LOUISIANA
EMERGENCY
RESPONSE
NETWORK

Right Place. Right Time. Right Care.

USER & TRAINING MANUAL FOR NON IMAGE TRAUMA REGISTRY USERS

Powered by ImageTrend

LOUISIANA
EMERGENCY
RESPONSE
NETWORK

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.

TABLE OF CONTENTS:

This manual will explain: HOW TO ENTER DATA INTO THE WEB BASED STATEWIDE TRAUMA 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

Hospitals that have been approved and given access to the "UPLOAD" function for the LSB should submit on a quarterly basis at a minimum. The time between a trauma patients discharge from the reporting facility until entry into the LSB shall NOT be longer than six (6) months. An example of a yearly reporting schedule is provided below in Table 1.

TABLE 1

Calendar Year Quarter		**Submission Deadline**
January - March Admissions		June 1
April - June Admission		September 1
July - September Admission		December 1
October - December Admission		March 1

INCLUSION CRITERIA

To ensure consistent data collection across the State into the LERN State Registry, LERN has adopted the NTDS Data Dictionary Patient Inclusion Criteria as applied by ACS for the data collected within the standards applicable for that year.

To reference current and past NTDS data collection standards please follow the link below:

https://www.facs.org/quality-programs/trauma/quality/national-trauma-data-bank/national-trauma-data- standard/

DATA SUBMISSION

LOUISIANA STATE BRIDGE DATA ELEMENTS:

LERN in conjunction with state and national stakeholders has adopted the National Trauma Data Standards (NTDS) as its LSB data elements. The NTDS is a dataset defining standardized data elements collected by the American College of Surgeons within the National Trauma Data Bank (NTDB). This standardized dataset includes only core variables that would prove useful if aggregated on a state level.

Each individual hospital trauma registry will likely collect additional variables important to patient care. However, the LSB data elements should be collected by all hospitals.

For full definitions and additional information PLEASE go to: https://www.facs.org/quality-programs/trauma/quality/national-trauma-data-bank/national-trauma-data-standard/

ADDITIONAL DATA ELEMENTS

Louisiana's Trauma Registry has 5 additional data elements not found in NTDS.

- Facility Transferred To (TR25.35): Non-hospital facility trauma patient is transferred to the trauma center.
- Referring Hospital Name (TR33.1): Hospital trauma patient is transferred from to the trauma center.
- Hospital Transferred To (TR25.35): Hospital receiving trauma patient transferred from the trauma center (not ED to ED).
- ED Hospital Transferred To (TR17.61): Hospital receiving trauma patient transferred from the trauma center (ED to ED transfer).

DATA SUBMISSION PROCESS

The System Administrator sets up non Image Trend users under the facility profile page. The System Administrator will replace AHA number with facilities NTDB Facility number. This number MUST be obtained from the individual hospital as ACS will not give this information out.

1. Each non Image Trend Hospital will run their NTDB export from their individual software

2. Correct Level 1 and Level 2 errors – same as NTDB

3. Rerun NTDB export

4. Go to State Image Trend Site www.lerntrauma.com and log in with your credentials

5. Click Data Exchange → Import → NTDB Import

6. Click the green IMPORT button in the upper right side of the page

7. Name the file, use the BROWSE button to navigate to the file you wish to import.

8. After you have verified that the Channel and Form Type are correct, click UPLOAD AND VALIDATE button to start the file transfer. Depending on the number of incidents, this step may take a moment. Be patient and when it is complete you will be notified.

The system will automatically run the data importing, processing, and validation routines. Changes will be reflected in the system within 24 hour

PURPOSE OF THE STATE TRAUMA 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 trauma registry is an important management tool that is used for performance management and improvement, research, and injury prevention.

Individual trauma centers that are verified by the Committee on Trauma, American College of Surgeons (COT ACS) must develop and maintain their own trauma registries and submit their data to the National Trauma Data Bank (NTDB). In Louisiana, hospitals must successfully complete the COT ACS verification process as a condition of state certification as a trauma center.

Louisiana's statewide trauma 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. You will find materials for administrators, users, and trainers to use including: Here you will find a complete user's guide, as well as several short educational videos on the Image Trend Patient Registry.

- 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 at 225-756-3440 for questions. Additionally, under the Image Trend contract with LERN facilities may also contact their support center at: 1-888-730-3255 or support.imagetrend.com.

You can go to the LERN website at: www.LERN.la.gov and Click on **Contact us** on the left side under ABOUT US. This link lists phone numbers, fax numbers, and email addresses for obtaining help related to the web based LSB. LERN's contact information is below:

Louisiana Emergency Response Network
14141 Airline Hwy, Building 1, Suite B
Baton Rouge, LA 70817
225-756-3440
Lern.la.gov

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 service.
- Multiple Service Administrators – User access and administration to multiple services.
- Hospitals – Access to all runs delivered to their facility.

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
- Service
- Hospital

On the service level, there are typically two levels:

- Administrator
- 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.

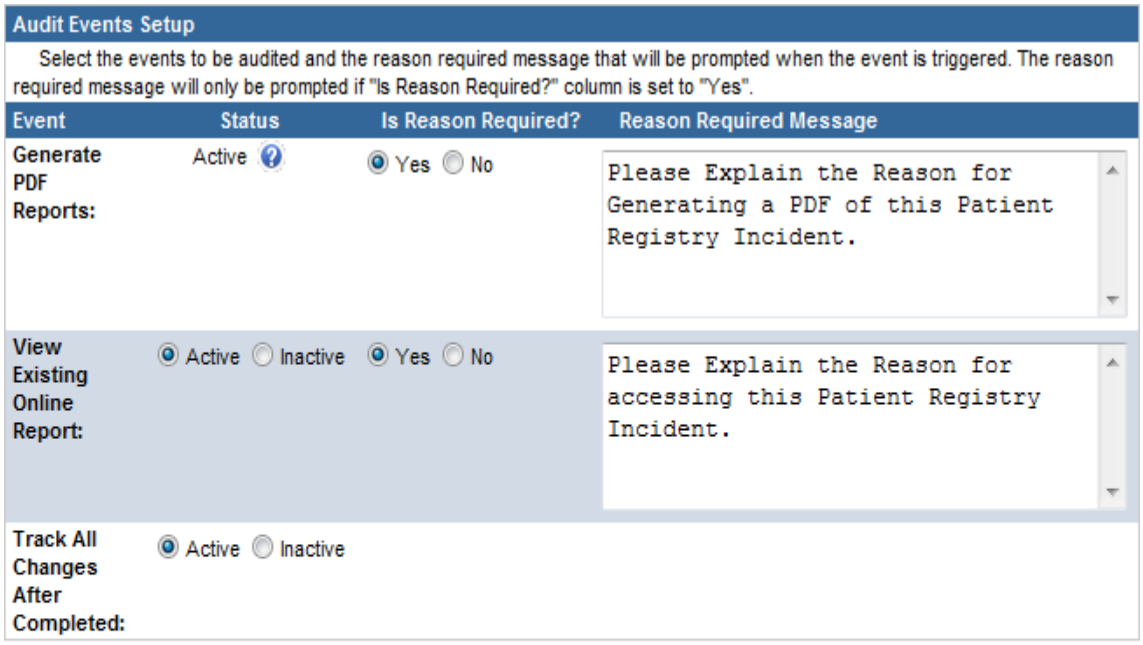
Applications are monitored for availability and performance from multiple locations to ensure an accurate measure of current system health. Slow application pages and long running database queries are logged for analysis by server administrators and development staff. Serious errors and performance degradation 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.

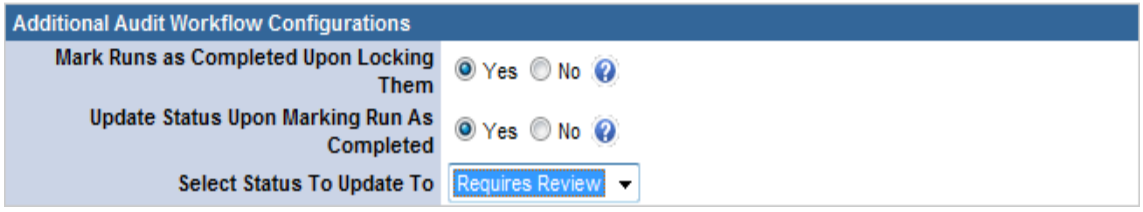
Auditing

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.





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.

FACILITY ADMINISTRATOR:

A facility administrator is the lead contact at an individual hospital. This position will typically be the trauma program manager or trauma administrator. The facility administrator will then be responsible for enrolling their own local staff for access into the LSB. The facility administrator will be able to grant different levels of access to these staff members depending on their job titles and responsibilities. The facility administrator will be allowed full access to their individual facility data, but will be unable to view any other facility information in the LSB.

EMPLOYEE ACCESS:

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

APPENDIX A: Louisiana Emergency Response Network

Business Associate Agreement

Name of Hospital:	
Hospital Address:	
City, State, Zip:	
Effective Date:	

Hospital participates in the Louisiana Emergency Response Network ("LERN") Louisiana State Bridge ("LSB"). 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.

LSB 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 LSB is to gather information more efficiently in order to better analyze treatment methods to reduce morbidity and mortality.

Hospital participates in LSB in order to meet certain requirements for accreditation and to facilitate internal quality assurance activities.

LSB requires the Hospital 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 Hospital and LERN enter into a Business Associate Agreement to protect PHI.

I. Agreement:

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

(1) To set standards for quality, multidisciplinary trauma care delivered in numerous hospital settings statewide;

(2) To survey hospitals to assess compliance with those standards;

(3) To analyze, aggregate, produce, and publish aggregated de-identified data on clinical patterns of diagnosis, treatment, and outcomes of trauma patients;

(4) To produce reports of aggregated, de-identified data that describe the diagnosis, treatment, and outcomes of trauma patients;

(5) To evaluate hospital performance, develop effective interventions to improve trauma care outcomes at the local and national level, and provide feedback in the form of an individual facility's data benchmarked against aggregated, de-identified regional and national data (NTDB).

(6) To de-identify the PHI; and

(7) To create a limited data set ("LDS") for use and disclosure pursuant to the PDUA.

(b) The hospital 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 Hospital. LERN is a Business Associate and the Hospital 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 the PDUA, 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 Hospital 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 Hospital, 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 Hospital'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 Hospital made the same or similar disclosures.

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

(h) LERN agrees to cooperate with Hospital 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 Hospital.

(j) LERN shall promptly report to Hospital 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):

(1) LERN shall notify Hospital 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 Hospital 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 Hospital

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

(1) Hospital shall notify LERN of any limitation(s) in the Hospital's Notice of Privacy Practices, to the extent that such limitation may affect LERN's use or disclosure of PHI. The Hospital will make its Notice of Privacy Practices available to LERN upon request.

(2) Hospital 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) Hospital 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 Hospital will notify LERN of any restriction on the use or disclosure of PHI that the Hospital 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 Hospital. The Hospital 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 Hospital; except as otherwise provided for in this Agreement.

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

(1) appoint a Facility Administrator to be responsible for properly employing the security features of the LSB system; and

(2) understand and use the security features in the LSB 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.

(c) 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 Hospital's direction, destroy all PHI received from the

Hospital, or created or received by LERN on behalf of the Hospital 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 Hospital 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 Hospital 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 Hospital 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)	**HOSPITAL**
_____	_____
Name: _____	Name: _____
Title: _____	Title: _____

APPENDIX B: Louisiana Emergency Response Network

Participation and Data Use Agreement

Name of Hospital:	
Hospital Address:	
City, State, Zip:	
Effective Date:	

This Participation Agreement ("Agreement") is entered into between the hospital listed above ("Hospital") 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 State Bridge ("LSB"), 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 LSB is to gather information more efficiently in order to better analyze treatment methods to reduce morbidity and mortality; and

WHEREAS, Hospital participates in LSB in order to meet certain requirements for accreditation and to facilitate internal quality assurance activities.

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

1. Louisiana State Bridge

1.1 LERN has established the Louisiana State Bridge, a detailed description of which is contained on the LERN website – www.lern.la.gov.

1.2 Hospital agrees to participate in the LSB 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. Hospital enters into this Agreement, and participates in the LSB, to evaluate Hospital performance, develop effective interventions to improve trauma care outcomes at the local and national level, and receive feedback in the form of an individual facility's data benchmarked against aggregated, de-identified regional and national data (NTDB).

2. LERN use of data.

2.1 The Hospital agrees that LERN may use the PHI received for the following purposes as more fully described on the LERN Website:

2.1.1 To set standards for quality, multidisciplinary trauma care delivered in numerous hospital settings statewide;

2.1.2 To survey hospitals to assess compliance with those standards;

2.1.3 To analyze, aggregate, produce, and publish aggregated de-identified data on clinical patterns of diagnosis, treatment, and outcomes of trauma patients; and

2.1.4 To produce reports of aggregated, de-identified data that describe the diagnosis, treatment, and outcomes of trauma patients.

2.2 The Hospital 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 Hospital agrees that LERN may use or disclose that limited data set ("LDS") for the following research and public health purposes as more fully described in the LERN website

2.2.1 To promote performance improvement and to improve the quality of multi-disciplinary trauma care delivered in various settings statewide;

2.2.2 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;

2.2.3 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, and

2.2.4 To disclose the protected health information to interested parties for research and public health purposes, so long as this disclosure is otherwise consistent with this Agreement and compliant with the requirements of 45 CFR 164.514(e) or as otherwise required by law.

2.3 The LDS will be used by LERN's workforce, business associates, and those specific parties for whom LERN contracts to share the LDS for research purposes, and only for the foregoing purposes

2.4 Hospital further agrees that LERN may use or disclose the PHI as required by law or for research purposes as more fully described on the LERN website so long as this disclosure is otherwise compliant with the requirements of 45 CFR 164.512(a) or (i).

2.5 With regard to the PHI, LERN will:

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

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

2.5.3 Report to Hospital any use or disclosure of the LDS not provided for by the Agreement of which LERN becomes aware;

2.5.4 Ensure that any agents or parties, 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

2.5.5 Not identify the LDS or contact the individuals.

3. Warranties. Hospital 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 LSB or otherwise.

4. Privacy and security. LERN, as the business associate of Hospital, has entered into the Business Associate Agreement attached hereto as Exhibit I, and agrees to abide by same as provided therein.

5. Use of Image Trend Patient Registry software. LERN has acquired, for the implementation and operation of the LSB, certain licenses for the use of the Image Trend Patient Registry, which is a web-based tool more fully described on the LERN Website. Hospitals may derive independent benefit from the use of that tool, and LERN's licenses allow LERN to authorize the use of that tool by hospitals participating in the LSB. Therefore, in consideration of Hospital's participation in the LSB and other valuable consideration, receipt and sufficiency of which is hereby acknowledged, LERN hereby grants to Hospital the right to use the Image Trend Patient Registry for its own purposes, subject to the then current terms and conditions provided on the LERN Website.

6. Term and termination.

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

6.2 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.

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

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 herefrom, 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)	**HOSPITAL**
_____	_____
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 14 of the LERN User & Training Manual for Non Image Trend Registry Users for more detail on the facility 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, Mi le, 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
- ☐ Hospital Administrator
- ☐ Hospital 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

American College of Surgeons, National Trauma Data Standards, Data Dictionary, 2022 Admissions: ntds_data_dictionary_2022.pdf (facs.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

North Carolina Data Dictionary

A special Thank You to Image Trend

LOUISIANA
EMERGENCY
RESPONSE
NETWORK

Right Place. Right Time. Right Care.

LERN.LA.GOV