

August 14, 2020

National EMS Coordinated Database Information Security Policy

Intent

This policy describes the data security for National EMS Coordinated Database (NEMSCD) information.

Scope

This policy applies to all computer systems and facilities related to and used for NEMSCD, with a target audience of the National Registry and Partners.

Definitions

Commission – The national administrative body of which all states that have enacted the Interstate Recognition of Emergency Medical Services Personnel Licensure Interstate Compact (REPLICA)

Compact – The Recognition of Emergency Medical Services Personnel Licensure Interstate Compact (REPLICA)

Member States – State EMS Offices that are members of the Compact or organizations authorized by Member States to submit data into NEMSCD on their behalf

NEMSCD – National EMS Coordinated Database, a database and reporting system capable of collecting, storing, safeguarding, and accessing information related to the licensure of all licensed individuals in Member States and any significant investigative information or adverse action taken against those persons or their licenses

NEMSCD - Administrator – The Director of Stakeholder Partnerships, appointed by the Executive Director as the delegated National Registry official responsible for the administration of NEMSCD.

Partner – Any non-employee of National Registry who has access to information systems or data.

Policy

1. Data Security Management

NEMSCD data security management shall be aligned and comply with the National Registry's Information Technology Systems Security Policy, utilizing security and privacy controls for Protecting Unclassified Information in Nonfederal Information Systems and Organizations. The National Registry uses the National Institute of Standards and

Technologies (NIST) 800-171, moderate-impact security controls framework for information security to protect the confidentiality, integrity and availability of information that is processed, stored and transmitted by National Registry information systems. National Registry has corporate security policies, procedures and contractual security requirements that promote the protection of intellectual property, employee and customer personal information, proper data security and data handling procedures, and data transmissions. National Registry also performs assessments, third-party audits, penetration tests, and vulnerability scans to help assure NIST 800-171, moderate-impact security control compliance.

2. Computer Incident Response

Computer Emergency Response Plans – National Registry management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service.

Computer Emergency Response Team- The Information Technology Director must organize and maintain a computer emergency response team (CERT), either in-house or vendor supplied, that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies such as virus infestations and hacker break-ins.

Mandatory Reporting - All suspected policy violations, system intrusions, virus infestations, and other conditions that might jeopardize National Registry information assets or National Registry information systems must be immediately reported to the Information Technology Director.

The National Registry shall notify the Commission within 24 hours if such violations, system intrusions, virus infestations or other conditions involve or potentially impact the NEMSCD.

3. Information Owner as defined by National Registry Information Systems Security Policy

As required by the National Registry Information Systems Security Policy, the NEMSCD Administrator is designated as the Information Owner for NEMSCD related data, with duties specified by National Registry Information Systems Security Policy to include designation of system security requirements.

4. Management of Known or Suspected Breach

The NEMSCD Administrator will ensure collaborative management of known or suspected breach of information security, as defined by the appropriate procedure and in conjunction with activities required by National Registry Information Systems Security Policy.

Rationale

The Agreement Between Interstate Commission for EMS Personnel Practice and National Registry of Emergency Medical Technicians necessitates the collaborative development of policy for defining the appropriate information systems security posture.

Related Policies and Procedures

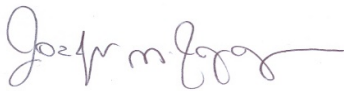
Information System Security Policy
NEMSCD Database Access Policy
NEMSCD Managing Suspected or Realized Cyber Breach Policy

References

Agreement Between Interstate Commission for EMS Personnel Practice and National Registry of Emergency Medical Technicians, executed June 29, 2018

Rules of the Interstate Commission for EMS Personnel Practice, www.emscompact.gov

NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations



Joseph Schmider, Chair

Interstate Commission for EMS Personnel Practice

CHAIR
Joe Schmider
Texas

VICE CHAIR
Donnie Woodyard
Colorado

SECRETARY
Joe House
Kansas

TREASURER
Wayne Denny
Idaho

MEMBER-AT-LARGE
Gary Brown
Virginia