U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration (NHTSA)

National Emergency Medical Services Information System (NEMSIS)

Responsible Official

David Bryson
Email:dave.bryson@dot.gov
Phone Number: 202-366-4302

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The National Emergency Medical Services Information System (NEMSIS) is a system used to collect, store, and share Emergency Medical Services (EMS) data from the U.S. States, Territories, Tribal Nations, and the District of Columbia (collectively, States). Through NEMSIS, the National Highway Traffic Safety Administration (NHTSA) develops and maintains a national standard for how patient care information resulting from prehospital EMS activations is documented. This information is voluntarily submitted to NEMSIS by State EMS Officials.

NEMSIS aims to improve prehospital motor vehicle crash related patient care through the standardization, aggregation, and utilization of point of care EMS data collected by emergency services personnel. NEMSIS is administered and funded by the NHTSA's Office of Emergency Medical Services and operated by the University of Utah NEMSIS Technical Assistance Center (NEMSIS TAC).

This Privacy Impact Assessment (PIA) is being conducted to disclose to the public what Personally Identifiable Information (PII) is collected from individuals, how the information is processed, shared, disclosed, and what controls NHTSA has in place to protect the identity of such individuals.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

NEMSIS is a collection of EMS information related to motor vehicle crashes and other EMS responses through the establishment of a standardized approach to document and report EMS incident response and patient care at the emergency services agency. The NEMSIS standard enables standard and automated transmission of EMS data from the point-of-care to state EMS data systems.

Pursuant to 23 U.S.C. § 403[2], NHTSA is authorized to conduct research and demonstration activities, including demonstration projects and the collection and analysis of highway and motor vehicle safety data and related information needed to improve traffic safety.

NEMSIS provides the framework for collecting, storing, and sharing standardized EMS data from States. The NEMSIS uniform dataset and database help EMS stakeholders more accurately assess EMS needs and performance at a local, state, and national levels. Data from NEMSIS is also used to help benchmark performance, determine the effectiveness of clinical interventions, and facilitate cost-benefit analyses.

The University of Utah administers the NEMSIS TAC on behalf of NHTSA. The NEMSIS TAC negotiates Data Use Agreements (DUAs) with States to collect the EMS data.[3]

[2] Section 403 permits the collection of motor vehicle safety data to:
(A) all aspects of highway and traffic safety systems and conditions relating to, among other things, emergency medical services, including the transportation of the injured;
(B) human behavioral factors and their effect on highway and traffic safety,
(C) an evaluation of the effectiveness of countermeasures to increase highway and traffic safety, including occupant protection and alcohol- and drug-impaired driving technologies and initiatives;
(D) the development of technologies to detect drug impaired drivers;
(F) the effect of State laws on any aspects, activities, or programs described in subparagraphs (A) through (E).

[3] https://nemsis.org/using-ems-data/state-data-use-agreements/

The State submitted information supports NHTSA to research and develop programs related to EMS activities responding to motor vehicle crashes. NHTSA research supports the development of EMS evidence-based guidelines to improvement in EMS systems, out-hospital clinical care, and health and safety of the EMS workforce responding to motor vehicle crashes.

States submit 165 data elements from an EMS response to NEMSIS. The data includes information that describe the EMS agency, the activation and response of the individual EMS units to the emergency, the type of emergency care provided to individuals on scene and during transport to a health facility, the transport decision, the disposition of the patient and incident, and the EMS system times, such as response time. In particular, the types of emergencies that the reports cover are:

- pedestrian injuries and fatalities under EMS care;
- motor-vehicle crash injuries; and
- non-vehicle related emergencies (e.g. heart attack at a residence).

States submit deidentified information to NEMSIS. They do not submit the patient's name, address, phone number, email, date of birth, social security number, or other identifying information to NEMSIS. From the 165 data elements submitted from an EMS to NEMSIS, the only data related to a patient requiring EMS care is:

- Patient's county, state, and zip code
- Gender
- Race
- Age
- Age Units (minutes, hours, days, months, years)
- Injury/medical condition

States also submit to NEMSIS the county, state, zip, date, and time of where the incident occurred.

NEMSIS generates and assigns a unique identifier to a record when it is created in the system, which allows the record to be retrieved if the information needs to be updated.

NHTSA makes NEMSIS data publicly available research datasets, national reports, and searchable databases.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk.

The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[4], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[5].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Prior to the initiation of a data collection, and in accordance with the Paperwork Reduction Act (PRA), NHTSA obtains approval from the Office of Management and Budget (OMB) to conduct a collection of information. Prior to submission for approval by OMB, the public is notified of the proposed collection through a Federal Register notice and is given 60 days to provide comments through an electronic docket at regulations.gov. The notice includes the purpose of the collection—including the specific information that will be collected from the State participants and the forms used to collect this information. After addressing any comments received during the comment period, NHTSA submits a second Federal Register notice notifying the public that the collection is being submitted to OMB and invites public comment to be sent directly to OMB. The OMB approved information collection request (ICR) number for NEMSIS is 2127-0717 and can be accessed here.

Additionally, NHTSA also informs the public that their PII is collected and stored through this Privacy Impact Assessment (PIA) to inform the public that its information is stored and used by NEMSIS. This PIA identifies the information collection's purpose, use, and storage of PII. It can be found at: https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

NEMSIS contains deidentified records that are not retrieved by a unique identifier associated with an individual. While the records have information that relate to individuals, the records are about the EMS response, treatment, and disposition to improve EMS care and as such, NEMSIS does not require a System of Record Notice (SORN).

[4] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[5] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

Users' usernames accessing the system are collected in audit logs to understand the users' accesses and troubleshoot technical issues. These records are maintained in accordance with DOT/ALL 13 - Internet/Intranet Activity and Access Records - 67 FR 30757 - May 7, 2002.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Deidentified information submitted to NEMSIS is provided by States that are obtained during an EMS call to render aid to an individual during an emergency.

NEMSIS contains records related to individuals who received EMS care and transport to a hospital or other health facility. The purpose of the system is to collect data on the EMS incident itself to support EMS clinical assessment and research of EMS activities. The names of the patients of each incident are unnecessary for purposes of the system. Accordingly, NHTSA does not obtain the name, social security number, or other unique identifier that would permit NHTSA to identify a specific individual that is the subject of the evaluation. Because the information obtained by NHTSA is anonymized, the Agency would be unable to identify individual records and correct them. If an individual (patient or guardian) would like to get access to the information collected by a State EMS, the individual (patient or guardian) must contact the EMS office in the State containing the record.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

Pursuant to 23 U.S.C. § 403[2], NHTSA is authorized to conduct research and demonstration activities, including demonstration projects and the collection and analysis of highway and motor vehicle safety data and related information needed to improve traffic safety. The NEMSIS collection obtains information related to emergency medical services in response to motor vehicle crashes, including the transportation of the injured.

The OMB published the approved information collection requests (ICR) for NEMSIS. The NEMSIS ICR number is 2127-0717.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

NHTSA collects, uses, and retains data that are relevant and necessary for the purposes of improving EMS treatment related to traffic safety. The data submitted to NEMSIS is anonymized, but includes information that is relevant for NHTSA's purposes such as the EMS agency, the activation and response of the individual EMS units to an emergency, the type of emergency care provided to individuals on scene and during transport to a health facility, the transport decision, the disposition of the patient and incident, and the EMS system times, such as response time. NHTSA limits the type of patient information it collects to the patient's county, state, ZIP code, gender, race, age and injury or medical condition.

NHTSA will submit to the National Archives and Records Administration (NARA) a records retention schedule to dispose of NEMSIS records after 20 years. All records are kept permanently until NARA approves the proposed record retention schedule.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

NHTSA collects and uses only the data elements that are relevant and necessary for the purposes of the establishment of a standardized approach to document and report EMS incident response and patient care to improve patient care, improving EMS curriculums, accessing resources for natural disasters and mass casualty incidences.

NHTSA has limited access to and use of NEMSIS data to NHTSA employees and its contractors in accordance with the roles and responsibilities to analyze the collected data, create reports and publish the results on the NEMSIS website.

NHTSA publishes annual deidentified NEMSIS research datasets, maintenance of national reports and searchable databases to the public[6],[7].

Users' usernames accessing the system are collected in audit logs to understand the users' accesses and troubleshoot technical issues. These records are maintained in accordance with DOT/ALL 13 - Internet/Intranet Activity and Access Records - 67 FR 30757 - May 7, 2002.

[6] https://nemsis.org/using-ems-data/
[7] https://nemsis.org/view-reports/

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

NEMSIS receives all EMS agency data directly from the State EMS agencies. These EMS agencies have the responsibility for ensuring that the information provided is accurate and must also correct any inaccurate information promptly. The system provides data validation checks to make sure information is entered in the correct data field and format.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

NHTSA requires a secure web-based, data transmission process using TLS or VPN technologies, both of which provide at least 128-bit encryption, and firewall hardware, automatic network intrusion detection and prevention for States to transmit data to NEMSIS. States submit raw data (XML) via a web service to the NEMSIS system. Data is processed through a series of defined business rules, which include removal of duplicates and validation against both the NEMSIS National Standard and Data Dictionary. Records that have passed validation are loaded into a Data Warehouse and a subset of that data is transferred to a data mart, which makes the data accessible by NEMSIS State, Federal and professional organizations via reporting tools such as Tableau. These reports are refreshed on a pre-defined scheduled (daily, weekly, ad-hoc).

Data collected and maintained in NEMSIS is safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. NHTSA security policy and practices are based on NIST Information Risk Management and Security standards. These are supplemented by privacy-specific guidance provided in NIST 800-122 and NIST Special Publication 800-53 Revision 4, and the DOT Privacy Risk Management Policy 1351.18 and the Office of Management and Budget circular A-130, Section 8b (3), Securing Agency Information Systems. The NIST security guides and standards are used by NHTSA to, among other things; assess information confidentiality, integrity, and availability risks, identify required security safeguards, and adjust the strength and rigor of those safeguards to reduce risks to appropriate acceptable levels. Under this policy, NHTSA has implemented appropriate Administrative, Physical, and Technical safeguards to protect the confidentiality, availability, and integrity of the NEMSIS system and information.

NHTSA maintains the security of data in NEMSIS through each step in the data collection process. Security varies depending on the technology to collect the information, the format of the data and the way it is transferred to NEMSIS.

NHTSA employees and contractors with NEMSIS access must adhere to DOT policy and procedures to ensure that the data collected, regardless of form, is protected from any misuse or unauthorized disclosure. Furthermore, all NEMSIS users are required to take security training and sign a Rules of Behavior (ROB) document prior to obtaining access to any NEMSIS assets.

Further protection of data in NEMSIS include:

- All NHTSA employees and contractors undergo the mandatory DOT background checks prior to being granted access to the DOT network. In addition, all NEMSIS users receive both general, and role-based security training on an annual basis.
- NHTSA utilizes role-based security in NEMSIS to restrict user access to specific applications depending on their roles in the studies.
- NHTSA enforces assigned authorizations in NEMSIS for controlling access to the system using multi-factor authentication technology.
- The NEMSIS system maintains an audit trail of changes made, date/time of change and the user for each database change.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

NHTSA is responsible for identifying, training, and holding its personnel and contractors accountable for adhering to DOT/NHTSA privacy and data security policies, and regulations. NHTSA follows the fair information practice principles (FIPPS) as best practices for the protection of information associated with the records NEMSIS. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to the protection, retention, and destruction of records. The NHTSA Security and Privacy Officers will conduct periodic security and privacy reviews of NEMSIS consistent with the Office of Management and Budget Circular A-130, Section 8b (3), Securing Agency Information Systems and follow the DOT Privacy Risk Management Policy 1351.18. https://www.transportation.gov/sites/dot.gov/files/docs/CIOP - Privacy Risk Management - 1351.18 - Policy - 09302014.pdf.

Responsible Official

David W. Bryson
System Owner
EMS Specialist, Office of Emergency Medical Services

Prepared by: Jose R. Delgado-Forastieri, NHTSA Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2025.07.01 15:44:44 -04'00'