

EMSC DATA CENTER BEST PRACTICES

AN EMSC STATE PARTNERSHIP PROGRAM GUIDE



EDC
EMSC Data Center







Hilary Hewes MD, Principal Investigator, Michael Ely MHRM, EMSC
Data Center Director, Patricia Schmuhl BA, EDC Data Manager, Jane
Ostler MS CHES, Business Data Analyst

EMSC DATA CENTER | SALT LAKE CITY, UTAH

EMSC Data Center (EDC) Best Practices

The Emergency Medical Services for Children (EMSC) Data Center (EDC) is a national resource center helping state and territory EMSC Program Managers and EMS offices develop capabilities to collect, analyze, and utilize emergency care data. The EDC works to ensure data security through every phase of the data cycle. We offer technical assistance, education, and support to our customers to ensure best practices for safe data use, storage, and sharing. This document details important information about data that all EMSC State Partnership (SP) grantees should know.

Use the **EDC Best Practices Quick Guide** below for easy-to-remember topic descriptions. Detailed information in this document can be accessed quickly by clicking on the icons or text below:

EDC Best Practices Quick Guide	
	Keeping data secure, private, and confidential is a top priority in the EMSC Program
	The EDC provides guidelines to address different scenarios in which data has the potential to be compromised.
	It is the responsibility of the EMSC Program Director/Manager to protect state-level data.
	Understanding Personal Identifiable Information (PII) can help EMSC SP grantees protect all information.
	The EDC uses several integrated systems that support data collection, storage, visualization, use, and security.
	Understanding the difference between access and permission helps EMSC SP grantees to keep data safe.

Keeping Data Secure, Private, and Confidential

Keeping data secure, private, and confidential is a top priority in the EMSC Program. The EDC manages and maintains large datasets for the EMSC Program through data collection and research projects housed at the University of Utah's Data Coordinating Center (DCC). In addition to the EDC recommendations below, please refer to your organization's data policies/protocols.

For the safety of any data shared within the EMSC program by the EDC, we recommend that data only be stored on devices that are encrypted or password protected. Devices should be locked or monitored in a safe location at all times. Where possible, any data transmitted via email should also be encrypted. Reach out to your EDC contact for information on document encryption.

When it comes to data privacy and confidentiality, the University of Utah Institutional Review Board (IRB) said it best:

"Privacy refers to persons and to their interest in controlling access of others to themselves. Privacy can be thought of in terms of having control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.

Confidentiality is an extension of the concept of privacy, but it refers to the research participant's understanding of (and agreement to) the ways that their identifiable information will be stored and shared. Identifiable information can include printed information, electronic data or media, or visual information (photographs, video records, etc.).

The bottom line: Privacy refers to people; Confidentiality refers to data about people."

Understanding privacy and the role of confidentiality in data collection can help EMSC SP grantees to protect all data.

The EMSC Program does not sell or share data with outside entities or anyone for any reason unless approved by the EMSC Program for research purposes through a verified application process. This means that data is not used for listservs, is not sold to marketing firms, and is not shared with for-profit or non-profit organizations. Information gathered from any source is kept secure, private, confidential, and only used for EMSC programmatic purposes.

Researchers and Investigators outside of the EMSC Program must complete a Manuscript Analysis Request Form (MARF) and follow strict protocols for data use in their studies. Learn more about the [Research Opportunities Request Process](#) if you would like to use EMSC data for research purposes.

The **EDC** does everything they can to keep data secure, private, and confidential.
We ask that all EMSC Program State Partnership grantees do the same.

EDC Guidelines

Using safe data storage, sharing, and security practices is the key to maintaining good relationships within the EMSC Program and with collaborative partners for quality improvement.

EMSC Program Directors/Managers can utilize data from surveys and assessments for **internal** EMSC Program purposes at their discretion with those who have an EMSC work-related need.

Examples of **internal** collaborators could include individuals within their state EMSC program such as EMSC Project Directors, State Medical Directors, State EMS Directors, and EMSC Advisory Committee members.

EMSC survey and assessment data shared with **external** collaborators should be deidentified and combined with multiple results to protect respondent confidentiality, such as, to illustrate an average of statewide hospital scores (see chart below). Examples of **external** collaborators include other national organizations, hospital systems, prehospital systems, researchers, or the public.

The EDC provides guidelines that address different scenarios in which ALL data points, including respondent confidentiality, have the potential to be compromised. Thinking about raw, clean, analyzed, and visualized data, here are some things to DO internally and NOT DO externally:

Internal	External
DO ensure that the data are kept in a secured environment and that ONLY the necessary individuals within the State EMSC Program with a <u>work-related need</u> (to be determined by the EMSC State Partnership Project Director) will have access to the raw data set.	DO NOT release or disclose the raw dataset (or any part of the data set) to any person whom you have not determined to have an EMSC <u>work-related need</u> (to be determined by the EMSC State Partnership Project Director), except with the express written approval of each hospital/ED and/or prehospital agency whose information is to be released.
DO share results on a broader level by presenting the data in a combined format (at least 5 or more).	DO NOT release or disclose information where the number of EDs or prehospital agencies providing data for any given question is fewer than 5, as it is possible to determine which ED or prehospital agency likely responded within a small grouping (again unless permission is granted by the participating EDs or prehospital agencies).
DO acknowledge or reference in all reporting or materials produced the appropriate source of the data. For example, the “National Pediatric Readiness Project” or the “EMS for Children Survey”.	DO NOT use the dataset concerning individual EDs or prehospital agencies (1) for personal, commercial, or competitive purposes involving those individual EDs or prehospital agencies; (2) to determine the rights, benefits, or privileges of individual EDs or prehospital agencies; or (3) to report, through any medium, data that could identify, directly or by inference, individual EDs or prehospital agencies.
DO Use appropriate safeguards to prevent the use or disclosure of the dataset other than as described in these guidelines.	If you have a question about safe data-sharing practices please reach out to your EDC Technical Assistance Liaison for more information.

Protect State-Level Data

Protecting state-level data is the responsibility of the EMSC Program Director and/or Manager. They are the owners and gatekeepers of their data. This includes [Personal Identifiable Information \(PII\)](#)

and any data point in a survey, assessment, report, or anything they have access to in an EDC-integrated system like the [Contact List Management System \(CLMS\)](#) and [Tableau](#) that can be directly linked to the respondent, agency, or hospital that provided that information.

State-level data should also be kept physically secure on encrypted devices and stored in a secure location when not in use. State-level data should only be shared with those that have an EMSC programmatic need. Contact the EDC or state-level data support for additional information about safe data-sharing practices.

Personal Identifiable Information (PII)

Personal Identifiable Information (PII) is generally defined as information that identifies an individual, such as a name, email, phone number, address, or title. PII is often readily accessible online and over social media. Thus, it may seem an insignificant matter to share this information if it is already publicly available.

However, maintaining transparency and trust among our survey respondents and other partners is important to us. During data collection periods we advertise in assessments and surveys “*Your answers are confidential. Only the project team and your state EMSC program will have access to the data*”. We also state that responses will be combined with the results of other participants for reporting purposes to protect individual Emergency Department (ED) and EMS agency information.

In addition to the EMSC Program, respondents are the owners of their individual scores, gap reports, and other information they receive when they take an assessment or survey. They decide with whom sharing this information is necessary and appropriate. Take care to protect confidentiality by forwarding any outside requests directly to the respondent listed on the survey or assessment. This gives them the opportunity to reply or remain anonymous to the person requesting information.

If you need to contact someone based on an EMSC Program-related need (e.g. survey follow-up, targeted outreach) please let the individual know why you are contacting them and that you are part of the EMSC leadership community.

EDC Integrated Systems

The EDC uses several integrated systems that support data collection, storage, visualization, use, and security. Managing and maintaining these systems is both the responsibility of the EDC and those who have access to EMSC Program data. Keeping data clean and updated within these systems is an ongoing process and necessary for accuracy in data collection and reporting.

EMSC Program Directors/Managers can learn more about what these systems do, how they work together, and why they are so [important for data collection, in this section](#). Your [EDC Technical Assistance Liaison](#) can also provide you with an orientation to these systems and are available to answer any questions you have.

Contact List Management System (CLMS)

In preparation for the need for future surveys and assessments, the EDC created the Contact List Management System (CLMS). The CLMS is a secure online system to serve as a centralized national repository for prehospital agency and hospital ED contact information. This repository was developed to reduce the burden for Program Managers, and more efficiently manage contact information for prehospital agencies and EDs needed for data collection. CLMS is open 24/7 all year long so EMSC Program Managers can update contact information, and basic agency and ED contact information are available at any time to EMSC Program Managers.

Tableau

Tableau is a data analysis and visualization software that links large datasets for tailored graphic display. Data within the Tableau system is hosted on a secured server and the website itself is encrypted requiring a username and password. The EDC utilizes this platform to give account users visual analytics from surveys and assessments. In turn, they can use this to report on EMSC Performance Measures and to assist in quality improvement initiatives.

Tableau dashboards were created to help EMSC managers explore their data, find key messages and areas for improvement, and to lessen the need for a high expertise level in Microsoft Excel. Any page, chart, or other visual can be downloaded as an image or a PDF for use in various reports and presentations. All the data behind these visualizations can also be downloaded in a tabular crosstab format for use in programs such as Excel for deeper analytics. Almost all data from any survey is included in a Tableau workbook and can be downloaded. Downloading and using any of the tabular data should follow the rules in this document. If a chart contains less than 5 different respondents that may identify a hospital or EMS agency should not be shared (see EDC Guidelines) except among a state EMSC program and stakeholders.

Access and Permission

Access and permission are NOT the same things. Understanding the difference between the two when sharing or using information from EDC-integrated systems helps EMSC SP grantees to keep data safe.

Access to data and information IS NOT permission for unrestricted use.

The EDC upholds best practices from the [Federal Cybersecurity and Infrastructure Security Agency](#) (CISA) regarding the principle of least privilege. This principle places restrictions on granting permissions for access:

“..a subject should be given only those privileges needed for it to complete its task. If a subject does not need an access right, the subject should not have that right. Further, the function of the subject (as opposed to its identity) should control the assignment of rights” (Bishop, 2020).

This means that only people who need access to data should be granted access to that data, regardless of the position they might hold.

EMSC SP grantee access to data through EDC integrated systems is provided through an Active Directory (AD) account that is managed and maintained by the EDC. Whole or partial access to data and information that are stored in the EDC Contact List Management System (CLMS) and Tableau is granted based on the need to use the information for programmatic purposes.

Those who have access to an AD account include leadership and staff from the Health Services and Resources Administration's (HRSA) EMSC Program, the EMSC Innovation and Improvement Center (EIIC), the EDC, EMSC SP grantees, and up to 3 of their support staff with EMSC Program Director/Manager approval.

Data that is stored in CLMS and Tableau comes from a variety of sources all working together for a common purpose. However, access to data and information by a user does not give the user unrestricted permission to use all or part of the information stored in these systems however they choose.

For example, access to CLMS is given to EMSC Program Managers and others within the state EMSC program who gather and store EMS agency and ED contact information in CLMS on behalf of their state. This information is unique to the manager and their relationship with the contact for the sole purpose of data collection processes. Sometimes the contact information listed in CLMS is different from the contact information given by a survey or assessment respondent. Any contact information provided by an EMSC manager or a respondent should be kept confidential.

We value the long-standing relationships our EMSC Program Managers have built in their states over the years and the people we serve within the EMSC Program. Protecting these relationships through data confidentiality, appropriate access, and proper use maintains trust among our collaborators and the EMSC Program.

Thank you for doing all you can to ensure safe and respectful data practices!

Please reach out to your EDC TA or state data supports if you have any questions about data confidentiality, use, or reporting outside of these recommendations.
This document is subject to periodic review and updates.

References

Bishop, M. (2020). *Computer security: Art and science* (Second). W. Ross MacDonald School Resource Services Library.

University of Utah, Institutional Review Board. Investigator Guidance Series: *Privacy and Confidentiality*. Retrieved May 11, 2023, from

<https://irb.utah.edu/resources/documents/pdf/IGS%20-%20Privacy%20and%20Confidentiality%20D0516.pdf>