FLORIDA DEPARTMENT OF
HEALTH

EMSTARS

FLORIDA'S

PREHOSPITAL
EMERGENCY MEDICAL SERVICES
TRACKING & REPORTING SYSTEM

END USER SECURITY POLICY MANUAL

1 INTRODUCTION

The purpose of this reference document is to present the EMSTARS End User Security Policy and its associated procedures. All prospective users of the EMSTARS system must acknowledge receipt and sign the End User Security Policy prior to obtaining access to the system.

Additional documentation material may be referenced though out this document and is available as supplemental reference material on the EMSTARS Website.

2 THE END USER SECURITY POLICY

2.2 PROTECTED HEALTH INFORMATION

Electronic Protected Health Information (ePHI) as defined by HIPAA is securely transmitted to the EMSTARS system from provider agencies across the state. However, this ePHI with personal identifiable information on patients is not accessible by unauthorized users and will not be displayed on reports that are generated.

2.3 CONFIDENTIALITY

Beyond protected patient information; the EMSTARS system also contains confidential information on Florida's EMS system and the delivery of services by local provider agencies. The information contained within the system and its reports is intended for use by Florida's local and state EMRCs and/or Quality Assurance Committees. Pursuant to § 401.425(5) Florida Statutes, the records obtained or produced by the EMRC providing quality assurance activities are exempt from the provisions of §119.07(1) and s. 24(a), Art. I of the State Constitution, and EMRC proceedings and meetings regarding quality assurance activities are exempt from the provisions of s. 286.011 and s. 24(b), Art. I of the State Constitution.

Local EMRC and/or Quality Assurance Committees are free to distribute any information regarding their particular agency. However, where system or provider performance information or sensitive performance data is involved, the distribution or sharing of electronic or paper reports with other organizations or public safety entities is strictly prohibited and regulated by DOH. This includes, but is not limited to, city or county government, law enforcement, hospitals, universities or other higher learning institutions, and any organization or person outside the state of Florida and not directly affiliated with Florida's EMS system.

The EMS Data Unit will provide information, upon request, to these types of organizations after a state level EMRC review has been completed. The EMRC provides a mechanism for statewide and national EMS data analysis for the purpose of statewide quality improvement. Information provided by Florida EMS agencies through the Emergency Medical Services Tracking and Reporting System (EMSTARS) and other data sources will be collected. The information will be queried including development of the report process as directed by the EMRC. All requests for data must be routed to the EMRC’s Bureau of EMS Representative. If an end user is unsure whether or not the information they have downloaded or printed may be distributed, the user must contact the EMS Data Reporting Manager for direction.

3 EMSTARS SECURITY

3.2 Data Structure

The EMSTARS system, and access to its data, will be structured in such a way to allow access only to authenticated users and only at authorized permission levels. The EMSTARS web site will be secured with SSL 128-bit encryption.

All personal identifiable patient information will be secured in a separate database schema. No end user may access the secured patient data. Most of the data and reports in the system will be aggregated (grouped / summed / sorted) rather than displayed at the record level. It is not the focus of the EMSTARS system and statewide database to provide search or display capabilities for individual incidents or patients.

3.3 AUTHENTICATION

The EMSTARS system employs a dual authentication mechanism to grant access to the system. All accounts are created with an Agency ID and password (to associate users to a specific provider agency) and a personal Username and password. The Agency password is maintained by the EMSTARS System Administrator and is provided to each user as applicable.

An agency’s Key User is the only person that can request new, or modified, user accounts. All account maintenance must be initiated by the Key Users.

For new accounts, the individual user passwords are system-generated, random passwords and must be changed by the appropriate user upon initial (or subsequent for a reset) login. As defined below, user passwords must meet minimum complexity requirements; password syntax and thresholds; and must be a combination of 8 or more characters:

- There must be at least one numerical character and one alphabetical character
- Passwords may also include special symbols (!@#$%^&*( ) { }[ ]<>~’”)
- User passwords should not spell any word that appears in the dictionary
- User passwords have to be reset at least biannually

Accounts are “locked out” after three unsuccessful login attempts. Only an agency’s Key User is allowed to contact the System Administrator to “unlock” an account. Accounts may also be “locked” manually by the System Administrator at the request of a Key User.

In the event of a lost or compromised password, only an agency's Key User may contact the System Administrator to request a reset. As with the initial setup, a random password is generated by the system and emailed to the user; this password must be changed upon initial login.

3.4 AUTHORIZATION

The EMSTARS system employs role based access control to assign permissions to groups of users. The profile to which an end user is assigned is determined by the agency administrator or the EMS Data Manager.

3.4.1 SYSTEM ADMIN

These users have access to all application services, all levels of reporting, and all data stored in the system (except ePHI as described above); this profile represents the highest level of permissions available. This role resides exclusively within the Bureau's Data Unit.

3.4.2 DATA ANALYST

These users have access to all application services and all levels of reporting. This role resides exclusively within the Bureau of EMS, Data Unit.

3.4.3 KEY USER

These users have access to application services required for direct communication and interaction with the Bureau of EMS, Data Unit. These permission levels include access to the Security Maintenance components, the XML Upload component for transmitting monthly data files, and the Submissions component to check for records that did not pass content validation and were quarantined. This profile has reporting permissions equivalent to the Platinum Reporting profile described below. At least two users per agency will be granted the Key User role and associated permissions.

3.4.4 PLATINUM REPORTING

These users have access to reporting services offered by the application, including the ability to request the generation of custom queries and reports; this profile represents the highest level of secured reporting access and permissions. This profile is targeted towards Key Users and leadership roles within the provider agency such as EMS Chief / Administrator, Medical Directors, and Quality Managers.

3.4.5 GOLD REPORTING

These users have access to reporting services offered by the application including the ability to request the generation of custom queries and reports; this profile represents the middle level of secured reporting access and permissions. This profile is targeted towards mid-level management within the provider agency, DOH users external to the Data Unit, and others in the Florida EMS community such as Advisory Council members, EMS Educators, Constituency Presidents, etc.

3.4.6 SILVER REPORTING

These users have access to reporting services offered by the application; this profile represents the lowest level of secured reporting access and permissions and no access to custom reporting requests will be granted. These users represent the largest quantity of all the system profiles. This “entry-level” profile is targeted towards most users across the state including all provider agency staff and other interested members of Florida’s EMS community.

3.4.7 PUBLIC ACCESS

These users have access only to public reports and information linked to the EMSTARS home page. This access level does not require an account or login and, therefore, does not have access to any of the secured components.

3.4.8 MULTIPLE AGENCIES

Users such as a paramedic who works for multiple agencies who require access to multiple agencies will require different personal usernames and passwords as well as the different agency id and password.

Users such a Medical Director, Administrator, Quality Manager, or similar position that has oversight authority for multiple agencies must be granted the Platinum Reporting permission level. This permission level gives the user the ability to view multiple agencies with the same personal username and password. These users will still need the different agency ID and password along with their username and password to view all data for that agency.

Both these scenarios must follow the authentication process describe in Section 3.3 Authentication of this document.

3.5 TRACEABILITY

EMSTARS logs all actions and transactions. This information is used to provide audit ability and traceability for the EMSTARS application.

As the EMSTARS system contains confidential and/or exempt information on both patients and provider agencies, any unauthorized access to the system or its assets will be reported to the proper authorities and may result in civil or criminal penalties.

3.6 USER RESPONSIBILITIES

The following guidelines must be adhered to by all end users who are authorized to access the EMSTARS system and its reporting resources.

3.6.1 PASSWORD PROTECTION

It is the responsibility of all end users to take reasonable steps to safeguard their passwords (agency and user). User passwords must not be shared with any other persons including other users. Agency passwords can be shared only with authorized personnel (EMSTARS end users) within that agency. A user may not offer to allow another user access to the system by using their username and / or password. Sharing of account information is prohibited.

3.6.2 ACCESS LOCATIONS

It is the responsibility of all end users to access the secure portion of the EMSTARS system and its assets only from agency-supplied computers. <u>Access from home or from public use computers is prohibited.</u>

3.6.3 MAINTAINING CONFIDENTIALITY

It is the responsibility of all end users to ensure that confidential information remains protected and is not distributed to or shared inappropriately. Please refer to the Confidentiality section for a complete explanation of what is, and is not, permitted.

End users who encounter any Protected Health Information (PHI), such as personal identifiable data, must report this to the Bureau of EMS, Data Unit. No patient information should be available in the EMSTARS system; however, if this level of information is inadvertently presented within the system, the Bureau of EMS Data Unit must be notified so they can take steps to correct the problem. Additionally, end users shall not attempt to use the EMSTARS data or reports to track or link an individual's data, determine real or likely identities, gain information about an individual, or contact an individual.

End users shall not use or further disclose the EMSTARS data or reports except as permitted. Provider agencies shall establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of and to prevent unauthorized use or access to the EMSTARS data or reports.

End users shall not release, or allow the release of, the EMSTARS data or reports to any persons or entities other than as permitted and described in the Confidentiality section. Furthermore, where release of EMSTARS data or reports is permitted, end users shall instruct individuals, to which the EMSTARS data or reports are disclosed, of all obligations for their protection and shall require the individuals to maintain those obligations.

<u>End users shall secure the EMSTARS data or reports when they are not under the direct and immediate control of an authorized individual performing the functions.</u>

3.6.4 REPORTING UNAUTHORIZED ACCESS

End users shall make a good faith effort to identify any misuse or unauthorized disclosure of the EMSTARS data or reports. End users shall notify the Bureau of EMS, Data Unit within twenty-four (24) hours of discovery. Furthermore, any end user who observes, or is made aware of, any unauthorized person attempting to access the EMSTARS system and its assets must report the violation to the Bureau of EMS, Data Unit.

3.6.5 PENALTIES

End users acknowledge that failure to abide by the terms of the End User Security Policy may be subject to penalties for wrongful disclosure of protected health information under federal law. End users shall inform all persons, with authorized access to the EMSTARS data or reports specified, of the penalties for wrongful disclosure of protected health information.

The EMSTARS End User Security Policy

The security and protection of patient and EMS provider information is of the utmost importance to the EMSTARS program. Accordingly, each registered EMSTARS user must agree to adhere to the terms and conditions of the EMSTARS End Users Security Policy. As part of the New Account process (as documented in the EMSTARS Program Manual), Key Users must supply each new end user with a copy of the Security Policy which must be signed and submitted to the Data Unit. Key Users should answer any questions the end user may have regarding the policy. If the Key User is unable to answer a specific question, they may contact the Data Unit for clarification.

Statement of Acceptance by the Registered EMSTARS End User

With my signature below, I acknowledge the fact that I have been provided a copy of the EMSTARS End User Security Policy, I have reviewed the policy, any questions have been answered, and I accept the terms set forth within.

____
Name of End User
(Please print)

____
Signature of End User

____
Date

____
EMSTARS User Name
(Your assigned login name)

____
Agency Name

____
Agency ID

____
Signature of Agency Key User
(Required for EMS agency end users)

Please fax this signature page to:

Bureau of EMS Data Unit
850-488-2512
ATTN: EMS Data Manager

Or, you may scan this page, with the original signature, and email the document to:

emstars@doh.state.fl.us

■ END OF DOCUMENT –