- Hospitals access to AZ-PIERS
- Maintenance of AZ-PIERS records
- AZ-PIERS Data Process

**Arizona State Trauma Registry (ASTR)** .................................................................................... 3
- Hospital access to ASTR
- Maintenance of ASTR records
- ASTR data process

**Data presentation** ...................................................................................................................... 4
- Reports to data contributors
- Reports to the public
- National datasets
- Third Party State Agencies
- Grant data requests
- Research data requests

**Additional data protection information** .................................................................................... 5

**Provider legal protections** .......................................................................................................... 6
1) **Introduction**

The purpose of this manual is to set forth the written standards and criteria that the Data and Quality Assurance (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 following written standards and criteria that investigate the quality of health care through the review of professional practices, training and experience, patient cases or conduct of licensed health care providers or encourage proper utilization of health care services and facilities.

The collection of Arizona EMS and Trauma data currently occurs through two systems: the Arizona Pre-hospital Information & EMS Registry System (AZ-PIERS) and the Arizona State Trauma Registry (ASTR). AZ-PIERS collects pre-hospital information from participating EMS agencies comprised of ambulance, fire, and tribal agencies. ASTR collects information from participating hospitals comprised mostly of designated trauma centers.

As the ADHS QA staff progresses in linking and managing EMS data from internal, external, local, state and national sources, its ability to provide useful reports integrating the data for state QA purposes will increase. Progress on data linkages will be updated through this manual on a regular basis.

2) **AZ-PIERS**

The intention of the AZ-PIERS system is to measure and improve the performance of EMS care in Arizona through a QA policy. The inclusion criteria for AZ-PIERS are all EMS calls including inter-facility transfers, cancelled calls, stand-by calls, 911 calls, etc. All identifiable data collected by an agency belongs to that agency. Unless approval is received from the agency representative granting approval of the access or release of data, it must remain protected and accessible only by that specific agency and ADHS QA staff.

*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 coordinator 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. 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 the 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.

**Maintenance of AZ-PIERS records:**
Agencies have the ability to modify their records one month after the submission 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. As agreed upon in contract with ImageTrend, all records will be maintained indefinitely. ADHS also maintains records as part of the report writing process. Agencies will also have the ability to access their data. Notices will be given to agencies prior to the removal of any records.

**AZ-PIERS Data Process:**
Pre-hospital 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.
3) **ASTR**

The intention of the ASTR system is to measure and improve the performance of trauma centers in the state of Arizona through a QA policy. The ASTR patient inclusion criteria can be found on the BEMSTS website and has been established by the State Trauma Advisory Board (STAB) and the Trauma and EMS Performance Improvement committee (TEPI). Unless approval is received from the hospital representative granting approval of the access or release of data, it must remain protected and accessible only by that specific hospital and ADHS QA staff.

**Hospital access to ASTR:**

To gain access to the ASTR system, hospitals must fill out the required application. All applications are submitted to the ASTR data manager. After initial granting of access the hospital's liaison will be responsible for informing the ASTR data manager of changes in user status. New users must fill out the required paperwork and email/fax/mail to the ASTR data manager. Hospitals may access all of their identifiable data through the state but are limited to de-identified data from other participating hospitals.

Agencies 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. ADHS will maintain all records in their servers to the best of their ability. Notice will be given to hospitals prior to removal of any records.

**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. Agencies 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 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.

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

**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 confidentiality 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.

5) **Data presentation:**

**Reports to data contributors:**
Reports are regularly provided to participants on a quarterly basis to assist in their performance improvement initiatives. The reports are scheduled to be sent 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 may not receive other agency’s data unless authorized by that organization.
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 has been removed from all reports that are distributed to the public. 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 performance improvement 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 data to NEMSIS national elements as of June 3, 2013, for 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 Department of health. The additional level of protections on the EMS and Trauma Center registries must be considered with collaborative efforts. Data is de-identified outside of DQA and is protected per ADHS policy and the policies outlined in this manual.
All identifiable data collected by a hospital/agency belongs to that agency. Unless approval is received from the hospital/agency representative granting approval of the access or release of data, it must remain protected and accessible only by that specific hospital/agency and ADHS QA staff.

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 DQA sections works closely with the Strategic Planning and Communications Section for grant funding projects. Care in protecting individual level data is maintained and is not reported on grant applications. Data is de-identified outside of ADHS QA staff and is protected per ADHS policy and the policies as outlined in this manual.
All identifiable data collected by a hospital/agency belongs to that hospital/agency. Unless approval is received from the hospital/agency representative granting approval of the access or release of data, it must remain protected and accessible only by that specific hospital/agency and ADHS QA staff.

**Research data requests:**
DQA is required to maintain the ability for individuals to conduct research using AZ-PIERS and ASTR data. Data that is requested from registries that are not from AZ-PIERS or ASTR is unable to be processed by DQA staff; these requests must go to the appropriate data owner.

Entities requesting data for research purposes that require record-level protected health information (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 for any data that is requested which coincides with the stringent approval criteria of the HSRB. Information on the HSRB review process can be found here. The data elements that are available for research can be found on the AZ-PIERS homepage and the ASTR homepage.

All requests for ASTR or AZ-PIERS data, whether aggregate or PHI, must be submitted to the DQA Section using BEMSTS approved data request forms.

6) **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.

7) Provider legal protections
All data received by the ASTR and AZ-PIERS are confidential, not subject to civil discovery or subpoena, and are not medical records under Arizona Revised Statutes (A.R.S.) §§ 36-2220, 36-2221, 36-2400, et seq., and § 12-2291 on the basis that the ASTR AZ-PIERS, and data therein, are part of a quality assurance process. Pursuant to A.R.S. § 12-2291, materials prepared in connection with quality assurance activities are not medical records. Because ASTR and AZ-PIERS data are strictly part of a quality assurance process, the Bureau of EMS and Trauma System cannot utilize ASTR or AZ-PIERS data for enforcement purposes at any level.