



LOUISIANA
EMERGENCY
RESPONSE
NETWORK

**USER & TRAINING MANUAL FOR
NON IMAGETREND TRAUMA
REGISTRY USERS**

Powered by
 **IMAGETREND**

TABLE OF CONTENTS

Introduction, Mission Statement.....	4
Introduction to the Louisiana State Bridge Web Application.....	5
Submission Guidelines.....	5
Purpose of the State EMS Registry.....	6
System Requirements.....	6
User Assistance Availability.....	7
Computer Security Awareness Requirements.....	8
Image Trend Specific Security Information.....	8
Application Securities.....	8
Secure User Login.....	8
Password Encryption.....	9
Password Requirements.....	9
Login Expirations.....	9
Page Access Checking.....	9
SSL Server Certificate.....	9
User Status.....	9
User Securities.....	9
View Patient Identifiable Information.....	9
Staff Runs Restriction.....	9
Access to Run Report.....	9
Export Security.....	9
Permissions Administration.....	10
Manage Users and Groups.....	10
Permissions and Rights.....	10
Procedural Securities.....	10
Personnel.....	10
Hosting Environment.....	10
Auditing.....	11
System Administrator.....	12
Facility Administrator.....	12
Employee Access.....	13
User Logon Request Forms.....	13
Password Regulations.....	13
Training.....	13
Initial Passwords.....	13
Changing Passwords.....	13
Oversight.....	14
Security Measures Related to Application.....	14
Code Backups.....	14
Database Backups.....	14
Restore Procedures.....	15
Louisiana State Bridge Data Elements.....	15
Data Submission Process.....	22

TABLE OF CONTENTS (continued)

Appendix A: Business Associate Agreement Reference.....34

Appendix B: Data Participation Agreement Reference.....40

Appendix C: User Logon Request Form.....44

References.....47



Right Place. Right Time. Right Care.

Introduction

Louisiana Emergency Response Network's (LERN) vision and mission statement reflect the intent of our enabling legislation and the Board's commitment to building a comprehensive statewide trauma system that meets national model standards and requirements established by the American College of Surgeons Committee on Trauma (ACS COT).

Our Vision

To build and oversee a comprehensive trauma system for the State of Louisiana

Our Mission

To defend the public health, safety, and welfare by protecting the people of the state of Louisiana from unnecessary deaths and morbidity due to trauma and time-sensitive illnesses.

Louisiana EMS State Registry Bridge User and Instructional Training Manual for Non Facility Based Image Trend Trauma Registry Users

This manual will explain: HOW TO ENTER DATA INTO THE WEB BASED EMS STATEWIDE REGISTRY APPLICATION

INTRODUCTION TO THE LOUISIANA STATE BRIDGE WEB APPLICATION

The Louisiana State Bridge (LSB) is an automated web based system called Image Trend Patient Registry and it is used to collect and analyze information on the incident, severity, cause, and outcomes of trauma patients to evaluate factors and the health system's response. The goal of the Image Trend Patient Registry is to gather information more efficiently in order to better analyze treatment methods to reduce morbidity and mortality.

The Image Trend Patient Registry is a database driven web application based on Microsoft SQL Server allowing for secure access from anywhere at any time to authorized persons. Information gained through research has significantly contributed to evidence-based medicine which has helped providers improve procedures and outcomes. The management process of trauma is complex, involving both the pre-hospital and in hospital phases and many medical disciplines.

The Facility Based Image Trend Patient Registry user will benefit from the quality assurance tools provided. Quality patient care requires involvement of all levels of the system in monitoring the relationship and process of care. This system incorporates quality assurance / quality improvement tools to support peer review monitoring within a secure environment. This discretion promotes confidence, understanding, and patience for change. This confidential information is ONLY seen and accessible by the individual facility, and not by LERN, or other LSB employees.

SUBMISSION GUIDELINES

EMS providers that have been approved and given access to the "UPLOAD" function for the LSB should submit on a monthly basis at a minimum. In compliance with national standards set forth by the National EMS Information System, 80% of all trauma patient records must be entered into the LSB within 30 days from transport date. LERN's standard for completion is 100% of all trauma patient records into the LSB within 60 days from transport date.

An example of a yearly reporting schedule is provided below in Table 1 for agencies who are not submitting data live.

TABLE 1

Month	Submission Deadline
January Data	March 1
February Data	April 1
March Data	May 1
April Data	June 1

PURPOSE OF THE STATE EMS REGISTRY

The purpose of the state trauma registry is to mine the data for what it can tell us – registry data can be coded, compiled, analyzed, and reported. A state registry is an important management tool that is used for performance management and improvement, research, and injury prevention.

Louisiana’s statewide registry was authorized by the Louisiana Legislature in 2010. The legislation charges the LERN Board to “establish and maintain a statewide trauma registry to collect and analyze data on the incidence, severity, and causes of trauma, including traumatic brain injury. The registry shall be used to improve the availability and delivery of pre-hospital or out-of-hospital care and hospital trauma care services.”

SYSTEM REQUIREMENTS:

The following system specifications and recommendations are for all EDS Web-based solutions.

Network Requirements

Networking: Any TCP/IP Network may be used, including wired and wireless technologies. An Internet connection to the server may be required for remote access and remote data posting.

Operating Systems Supported

Windows 2003 Server with IIS version 6.0 (minimum)

Windows 2008 Server R2 with IIS version 7.5 (recommended)

**Windows 2008 Server RTM not supported

Web Server Hardware (not required if hosted by ImageTrend)

Required:

1 GHz Processor or better

3 GB RAM

20 GB Available Hard Disk Space

Recommended:

Dual 2 GHz Processors or better

4 GB RAM or more

50 GB Available Hard Disk Space

RAID 5 SCSI Hard Drives

ImageTrend Hosted:

Quad 2 GHz Processors

8 GB RAM

100 GB Available Hard Disk Space
RAID 5 SCSI Hard Drives

Server Database (not required if hosted by ImageTrend)

Microsoft SQL Server 2005 (minimum)
Microsoft SQL Server 2008 R2 (recommended)

Required:

Dual 2 GHz Processors or better
4 GB RAM or more
50 GB Available Hard Disk Space
RAID 5 SCSI Hard Drives

Additional Software Required (not required if hosted by ImageTrend)

Adobe ColdFusion 8 Standard or Enterprise Server (minimum)
Adobe ColdFusion 9 Standard (smaller services) or Enterprise Server (50,000+ annual incidents) (recommended)
Microsoft .NET Framework 3.5 SP1
Microsoft Tablet PC SDK

Internet Browser Requirements for End Users

Microsoft Internet Explorer 6.0 and above
Other browsers that support Mozilla 4.0 and above
Adobe Flash 8 or higher (recommended)
Adobe Reader 8 or higher
Microsoft Silverlight 4.0

USER ASSISTANCE AVAILABILITY

LERN and its staff will serve as Louisiana’s system administrator. The actual on-line web application contains a user’s guide which can be accessed by clicking on the “HELP” button in the upper right corner. This will bring the user to the Image Trend University. Here you will find a complete user’s guide, as well as several short educational videos on the Image Trend Patient Registry. You will find materials for administrators, users, and trainers to use including:

- Educational Videos
- Downloadable Manuals
- Downloadable Quick Guides
- Downloadable Workbooks
- Education-oriented PowerPoint
- Presentations

Common symbols, buttons, and shortcuts are available in the downloadable manual, as well as clear directions on log on / log off / and password changes.

At anytime the individual facility may also contact LERN for questions. Additionally, under the Image Trend contract with LERN facilities may also the following centers for support:

Imagetrend at 888-469-7789 or support@imagetrend.com
LERN at 866-320-8293
LA Rural Ambulance Alliance (LRAA) at 225-612-3177

COMPUTER SECURITY AWARENESS REQUIREMENTS FOR LSB APPLICATION – USERS:

A. All application-users are required to read the below computer security awareness best practices policies and agree to abide by them when signing the LERN LSB application user Access and Confidentiality agreement.

B. All application-users must be aware that:

1. Application-users are not permitted to share passwords except for web page saver passwords and then only when management documents, in writing, that it is necessary to share.
2. Application-users must locate their desktops / laptops in a direction that does not permit unauthorized individuals to view client information.
3. Application-users must use password-protected desktops / laptops when accessing personal health information (PHI) of clients.
4. Application-users must ensure that Virus Protection is implemented on all desktops / laptops.
5. Application-users must log out of the LERN LSB trauma application when their terminal or computer is going to be left idle and unattended for a significant period of time.

IMAGE TREND SPECIFIC SECURITY INFORMATION

Image Trend applications meet or exceed state and federal data privacy requirements and the HIPAA guidelines. Secure logins are an industry standard process and are part of the HIPAA guidelines for data protection. These are implemented throughout the application with the use of the hierarchical security access features of the ImageTrend security module, which provides the environment for controlling the access necessary to provide data protection. The application also provides for security breach notifications and audit trails.

Application Securities

Secure User Login

The application adheres to business standard practices for security to ensure only authorized access to the system.

Password Encryption

Hash function implementation
For sessions failing to successfully login after three tries
Check access log for sequential unsuccessful logins
Set session logout variable

Password Requirements

Length and Complexity Enforcement
Validate Password for Case, Length (8 characters), and Composition

Login Expirations

Validate for expired logins
Force password changes on expired logins and restrict site access until new, valid password is created

Page Access Checking

Page Access checking to make sure user has properly logged in and is not entering the site via an external link.

SSL Server Certificate

128-bit encryption Security Certificate

User Status

Users can be inactivated to restrict access to the site but still maintain data integrity.

User Securities**View Patient Identifiable Information**

On each user record permissions can be set to view or not view patient identifiable information.

Staff Runs Restriction

Agency staff can be restricted to only see the runs that they have entered or were one of the crew members on that run.

Access to Run Report

The ability to view, add, change, or delete runs are also controlled on an individual basis.

Export Security

Exports are maintained and controlled by system administrators.

Permissions Administration

Manage Users and Groups

The application employs a hierarchical based password administration as a series of group policies to control application entry and level of access within the application. With the system administrator being the highest level of security, groups can be created below that to encompass all other group needs, which may include:

- Director – Access to view all runs within their agency.
- Multiple Service Administrators – User access and administration to multiple services.
- Individual – Access to enter records within their agency

Permissions and Rights

Permission and rights are governed by the ability of what the user can see and do. At the global level, rights are typically based on the following criteria:

- County
- City
- Agency

On the service level, there are typically two levels:

- Agency Administrator
- Individual User

Service administrators can control and edit all the functions within their own service.

Procedural Securities

Personnel

All Image Trend employees are subjected to background checks and are required to attend and successfully complete HIPAA training. The Image Trend Project Management System gives us a facility to track any HIPAA Security Incidents or Information Disclosure Incidents for reporting purposes.

Only those certified Image Trend employees that work with either hardware or software related to the specified application or project will access the data center and interact with our servers. These employees have worked with our hardware as part of our IT support staff or are part of our Implementation team as software developers. Authorization is granted from the management.

Hosting Environment

Image Trend's Web applications are hosted in their state-of-the-art 4,500 square foot data center. Built in a vault with 21" concrete walls, their facilities offer the maximum level of security and stability for hosting needs. The data center features triple redundant, high-speed internet connections over fiber optic trunk lines. Only

authorized personnel have access to the data floor. The data center is monitored electronically, as well as a log book to monitor and record individuals accessing the server room.

Image Trend's production network consists of application/web and database servers. The databases are on a private network with access control managed through the firewall permitting only authorized administrators or approved VPN access.

Applications are monitored for availability and performance from multiple locations to ensure an accurate measure of current system health. Slow application pages and long running database queries are logged for analysis by server administrators and development staff. Serious errors and performance degradation trigger email alerts which are sent to support staff and cell phone alerts to Image Trend's 24/7 X-Team Support staff. Their X-Team support employees have VPN access to our production servers to ensure accessibility and security when accessing our servers from outside of our network.

Auditing

The Patient Registry's audit trail tracks user information when accessing the secure portion of the application. The IP address, User ID, date/time, browser information, and information on each file accessed is all tracked within a separate database, which is kept for a period of time for reporting purpose and audit trails.

Any security breaches are logged within our Project Management system for any HIPAA disclosures related to security breaches or information disclosers. If a security breach happens, the security module currently sends an email to their Director of Development and the Security Officer, who in turn notifies the designated customer contact.

This setup can be controlled at the Facility Administrator level. When the "Track all changes after completed" is active a "Mark as Complete" button will appear on the top of the form. Once a registrar has completed entering the information for an incident they can click this button to lock the form and enable field level audit tracking. Audit information is displayed on the "History" record that is associated with each incident. This information can be accessed from the Incident History page or directly from the incident form.

Audit Events Setup			
Select the events to be audited and the reason required message that will be prompted when the event is triggered. The reason required message will only be prompted if "Is Reason Required?" column is set to "Yes".			
Event	Status	Is Reason Required?	Reason Required Message
Generate PDF Reports:	Active ?	<input checked="" type="radio"/> Yes <input type="radio"/> No	Please Explain the Reason for Generating a PDF of this Patient Registry Incident.
View Existing Online Report:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive	<input checked="" type="radio"/> Yes <input type="radio"/> No	Please Explain the Reason for accessing this Patient Registry Incident.
Track All Changes After Completed:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive		

Additional Audit Workflow Configurations	
Mark Runs as Completed Upon Locking Them	<input checked="" type="radio"/> Yes <input type="radio"/> No ?
Update Status Upon Marking Run As Completed	<input checked="" type="radio"/> Yes <input type="radio"/> No ?
Select Status To Update To	Requires Review ▾

SYSTEM ADMINISTRATOR:

LERN or its representative will serve in the capacity of system administrator. In this role, all of the facility will be enrolled in the LSB upon completion of Access/Security User Logon Request Forms. A facility profile including hospital pertinent information will be completed and a facility administrator will be named. The LERN system administration will maintain the highest level of access into the LSB as allowed by Image Trend and will be able to review data in compliance with the Data Users Agreement for all facilities.

AGENCY ADMINISTRATOR:

An agency administrator is the lead contact at an individual EMS agency. The agency administrator will be responsible for enrolling their own local staff for access into the LSB. The agency administrator will be able to grant different levels of access to these staff members depending on their job titles and responsibilities. The agency administrator will be allowed full access to their individual facility data, but will be unable to view any other agency information in the LSB.

EMPLOYEE ACCESS:

Employee access is granted to an employee or staff member at an individual EMS agency by the agency administrator. This access will be limited related to their job title and responsibilities, and will be for their individual agency data only. The agency administrator has the right / authority to limit access, or terminate access as established by their facility. The LERN system administrator will not have the authority to set up agency employees. It will be the responsibility of the agency administrator.

USER LOGON REQUEST FORMS:

Please see Appendix C for Access and Confidentiality of Records agreement and User Logon Request Forms. These forms are to be completed by the facility administrator to gain access and privileges to the LSB and returned to the LERN System Administrator. All employee requests will be completed and returned to the Facility Administrator.

NOTE: Each user must complete both forms.

PASSWORD REGULATIONS:

HIPAA PASSWORD REGULATIONS:

The Health Insurance Portability and Accountability Act (HIPAA) is a comprehensive piece of legislation passed by the United States Congress. In 2003 a section was added known as the Security Rule, which establishes national standards for protecting the privacy of individuals who partake in electronic healthcare transactions. The HIPAA Security Rule also includes regulations for password management by the healthcare provider. The act gives database administrators flexibility in establishing password regulations, but it does require them to take certain basic steps.

TRAINING

The act requires that administrators of healthcare databases train their employees in password management and how to create a strong password. The act does not make specific requirements on the length of the password that employees create.

INITIAL PASSWORDS

When healthcare employees are originally given access to a password, the password must be randomly generated.

CHANGING PASSWORDS

Employees must change their passwords every 90 to 120 days, and they also must change their passwords after they initially log in with the randomly generated password. Database administrators must clearly define to users the procedure for resetting passwords.

OVERSIGHT

Administrators must create a system that logs computer usage and automatically flags attempts to access healthcare databases. Additionally, even after logging in with their passwords, employees shall have no expectation of privacy when using a healthcare database.

IMAGE TREND PASSWORD SET UP

Time Suspend:	120	Number of days without login to the application before the user's account is suspended
Password Attempts:	4	Number of attempts a user can attempt to login before their account is placed on temporary suspend
Numeric Characters:	1	Number of numeric characters required in the user's password
Special Characters:	0	Number of special characters required in the user's password
Change Password Time:	0	Time in hours that a user cannot change their password after last change
Account Password:	10	Number of past passwords stored in the log table for a user
Password Compare:	10	Number of passwords in the log table to be compared with the newest password to see if the same password is being used
Password Length:	7	Minimum number of characters in the password

SECURITY MEASURES RELATED TO APPLICATION SYSTEM BACKUP

Code Backups

Application code is backed up daily; at least a daily backup exists for all applications hosted in Image Trend's production environment and is included in hosting costs. These backups are retained for particular customers as needed on a weekly, monthly, quarterly, or annual basis as agreed to by contract. Daily backups are retained for longer as unallocated storage permits but not guaranteed to be available beyond the previous calendar day. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to Image Trend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Database Backups

Database files are backed up daily; at least a daily backup exists for any database hosted in Image Trend's production environment and is included in hosting costs. Daily backups are retained for several days as unallocated storage permits but not guaranteed to be available beyond three previous calendar days. Database backups are retained for particular customers as needed on a weekly, monthly, quarterly, or annual basis as agreed to by contract. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data

synchronization is run across a secure network connection back to Image Trend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Restore Procedures

Daily backup files are stored uncompressed to facilitate quick recovery of one or more files as needed. Archive copies are compressed to conserve disk space. All database files are compressed to conserve disk space and must be uncompressed and reattached for restoration. When restoring a file the newer file, if it exists, is renamed and kept before replacing with the backup version. When restoring an entire database file, the copy being replaced is itself backed up before being modified. When restoring part of a database file, the current file is first backed up and the backup database is mounted with a different name, then the needed tables are restored and the backup file is detached. If restoring a complete backup of application code over a corrupted install, a copy of the bad files is kept to maintain any new user-added files since the backup was created.

LOUISIANA STATE BRIDGE DATA ELEMENTS:

LERN, in conjunction with state and national stakeholders, has adopted the National EMS Information System (NEMSIS) as its LSB data elements. NEMSIS stands for the National Emergency Medical Services Information System. NEMSIS is the national repository that will be used to potentially store EMS data from every state in the nation. Since the 1970s, the need for EMS information systems and databases has been well established, and many statewide data systems have been created. However, these EMS systems vary in their ability to collect patient and systems data and allow analysis at a local, state, and national level.

Each individual provider registry will likely collect additional variables important to patient care. However, the LSB data elements are required and should be collected by all providers.

EMS Agency Number
EMS Agency Name
EMS Agency State
EMS Agency County
Primary Type of Service
Other Types of Service
Level of Service
Organizational Type
Organization Status
Statistical Year
Total Service Size Area
EMS Agency Time Zone
EMS Agency Daylight Savings Time Use
National Provider Identifier
Agency Contact Last Name
Agency Contact Middle Name/Initial
Agency Contact First Name
Agency Contact Address

Agency Contact City
Agency Contact State
Agency Contact Zip Code
Agency Contact Telephone Number
Agency Contact Fax Number
Agency Contact Email Address
Agency Contact Web Address
Agency Medical Director Last Name
Agency Medical Director Middle
Name/Initial
Agency Medical Director First Name
Agency Medical Director Address
Agency Medical Director City
Agency Medical Director State
Agency Medical Director Zip Code
Agency Medical Director Telephone
Number
Agency Medical Director Fax Number
Agency Medical Director's Medical
Specialty
Agency Medical Director Email Address
State Certification Licensure Levels
EMS Unit Call Sign
Zones
Procedures
Medications Given
Patient Care Report Number
Software Creator
Software Name
Software Version
EMS Agency Number
Incident Number
EMS Unit (Vehicle) Response Number
Type of Service Requested
Type of Dispatch Delay
Type of Response Delay
Type of Scene Delay
Type of Transport Delay
EMS Unit Call Sign (Radio Number)
Complaint Reported by Dispatch
Crew Member Level
Incident or Onset Date/Time
PSAP Call Date/Time
Dispatch Notified Date/Time
Unit Notified by Dispatch Date/Time

Unit En Route Date/Time
Unit Arrived on Scene Date/Time
Transfer of Patient Care Date/Time
Unit Left Scene Date/Time
Patient Arrived at Destination Date/Time
Last Name
First Name
Middle Initial/Name
Patient's Home Address
Patient's Home City
Patient's Home County
Patient's Home State
Patient's Home Zip Code
Patient's Home Country
Social Security Number
Gender
Race
Ethnicity
Age
Age Units
Date of Birth
Primary Method of Payment
Insurance Company ID/Name
Work-Related
Patient's Occupational Industry
Patient's Occupation
Condition Code Number
ICD-9 Code for the Condition Code Number
Condition Code Modifier
Date/Time Initial Responder Arrived on
Scene
Number of Patients at Scene
Mass Casualty Incident
Incident Location Type
Scene GPS Location
Incident Address
Incident City
Incident County
Incident State
Incident ZIP Code
Prior Aid
Prior Aid Performed by
Outcome of the Prior Aid
Possible Injury
Chief Complaint

Duration of Chief Complaint
Time Units of Duration of Chief Complaint
Secondary Complaint Narrative
Duration of Secondary Complaint
Time Units of Duration of Secondary Complaint
Chief Complaint Anatomic Location
Chief Complaint Organ System
Primary Symptom
Other Associated Symptoms
Providers Primary Impression
Provider's Secondary Impression
Cause of Injury
Intent of the Injury
Mechanism of Injury
Vehicular Injury Indicators
Area of the Vehicle impacted by the collision
Seat Row Location of Patient in Vehicle
Position of Patient in the Seat of the Vehicle
Use of Occupant Safety Equipment
Airbag Deployment
Height of Fall
Cardiac Arrest
Cardiac Arrest Etiology
Resuscitation Attempted
Arrest Witnessed by
First Monitored Rhythm of the Patient
Any Return of Spontaneous Circulation
Estimated Time of Arrest Prior to EMS Arrival
Date/Time Resuscitation Discontinued
Reason CPR Discontinued
Cardiac Rhythm on Arrival at Destination
Advanced Directives
Medication Allergies
Environmental/Food Allergies
Medical/Surgical History
Medical History Obtained From
Current Medications
Current Medication Dose
Current Medication Dosage Unit
Alcohol/Drug Use Indicators
Pregnancy
Date/Time Vital Signs Taken

Obtained Prior to this Units EMS Care
Cardiac Rhythm
SBP (Systolic Blood Pressure)
DBP (Diastolic Blood Pressure)
Method of Blood Pressure Measurement
Pulse Rate
Electronic Monitor Rate
Pulse Oximetry
Pulse Rhythm
Respiratory Rate
Respiratory Effort
Carbon Dioxide
Blood Glucose Level
Glasgow Coma Score-Eye
Glasgow Coma Score-Verbal
Glasgow Coma Score-Motor
Glasgow Coma Score-Qualifier
Total Glasgow Coma Score
Level of Responsiveness
Pain Scale
Stroke Scale
Thrombolytic Screen
Date/Time of Assessment
Skin Assessment
Head/Face Assessment
Neck Assessment
Chest/Lungs Assessment
Heart Assessment
Abdomen Left Upper Assessment
Abdomen Left Lower Assessment
Abdomen Right Upper Assessment
Abdomen Right Lower Assessment
GU Assessment
Back Cervical Assessment
Back Thoracic Assessment
Back Lumbar/Sacral Assessment
Extremities-Right Upper Assessment
Extremities-Right Lower Assessment
Extremities-Left Upper Assessment
Extremities-Left Lower Assessment
Eyes-Left Assessment
Eyes-Right Assessment
Mental Status Assessment
Neurological Assessment
Protocols Used

Date/Time Medication Administered
Medication Administered Prior to this Units
EMS Care
Medication Given
Medication Administered Route
Medication Dosage
Medication Dosage Units
Response to Medication
Medication Complication
Medication Authorization
Medication Authorizing Physician
Date/Time Procedure Performed
Successfully
Procedure Performed Prior to this Units
EMS Care
Procedure
Size of Procedure Equipment
Procedure Successful
Procedure Complication
Response to Procedure
Procedure Authorization
Procedure Authorizing Physician
Destination/Transferred To, Name
Destination/Transferred To, Code
Destination Street Address
Destination City
Destination State
Destination County
Destination Zip Code
Incident/Patient Disposition
Condition of Patient at Destination
Reason for Choosing Destination
Type of Destination
Closest Receiving Bypassed?
If Bypassed, why?
Event Date/Time
ECG Lead
ECG Interpretation
Type of Shock
Total Number of Shocks Delivered
Pacing Rate
Device Pulse Oximetry
Device CO2 or etCO2
Device CO2, etCO2, or Invasive Pressure
Monitor Units

Law Enforcement/Crash Report Number
Trauma Registry ID
Potential Registry Candidate
Who Generated this Report?
Potential Registry Candidate

LSB Data Elements: ***for full definitions PLEASE go to**
<http://www.nemsis.org/v2/downloads/datasetDictionaries.html> and download a copy of the
National EMS Information System's Data Dictionary for the current year of datasets.



EMS STATE BRIDGE

VERSION 5.1

IMPORTING NEMSIS XML FILES

ImageTrend, Inc.
20855 Kensington Blvd.
Lakeville, MN 55044
Tel: (952) 469-1589
Toll Free: (888) 469-7789
Fax: (952) 985-5671
www.imagetrend.com



Copyright

EMS State Bridge Version 5.1

Copyright © 2012 ImageTrend, Inc. All rights reserved.

EMS State Bridge

Viewer contains copyrighted materials licensed from various copyright owners.

EMS State Bridge

Viewer contains copyrighted materials, which are licensed to you, the end user, for your personal use subject to the terms of the enclosed end user license agreement. You must treat this software and its contents like any other copyrighted material, such as a Portfolio or musical recording. Any other use, duplication, or distribution of this product or its contents may violate applicable U.S. or international copyright laws, and may subject you to prosecution under penalty of law.

State Bridge logo is a registered trademark, and is a trademark of ImageTrend, Inc.

NOTICE Unless otherwise provided by written agreement with ImageTrend, Inc., this publication, and the software sold with this publication, are provided “as is” without warranty of any kind either expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. The entire risk arising out of the user or performance of this publication and software remains with you. In no event will ImageTrend, Inc., or any of its suppliers, be liable for any lost profits, lost savings, direct, incidental or indirect damages or other economic or consequential damages, even if ImageTrend, Inc. or its suppliers have been advised of the possibility of such damages. ImageTrend, Inc. reserves the right to modify this document at any time without obligation to notify anyone.

Introduction

If you use a third party (non-ImageTrend) software to collect your EMS runs, you must upload the incident information to the State Bridge as a NEMSIS-compliant XML file. The ability to upload is based on your level of access to the system. If you do not have access to upload a file, please contact your system administrator.

Getting Started

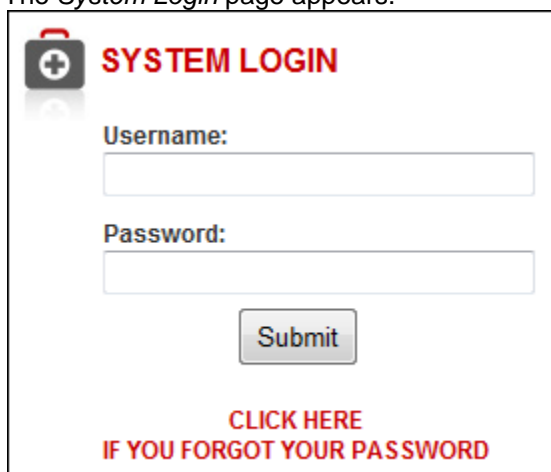
Submitting data via the NEMSIS XML data exchange requires (at a minimum) that users submit a XML file that follows the NEMSIS guidelines for structure and values. This may also include NISE values over and above NEMSIS, or state-specific requirements. Please contact your state administrator for additional information.

To generate a XML file from your software, please check with your vendor on how to export out a NEMSIS XML file. You may need to do some configuration within your software, and all files must have an .xml extension to be imported. Go to <http://www.nemsis.org> for a list of certified vendors.

Logging in to the State Bridge

Before you can work with the State Bridge system in any way or access any information, you need to log in to the system. The state has assigned you a username and password that will allow you to access the system. If you do not have a username and password, you should contact your service or state administrator; only they will have the authority to provide you with login information.

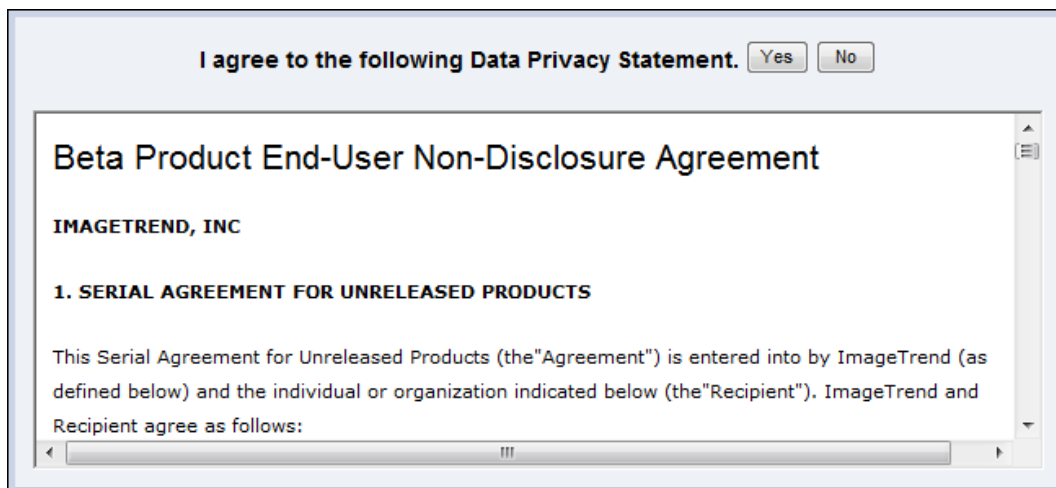
1. Using a Web browser, navigate to the URL for the service's State Bridge system. The *System Login* page appears.



2. In the *Username* field, type your username.
3. In the *Password* field, type your password.
4. Click *Submit* or press *Enter*.

Data Privacy Agreement

Once logged in, all users are required to read and agree to the terms of the Data Privacy Statement regarding all data related to services, users and patients on the site. Agreeing to the terms automatically creates a user history and audit trail of site access to comply with HIPAA requirements.




Security Questions

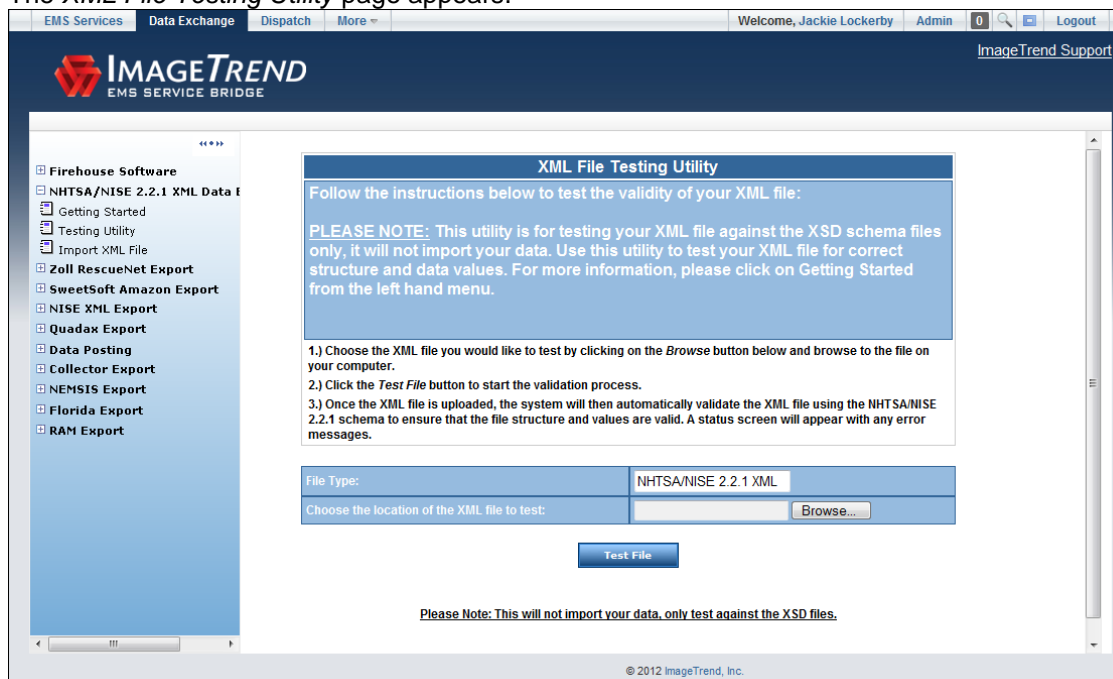
If the security question option is enabled, users will need to complete a security question before being able to access the State Bridge. These questions will be answered the first time the user logs in to the application and those answers will be required for any further logins in the future.

Testing Import Files

Before importing an XML file, you can use the testing utility to test the validity of the file. This utility is for testing your XML file against the XSD schema files only; it will not import your data. Use this utility to test your XML file for correct structure and data values.

1. From the top left, click *Data Exchange*.
 **HINT:** If you do not see the *Data Exchange* link in the upper left, it may be hidden under the *More* link. If this is the case, click *More* to expand the menu and then click *Data Exchange*.
2. From the left menu, click *NHTSA/NISE 2.2.1 XML Data Exchange*.
A sub-menu appears on the left side.

3. Click *Testing Utility*.
The *XML File Testing Utility* page appears.



4. Click *Browse...*
The *Choose File* dialog box appears.
 5. Navigate to and select the XML file to test,
 6. Click *Open*.
 7. Click *Test File*.
A status screen appears with a list of any errors.
- ⚠ WARNING:** This utility will process but will not import your file.

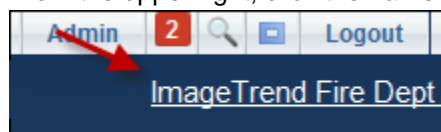
Importing XML Files

Ambulance service administrators can use the Data Exchange to import XML files for NHTSA and NISE 2.2.1. In order to properly import a file, the service profile must be set up correctly and the times must be formatted correctly within the file being imported.

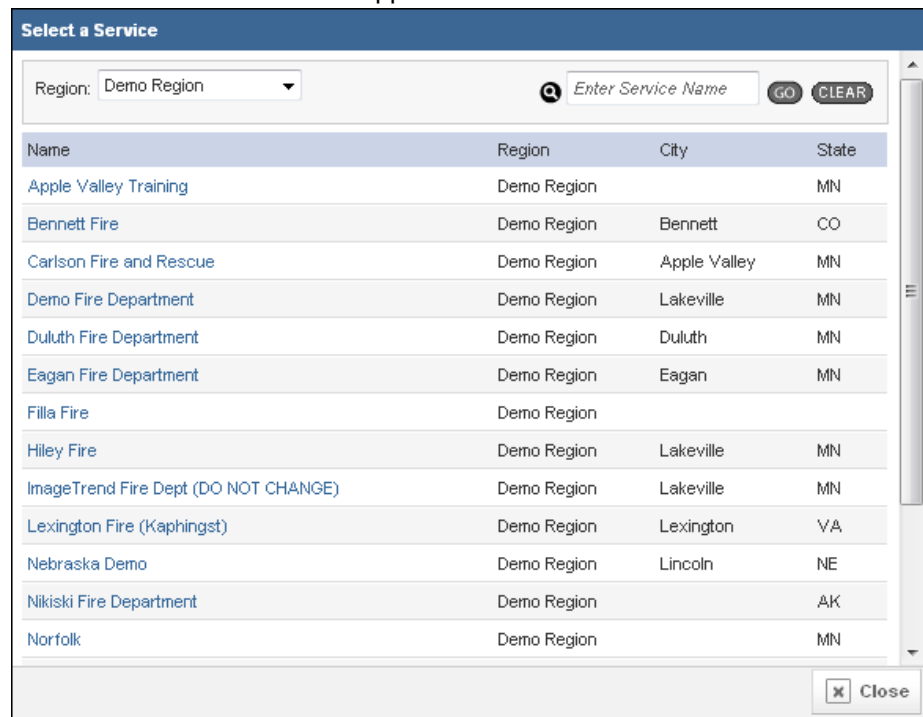
Setting Up Your Service for Importing

In order to properly import a file and to maintain the correct times, your service must have its time zone and compliance to daylight savings time recorded in the *Setup* section. This section will explain how to change these settings. You will also need to know whether your software vendor is converting your response times to UTC time (also known as Zulu time or GMT).

1. From the top left, click *My Service* or *EMS Services*.
2. If needed, to change the service you are setting up,
 - a. From the upper right, click the name of the currently displayed service.



The *Select a Service* window appears.




- b. As needed, from the *Region* drop down menu in the upper left, select the region containing the agency you want to view.
 - c. Click the name of the service.
The *Home* tab for that service is displayed.
3. Select the *Setup* tab.
The *View Service Info* page appears.




- 4. Click *Edit*.
The *Edit Service Info* page appears.

- In the *Address* section, from the *Agency Time Zone* drop down menu, select your service's time zone.

Address	
Address	20855 Kensington Blvd.
City	Lakeville
County	Dakota
State	Minnesota
Postal Code	55044
Agency Time Zone	GMT-6:00 Central Time
Daylight Saving Time Use	Yes

- In the *Address* section, from the *Daylight Saving Time Use* drop down menu, select whether your service is using daylight savings time at this time.
 **NOTE:** This information should be changed in April (to *Yes*) and November (to *No*) each year in order for the times to enter the system appropriately throughout the year, if your area uses daylight savings time.
- From the bottom of the page, click *OK*.

Importing the XML File

- From the top left, click *Data Exchange*.
 **HINT:** If you do not see the *Data Exchange* link in the upper left, it may be hidden under the *More* link. If this is the case, click *More* to expand the menu and then click *Data Exchange*.
- From the left menu, click *NHTSA/NISE 2.2.1 XML Data Exchange*.
A sub-menu appears on the left side.

3. Under *NHTSA/NISE 2.2.1 XML Data Exchange*, click *Import XML File*. The *Import Runs* page appears.

Import Runs with a NHTSA/NISE 2.2.1 XML File

Follow the instructions below to import your data using the NHTSA/NISE 2.2.1 XML Data Exchange:

- 1.) Choose the XML file you would like to use by clicking on the 'Browse' button and browse to the file on your local machine.
- 2.) Choose the agency that you are importing for. If you have rights to only one, that one will be displayed. If you have rights to more than one service, please select it from the list. If you are importing for more than one service, please select only one of the services, although data will be transferred to all services that are specified in the XML file.
- 3.) Select the format that was used for setting the time format in the XML. Choose Yes if the times are in UTC format, and No if the times have been already converted to your local time zone.
- 4.) Click the 'Import' button to start the file transfer and validation.

- Once the XML file is uploaded, a status screen will be displayed. The system will then automatically validate the XML file using the NHTSA/NISE 2.2.1 schema to ensure that the file structure and values are valid.
- If the schema validation is successful, the system will run through the import and validations routines to import your data. If problems are found, a detailed description of the issue(s) will be displayed.


For more information on NHTSA and NEMSIS XML Data models, click [here](#).

Choose the location of the XML file:

Which agency are you importing for?

Are the times in this XML file in Coordinated Universal Time (UTC), also referred to as Zulu time (Z)? If so, choose YES below to convert them to the service's time based on the Time Zone and Daylight Saving Time settings as defined within the Service Setup. If the times are already converted, choose NO. If you have questions, please contact your software vendor or the system administrator.

Yes No

4. In the *Choose the location of the XML file* section, click *Browse...*. The *Choose file* dialog box appears.
5. Using the *Choose file* dialog box, navigate to and open the desired XML file to upload.
6. From the *Which agency are you importing for* drop down menu, select the agency importing the file.
-  **NOTES:**
If you have rights to only one ambulance service, that service will be displayed and you will not be able to change it.
If the file will be used for multiple agencies, select only one of the agencies. If other agencies are included in the file, the data will also be transferred to them. The selected agency will allow the system to associate the data immediately with one agency ID.
7. In the *Are the times in this XML file...* section, if your service software vendor generates the XML file with the response times in your local time, select *No*.

OR

If your service is collecting response times in local time but your software is converting them to UTC time, select *Yes*.


 **NOTES:**

Selecting *Yes* will automatically change your collected response times from UTC (also known as Zulu time or GMT) to your service's local time to be correct when imported.

Selecting *No* will not make the conversion.

In order for the conversion to take place properly, the times must be formatted as shown in the example and your service must be set up with the correct time zone and daylight savings time settings as indicated in the *Setting Up Your Service for Importing* section.

EXAMPLE: Times in the XML file should be formatted as: **2001-12-17T09:00:00Z**

 **HINT:** The “Z” at the end is especially important, as it indicates that the time must be converted.

- In the *Select option for handling duplicate incident records* section, select the way that records with duplicate incident numbers should be handled during the import.

Overwrite

If there is only one duplicate record found, the existing record will be overwritten with the record in the import file. If there are multiple duplicate records, the existing record will remain in the system and a new record will be inserted.





Skip


If duplicate records are found, the existing record will remain in the system and no information will be imported for that record in the file.

- Click *Import*.
A *Please Wait...* window will appear while the file is uploading, followed by the *File Import Summary*.

NHTSA/NISE 2.2.1 XML File Import Summary

Your data file has transferred and validated successfully. The data will be imported automatically within the system usually within 24 hours. You can use the Data Transfer History report under your service's report section, to view updated information on the progress of this import.

Process	Status	Records	Start	Finish	Total	Run Now	View Details
+ Data Transfer	<input checked="" type="checkbox"/> Completed	n/a	04:30:59 PM	04:31:24 PM	0:0:25	n/a	
+ Data Processing	<input type="checkbox"/> Pending						
+ Validation	<input type="checkbox"/> Pending					n/a	

 Refresh

Viewing Error Details





If the file's formatting does not match the required format or if another problem arises, you may receive an error message when you try to upload your file. You can find out more information about the error if necessary.


- From the *File Import Summary* page, for the process displaying the error, click *View Details*.

NHTSA/NISE 2.2.1 XML File Import Summary

The file transfer and/or validation process has completed **with errors**. No incident data has been imported. You can view detailed information or any errors by clicking on the 'View Details' icon below.

Error Reason: Schema Validation Failed.

Process	Status	Records	Start	Finish	Total	Run Now	View Details
+ Data Transfer	 Completed w/Errors	n/a	04:21:36 PM			n/a	
+ Data Processing	<input type="checkbox"/> Pending					n/a	
+ Validation	<input type="checkbox"/> Pending					n/a	


 Refresh

















A new window appears with a list of all error details.

Type	Time	Record Number	Call Number Incident Number PCR Number	Message	Detail
Schema Validation Failed.	04:21:38 PM	0	Call:0 Inc:0 PCR:0	Severity = 0	The 'http://www.nemsis.org:E02_16' element has an invalid value according to its data type. An error occurred at , (29, 22).
Schema Validation Failed.	04:21:38 PM	0	Call:0 Inc:0 PCR:0	Severity = 0	The 'http://www.nemsis.org:E02_16' element has an invalid value according to its data type. An error occurred at , (449, 22).
Schema Validation Failed.	04:21:38 PM	0	Call:0 Inc:0 PCR:0	Severity = 0	The 'http://www.nemsis.org:E02_16' element has an invalid value according to its data type. An error occurred at , (79, 22).
Schema Validation Failed.	04:21:38 PM	0	Call:0 Inc:0 PCR:0	Severity = 0	The 'http://www.nemsis.org:E02_16' element has an invalid value according to its data type. An error occurred at , (1246, 22).
Schema Validation Failed.	04:21:38 PM	0	Call:0 Inc:0 PCR:0	Severity = 0	The 'http://www.nemsis.org:E02_16' element has an invalid value according to its data type. An error occurred at , (2022, 22).
Schema Validation Failed.	04:21:38 PM	0	Call:0 Inc:0 PCR:0	Severity = 0	The 'http://www.nemsis.org:E02_16' element has an invalid value according to its data type. An error occurred at , (2613, 22).
Schema Validation Failed.	04:21:38 PM	0	Call:0 Inc:0 PCR:0	Severity = 0	The 'http://www.nemsis.org:E02_16' element has an invalid value according to its data type. An error occurred at , (2893, 22).
			Call:0	Severity:	The 'http://www.nemsis.org:E14_06' element has an

Viewing the Data Transfer History Report

At any point, you can view a list of all XML files that were imported into the State Bridge system. This report also contains information about those files, including how many records were included in the file and whether the import was successful.

- From the top left, click *My Service* or *EMS Services*.
 **HINT:** Depending on your level of permissions, this link may be either *My Service* or *EMS Services*.
- Under the *Incidents* tab, click *Reports*.
The *Service Reports* page appears.
- Click *Data Transfer History*.
The *Data Transfer History* report appears.

Data Transfer History							
<input checked="" type="checkbox"/> = Completed  = Completed w/ Errors <input type="checkbox"/> = Pending <input checked="" type="checkbox"/> = Incomplete							
Uploaded Date	Utility	Total Records Found in File *	Total Records Imported *	User	Imported File	Import	Status Update Validation
 11/11/09 03:49 PM	XML 2.0		0	jackie lockerby	Test_Case_Paul_Bearer1.xml	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
 11/11/09 01:35 PM	ImageTrend EMS Field Bridge	1	1	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 11/11/09 01:16 PM	ImageTrend EMS Field Bridge	1	0	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/29/09 08:43 PM	ImageTrend EMS Field Bridge	2	2	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/29/09 08:42 PM	ImageTrend EMS Field Bridge	0	0	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/29/09 08:42 PM	ImageTrend EMS Field Bridge	0	0	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/29/09 08:42 PM	ImageTrend EMS Field Bridge	0	0	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/29/09 08:42 PM	ImageTrend EMS Field Bridge	1	1	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/29/09 08:42 PM	ImageTrend EMS Field Bridge	1	0	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/29/09 08:41 PM	ImageTrend EMS Field Bridge	0	0	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/29/09 08:39 PM	ImageTrend EMS Field Bridge	1	1	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/22/09 03:44 PM	ImageTrend EMS Field Bridge	1	1	Service Admin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/21/09 02:35 PM	ImageTrend EMS Field Bridge	0	0	Dave Zaiman		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/21/09 11:24 AM	ImageTrend EMS Field Bridge	1	1	Dave Zaiman		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
 10/21/09 08:49 AM	ImageTrend EMS Field Bridge	1	1	Chris Jones		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Records 1-15 of 330 [Next](#)

*** NOTES**
 1) Totals may represent more than one service's records if more than one service was uploaded at the same time.
 2) Total Records Found in File account for all records that could be found/read in from the imported data file.
 3) Total Records Imported indicates the total number of records that imported and are available through Run History and Reporting.

- If desired, to view more information about a particular record, click the *View Detail* icon .

Viewing the Imported Runs and Validation Information

Once you have imported your file, you can search the runs for the service they were imported to in order to make sure all runs imported correctly and to see the validity of each imported run. When you search for the runs you imported, you will see a list of all runs that match your search criteria. Each run will also display the validity score, which indicates the percentage of required fields that are completed in the run.

If your validity score is below the score required by the state, you can open the run and add additional information in the State Bridge.

1. From the top left, click *My Service* or *EMS Services*.
2. Under the *Incidents* tab, click *Run History*.

The *Search Run History* page appears.

3. Using the provided fields, enter all criteria to narrow down the reports that should be displayed.
 - HINT:** To display all runs entered by the signed-in user, make sure that the *Incident Date* text boxes display appropriate dates and that all other fields are empty of criteria.
4. When finished, to display a list of all run that you have created that match the set criteria, click *Search*.

The search results are displayed.

Customize Run History Page										
Val.	Status	Type	Incident Date	Incident #	Call #	PCR #	Date Entered	User Entered	Batch Print	Actions
87%	In Progress		11/11/09	AFDEMO0001	AFDEMO0001		11/11/09	Admin, Service	<input type="checkbox"/>	
84%	Completed		11/3/09		Test091103-0143	1	11/3/09	Admin, ImageTrend	<input type="checkbox"/>	
91%	Completed		11/3/09		Test091103-0142	1	11/3/09	Admin, Service	<input type="checkbox"/>	
87%	Completed		10/27/09	IOI	IOI		10/29/09	Admin, Service	<input type="checkbox"/>	
100%	Completed		10/27/09	2	2		10/29/09	Admin, Service	<input type="checkbox"/>	
98%	Completed		10/26/09	1	1		10/29/09	Admin, Service	<input type="checkbox"/>	
86%	Completed		10/26/09	091555	091555		10/29/09	Admin, Service	<input type="checkbox"/>	
92%	Completed		10/22/09	1234223	new call number 1234		10/22/09	Admin, Service	<input type="checkbox"/>	
86%	Completed		10/21/09	ImageTrend-EMS091021-00076	ImageTrend-EMS091021-00076	1321654	10/21/09	Zaiman, Dave	<input type="checkbox"/>	
95%	Completed		10/21/09	CJFREEM509100020	CJFREEM509100020		10/21/09	Jones, Chris	<input type="checkbox"/>	
96%	Completed		10/17/09	CJFREEM509100016	CJFREEM509100016		10/17/09	Jones, Chris	<input type="checkbox"/>	
91%	Completed		10/9/09	A1091009-009	A1091009-009	2	10/14/09	Sawyer, Eric	<input type="checkbox"/>	
96%	Completed		10/8/09	2987-a-987	2987-a-987		10/8/09	Kaphingst, Eric	<input type="checkbox"/>	
91%	Completed		10/8/09	1223454645	123456		10/8/09	Admin, Service	<input type="checkbox"/>	
92%	Completed		10/6/09	CJFREEM509100011	CJFREEM509100011		10/6/09	Jones, Chris	<input type="checkbox"/>	

5. To temporarily show only certain results within the list, use the drop down menus at the top of the window to select the criteria by which to filter.
6. To sort the results by a particular heading, click the desired heading. To reverse the order that the records are sorted by (e.g., to switch from sorting A–Z to sorting Z–A), click the heading again.
7. To view the desired record, click the any of the linked text in that record.

Help and Support

Before Contacting ImageTrend

Please have the following information accessible when calling ImageTrend:

- A description of your computer system.
- The name of your operating system and service pack version (if applicable).
- A description of what happened and what you were doing when the problem occurred.
- The exact wording of any error messages you see.
- Your company name and contact information.

Contacting ImageTrend

If you are unable to find the information needed to use EMS State Bridge effectively, please consult ImageTrend in any of the following ways:

- Phone (952) 469.1589
- Toll-Free (888) 469.7789
- Fax (952) 985.5671
- Web <http://support.imagetrend.com>
- Email support@imagetrend.com

ImageTrend support services are available:

Monday – Friday
8:30 a.m. to 5:00 p.m. central time

Technical Support

For 24-hour technical support, ImageTrend provides online assistance through their website and email services:

- Web <http://support.imagetrend.com>
- Email support@imagetrend.com

APPENDIX A: Louisiana Emergency Response Network

**Emergency Medical Services (“EMS”) Provider
Business Associate Agreement**

Exhibit 1

Name of EMS Provider (“Provider”):	
Provider Address:	
City, State, Zip:	
Effective Date:	

Provider participates in the Louisiana Emergency Response Network (“LERN”) Louisiana EMS Bridge Registry (“Registry”). LERN is an agency of the State of Louisiana created by R.S. 40:2841, et seq. to safeguard the public health, safety, and welfare of the people of this state against unnecessary trauma and time-sensitive related deaths and incidents of morbidity due to trauma, by establishing a comprehensive, coordinated statewide system for access to regional trauma-patient care throughout the state.

Registry is an automated web based system utilizing Image Trend Patient Registry software and is used to collect, and analyze information on the incident, severity, cause and outcomes of trauma patients to evaluate factors and the health system’s response. The goal of the Registry is to gather information more efficiently in order to better analyze treatment methods to reduce morbidity and mortality.

Provider participates in Registry in order to improve patient care through more effective processes and otherwise facilitate internal quality assurance activities.

Registry requires the Provider to disclose to LERN and for LERN to use patient ‘Protected Health Information’ (PHI) as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA requires that the Provider and LERN enter into a Business Associate Agreement to protect PHI.

I. Agreement:

(a) In addition to the permitted uses under the Participation and Data Use Agreement (“PDUA”) entered into between LERN and Provider, Provider agrees that LERN may use the PHI received for the following purposes:

- (1) As required to perform its business associate function;
- (2) To de-identify the PHI; and
- (3) To create a limited data set for use pursuant to the PDUA

(b) The Provider and LERN agree to the additional terms and provisions below in order to comply with the applicable requirements of HIPAA.

II. Definitions

Terms used, but not otherwise defined, in this Agreement will have the same meaning as those terms in the Privacy Rule. PHI will have the meaning ascribed to it in the Privacy Rule, but for the purposes of this Agreement will refer solely to PHI received from, or created or received by LERN, its agents or subcontractors, on behalf of the Provider. LERN is a Business Associate and the Provider is a Covered Entity under the terms of the Privacy Rule.

III. General Obligations of LERN

(a) LERN agrees not to use or disclose PHI other than as permitted or required by this Agreement or as required by law.

(b) LERN agrees to use appropriate safeguards to prevent use or disclosure of PHI by LERN or its agents, other than as provided for by this Agreement and will, at its own expense and at its own site, provide the equipment and software services necessary to reasonably protect and safeguard the PHI consistent with industry standards of similarly situated business associates.

(c) LERN agrees to report to the Provider any use or disclosure of PHI not authorized by this Agreement of which it becomes aware. .

(d) LERN agrees to ensure that any agent, including a subcontractor, to whom it provides PHI will agree in writing to comply with the same restrictions and conditions that apply to LERN through this Agreement.

(e) LERN agrees to make its internal practices, books and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by LERN on behalf of the Provider, available to the Secretary of the U.S. Department of Health and Human Services (“Secretary”), during reasonable business hours, for purposes of the Secretary determining the Provider’s compliance with the Privacy Rule.

(f) LERN agrees to document and account for disclosures of PHI and information related to such disclosures as would be required by the Privacy Rule if the Provider made the same or similar disclosures.

(g) LERN agrees to provide to the Provider or an Individual, within thirty (30) days, information collected in accordance with subsection (f) of this section to permit the Provider to respond to a request by an Individual for an accounting of disclosures of PHI.

(h) LERN agrees to cooperate with Provider in responding to any request by individuals for access to or amendment of PHI as required by the Privacy Rule.

(i) LERN shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that creates, receives, maintains or transmits on behalf of the Provider.

(j) LERN shall promptly report to Provider any security incident of which it becomes aware and any other use or disclosure of the information not provided for herein of which it becomes aware, have in place procedures to mitigate any harmful effects from the inappropriate use or disclosure, and mitigate, to the extent practicable, any harmful effect that is known to LERN of a use or disclosure of PHI by LERN in violation of this Agreement. Further, to the extent that such unauthorized use or disclosure constitutes a breach within the meaning of the 42 USC 17921(1) or applicable state law:

- (1) LERN shall notify Provider of the breach without unreasonable delay but in no case later than 15 calendar days after the first day on which such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate.
- (2) The notification to Provider shall include, to the extent possible, (1) the identification of each individual whose unsecured protected health information has been, or is reasonably believed by LERN to have been, accessed, acquired, used, or disclosed during the breach; (2) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (3) a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (4) any steps individuals should take to protect themselves from potential harm resulting from the breach; and (5) a brief description of what LERN is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

(k) LERN shall ensure that any agent, including a subcontractor, to whom it provides EPHI agrees in writing to implement reasonable and appropriate safeguards to protect EPHI.

IV. Additional Uses and Disclosure Provisions

(a) Except as otherwise limited in this Agreement, LERN may use PHI for the proper management and administration of LERN or to carry out the legal responsibilities of LERN.

(b) Except as otherwise limited in this Agreement, LERN may disclose PHI for the proper management and administration of LERN, provided that disclosures are required by law, or LERN otherwise obtains reasonable assurances from the person to whom the information is disclosed that the person will (i) protect the confidentiality of the PHI, (ii) use or further disclose it only as required by law or for the purpose for which it was disclosed to the person, and (iii) notify LERN of any instances of which the person is aware that the confidentiality of the information has been breached.

(c) Nothing in this Agreement will be interpreted to prevent LERN from disclosing PHI in accordance with the Privacy Rule [45 CFR 164.502(j)(1)] concerning disclosures in the public interest, or other permissible uses or disclosures by a business associate as set forth in the Privacy Rule.

V. Obligations of the Provider

(a) Provisions for The Provider to Inform LERN of Privacy Practices and Restrictions.

- (1) Provider shall notify LERN of any limitation(s) in the Provider's Notice of Privacy Practices, to the extent that such limitation may affect LERN's use or disclosure of PHI. The Provider will make its Notice of Privacy Practices available to LERN upon request.
- (2) Provider will provide LERN with any changes in, revocation of, or permission by an Individual to use or disclose PHI, if such changes affect LERN's permitted or required uses and disclosures.
- (3) Provider warrants that all disclosures of PHI made to LERN are permissible disclosures under the Privacy Rule and that no Individual has restricted disclosure so as to make the disclosure to LERN impermissible. The Provider will notify LERN of any restriction on the use or disclosure of PHI that the Provider has agreed to in accordance with the Privacy Rule [45 CFR 164.522] if such restriction affects LERN's use or disclosure of PHI.

(b) Permissible Requests by The Provider. The Provider will not ask LERN to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if undertaken by the Provider; except as otherwise provided for in this Agreement.

(c) Registry Security Tools. Provider acknowledges that the Registry system has imbedded security features. Provider agrees to:

- (1) appoint a Facility Administrator to be responsible for properly employing the security features of the Registry system; and
- (2) understand and use the security features in the Registry system.

VI. TERM AND TERMINATION

(a) Term. The Term of this Agreement will begin on the Effective Date and will remain in effect until terminated by mutual agreement of the parties or in accordance with the termination provisions in subparagraph (b) below.

(b) Termination for Cause. Either party may terminate this Agreement based on a material breach of this Agreement, provided that the non-breaching Party gives the breaching party thirty (30) days written notice of termination and the opportunity to remedy the breach, and the breach is not remedied during the notice period. Further, In the event either Party has breached a material term of this Agreement and cure is not possible, the non-breaching Party may immediately terminate this Agreement and may report the violation to the Secretary of the Department of Health and Human Services.

(c) Remedies. The Parties acknowledge that the use or disclosure of Protected Health Information in a manner inconsistent with this Agreement may cause Provider irreparable damage and that Provider shall have the right to equitable and injunctive relief to prevent the unauthorized use or disclosure and to such damages as are occasioned by such unauthorized use or disclosure in addition to other remedies available at law or in equity.

(d) Effect of Termination. Except as provided in paragraph (b) of this sub-section, upon termination of this Agreement, for any reason, LERN will, at the Provider's direction, destroy all PHI received from the Provider, or created or received by LERN on behalf of the Provider if the PHI has not yet been entered into LERN's database. LERN will retain no copies of the PHI, except to the extent that it has been entered into LERN's database.

In the event that LERN reasonably determines that destroying the PHI is infeasible due to inclusion of the PHI in LERN's database or for other legitimate reason, LERN will give the Provider a statement of reasons why the return or destruction of the PHI is infeasible. As the sole consequence of such determination, LERN will extend the protections of this Agreement to such PHI and limit further its use and disclosure to those purposes that make the return or destruction infeasible, for so long as LERN maintains such PHI.

The obligations of this sub-section (c) will survive any termination or expiration of this Agreement.

VI. MISCELLANEOUS

(a) Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended and for which compliance is required.

(b) Amendment. Any amendment to this Agreement must be in writing and signed by each of the Parties. The Parties agree to amend this Agreement from time to time as necessary for the Provider to comply with the requirements of federal and applicable state law and regulations including the Privacy Rule and HIPAA. Either party may request that the other party amend this Agreement in order to comply with applicable state and federal law and regulations. If amendment of this Agreement is not achieved to the satisfaction of both parties, then either party may terminate this Agreement without penalty.

(c) Interpretation. Any ambiguity in this Agreement will be resolved in favor of a meaning that permits the Provider and LERN to comply with HIPAA and applicable state and federal laws and regulations.

(d) Assignment. Except as otherwise provided herein, neither Party may without the written consent of the other assign, subcontract, delegate or otherwise transfer this Agreement or any of its rights or obligations under this Agreement. Nor may either Party contract with third parties to perform any obligations required by this Agreement except as may be contemplated in this Agreement, without the other Party’s prior written consent.

(e) Severability. If any part of this Agreement is determined to be invalid, illegal or unenforceable by any Act of Congress, state legislature, or by any regulation issued by the United States or a state, or declared null and void by any court with valid jurisdiction, then the Parties will modify such part, if possible, to conform to the law, and the remaining parts will be fully effective and operative insofar as reasonably possible.

(f) Entire Agreement. This Agreement constitutes the entire understanding and agreement between the Parties concerning the subject matter of this Agreement, and supersedes all prior negotiations, agreements and understandings between the Parties, whether oral or in writing, concerning its subject matter.

THUS DONE AND SIGNED on the date first written above.

**LOUISIANA EMERGENCY
RESPONSE NETWORK (LERN)**

PROVIDER

Name: _____

Name: _____

Title: _____

Title: _____

APPENDIX B: Louisiana Emergency Response Network

**Emergency Medical Services (“EMS”) Provider
Participation and Data Use Agreement**

Name of EMS Provider:	
EMS Provider Address:	
City, State, Zip:	
Effective Date:	

This Participation Agreement (“Agreement”) is entered into between the emergency medical services provider listed above (“Provider”) and the Louisiana Emergency Response Network (“LERN”), an agency of the State of Louisiana.

WHEREAS, LERN is an agency of the State of Louisiana created by R.S. 40:2841, et seq. to safeguard the public health, safety, and welfare of the people of this state against unnecessary trauma and time-sensitive related deaths and incidents of morbidity due to trauma, by establishing a comprehensive, coordinated statewide system for access to regional trauma-patient care throughout the state;

WHEREAS, LERN has created the Louisiana EMS Bridge Registry (“Registry”), which is an automated web based system utilizing Image Trend Patient Registry software and is used to collect, and analyze information on the incident, severity, cause and outcomes of trauma patients to evaluate factors and the health system’s response;

WHEREAS, the State’s goal of the Registry is to gather information more efficiently in order to better analyze treatment methods to reduce morbidity and mortality;

WHEREAS, LERN has determined that Providers frequently do not have electronic health records (“EHR”) systems, and that such systems are vital furthering the mission of LERN through the Registry;

WHEREAS, LERN desires to provide EMS Providers access to the statewide EMS Bridge Registry whereby data elements captured in the electronic medical record will be uploaded electronically into the registry; and

WHEREAS, Provider desires to participate in Registry to improve patient care through more effective processes and to further the public health mission of LERN.

NOW, THEREFORE, for and in consideration of the mutual promises and conditions contained herein, the parties agree as follows:

1. Louisiana EMS Bridge Registry

1.1 LERN has established the Louisiana EMS Bridge Registry, a detailed description of which is contained on the LERN website – www.lern.la.gov. (“LERN Website”).

1.2 Provider agrees to participate in the Registry according to the then current rules and policies contained on the LERN website, including but not limited to the following:

1.2.1 Accurately and timely enter the data elements for all applicable claims.

1.2.2 Access only its own data and such aggregated data as permitted by the then current rules and policies.

1.2.3 Strictly comply with the then current privacy and security rules and policies.

1.3. Provider enters into this Agreement, and participates in the Registry, in part to evaluate Provider performance, develop effective interventions to improve trauma care and time sensitive illness outcomes at the local and national level, and receive feedback in the form of an individual Provider’s data benchmarked against aggregated, de-identified regional and national data (NEMESIS).

2. LERN use of data.

2.1 The Provider has entered into a business associate agreement with LERN under which LERN is permitted to use the PHI to create a limited data set as defined in 45 CFR 164.514(e). The Provider agrees that LERN may use that limited data set (“LDS”) for the following research and public health purposes as more fully described on the LERN Website:

2.1.1 To promote performance improvement and to improve the quality of multidisciplinary trauma care delivered in numerous Provider settings statewide;

2.1.2 To analyze, aggregate, produce, and publish aggregated de-identified data on clinical patterns of diagnosis, treatment, and outcomes of trauma patients and of patients with time sensitive illness; and

2.1.3 To produce reports of aggregated, de-identified data that describe the diagnosis, treatment, and outcomes of trauma patients and of patients with time sensitive illness.

2.2 The LDS will be used only by LERN’s workforce and business associates, and only for the foregoing purposes.

2.3 With regard to the PHI, LERN will:

2.3.1 Not use or further disclose the LDS other than as permitted by this Agreement or as otherwise required by law;

2.3.2 Use appropriate safeguards to prevent use or disclosure of the LDS other than as provided for by this Agreement;

2.3.3 Report to Provider any use or disclosure of the LDS not provided for by this Agreement of which LERN becomes aware;

2.3.4 Ensure that any agents, including a subcontractor, to whom it provides the LDS agrees to the same restrictions and conditions that apply to LERN with regard to the LDS; and

2.3.5 Not identify the LDS or contact the individuals.

3. Warranties. Provider agrees to use its best efforts to enter its data accurately. LERN agrees to use its best efforts to have all participants enter their data accurately, and to accurately present same in aggregated form. Notwithstanding the foregoing, however, neither party hereto warrants the accuracy of any of the data made available to the other through the Registry or otherwise.

4. Privacy and security. Under this Agreement, the services provided by LERN to Provider make LERN the business associate of Provider. As a result, LERN has entered into the Business Associate Agreement attached hereto as Exhibit I, and agrees to abide by same as provided therein when acting as Provider's business associate.

5. Term and termination.

5.1 This Agreement shall become effect on the latest date of signature below, and shall continue in effect until terminated by either party.

5.2 Either party to this Agreement may terminate it, with our without cause, by providing written notice to the other, not less that thirty (30) days in advance.

5.3 Upon termination, unless otherwise agreed by the parties in writing, LERN shall be entitled to retain and continue to use Provider's data, in de-identified form, in the Registry.

6. Miscellaneous.

6.1 Each party is an independent contract of the other. Neither party shall be the legal agent of the other for any purpose whatsoever and therefore has no right or authority to make or underwrite any promise, warranty, or representation, to execute any contract, or otherwise to assume any obligation or responsibility in the name of or on behalf of the other party, except to the extent specifically authorized in writing by the other party. Neither party shall be bound by nor liable to any third party for the acts or obligations or debts incurred by the other toward such third party, except to the extent specifically agreed to in writing by the party to be so bound.

6.2 If any provision of this Agreement is held to be illegal, invalid or unenforceable under any present or future law, and if the rights or obligations of either Party

under this Agreement will not be materially and adversely affected thereby, (a) such provision shall be fully severable, (b) this Agreement shall be construed and enforced as if such illegal, invalid or unenforceable provision had never comprised a part hereof, (c) the remaining provisions of this Agreement shall remain in full force and effect and shall not be affected by the illegal, invalid or unenforceable provision or by its severance here from, and (d) in lieu of such illegal, invalid or unenforceable provision, there shall be added automatically as a part of this Agreement a legal, valid and enforceable provision as similar in terms to such illegal, invalid or unenforceable provision as may be possible and reasonably acceptable to the parties herein. To the fullest extent permitted by applicable law, each party hereby waives any provision of law that would render any provision prohibited or unenforceable in any respect.

6.3 Neither party hereto shall be liable for defending or for the expense of defending the other party, its agents, or employees, against any claim, legal action, dispute resolution or administrative or regulatory proceeding arising out of or related to the other party's actions or omissions under this Agreement. Neither party hereto shall be liable for any liability of the other party, its agents, or employees, whether resulting from judgment, settlement, award, fine or otherwise, which arises out of such other party's actions or omissions under this Agreement.

6.4 This Agreement shall be governed by the law of the State of Louisiana.

6.5 Any amendment to this Agreement must be in writing and signed by each of the Parties.

6.6 Except as otherwise provided herein, neither Party may without the written consent of the other assign, subcontract, delegate or otherwise transfer this Agreement or any of its rights or obligations under this Agreement. Nor may either Party contract with third parties to perform any obligations required by this Agreement except as may be contemplated in this Agreement, without the other Party's prior written consent.

6.5 This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

THUS DONE AND SIGNED on the date first written above.

**LOUISIANA EMERGENCY
RESPONSE NETWORK (LERN)**

PROVIDER

Name: _____

Name: _____

Title: _____

Title: _____

APPENDIX C: Louisiana Emergency Response Network

User Logon Request Form

This form is to be completed by the facility administrator for each individual hospital. See page 12 of the LERN User & Training Manual for Non Image Trend Registry Users for more detail on the agency administrator. **This form is to be submitted to the LERN System Administrator after completion of the Business Associate Agreement and the Data Participation Agreement.**

PLEASE PRINT CLEARLY

Name (First, Middle, Last)	
Facility Name	
Street Address	
City, State, Zip	
Work Phone Number	
Cell Phone Number	
Pager Number	
Fax Number	
E-Mail Address	

FACILITY INFORMATION

Region	
Trauma Center Level	
Rehab Facility	
Burn Center	
Facility Name	
NTDB Facility ID	
National Provider ID	
Facility State ID	
Medicare Provider Number	
Street Address	
City, State, Zip	

The following Data Privacy Statement will display each time you log into the Image Trend System. You must agree to this statement as denoted by clicking yes to proceed.

PLEASE READ THIS PRIVACY STATEMENT CAREFULLY

By accepting this Data Privacy Statement, you agree to keep the information contained within this site private and confidential. Any reporting or exporting of data must be done securely using industry standards and best practices for data privacy and adhering to all applicable federal and state data privacy requirements. It is the responsibility of the user to ensure that all applicable requirements are adhered to.

The State has taken steps to ensure that all information contained within this site is secure to protect against unauthorized access and use. All information is protected by our security measures, which are periodically reviewed. Information is protected through the use of passwords, strictly controlled server access, physical security of the hosting site, and 128-bit SSL encryption.

Although the State can assure the security and privacy of the data that has been submitted, we have no control over how individual users may handle their own data, either before or after they have submitted data. In order to protect the security and privacy of your records before or after you have submitted data, we recommend adopting the following procedures/practices:

- 1) Do not send incident records via email. Email does not offer the same level of security as submitting data via the internet to the Louisiana (LERN) Patient Registry because it is not encrypted.
- 2) Only assign user names and passwords to individuals who have responsibility for the Louisiana (LERN) Patient Registry.
- 3) Regularly change passwords.

If you have questions about the Privacy or Security of this site, please contact:

LERN OFFICE USE ONLY

User ID

Password

Permission Group

- System Administrator
- EMS Administrator
- EMS Staff
- Peer Review Committee

Report Writer

Permission Group

- Administrator
- Report User
- Report Read Only

View "MY" Incidents ONLY

- Yes (See only records individual enters)
- No (See all records for this facility)

Incident Forms

- Hidden
- View
- Edit
- Add
- Delete

Ability to Lock Incidents

- Yes
- No

Ability to Change Incident Status

- Yes
- No

View Patient Identifiable Information

- Yes
- No

Restrict Based on Date

- Last _____ Days
- Date Range: _____
to _____

References:

American College of Surgeons, Committee on Trauma, Resources for Optimal Care of the Injured Patient, 2006, Chapter 15, Trauma Registry

HIPAA Password Regulations, Drew Lichtenstein, m eHow Contributor,
http://www.ehow.com/list_6960330_hipaa-password-regulations.html

NEMESIS
<http://www.nemesis.org/>

www.wikipedia.org

LERN Image Trend Data Dictionary

Texas Data Dictionary

California Data Dictionary

Virginia State Trauma Registry User & Training Manual

Washington Hospital Data Dictionary

North Carolina Data Dictionary

Nevada Data Dictionary