NEMSIS Version 3 Compliance Policy

Date

September 18, 2015 (initial release)
September 29, 2017 (updated)
December 3, 2019 (process changes and v3.5.0 testing)
September 10, 2020 (added "defined lists" requirement)
November 24, 2020 (added requirements in "Maintaining Compliance" section)
December 1, 2021 (update to policy section)
November 23, 2022 (update to "Losing Compliance" section)
December 28, 2022 (added "Sunsetting NEMSIS Version" section)
June 1, 2023 (updated)
January 31, 2024 (added major and minor release sections)
April 1, 2024 (added when to join v3 Implementation Calls)
June 10, 2024 (added clarification about software version updates)

Resources

Compliance Process: https://nemsis.org/technical-resources/version-3/v3-compliance/

Purpose

The purpose of this document is to define "Compliance" with respect to the NHTSA National EMS Information System Dataset (NEMSIS dataset) actively being accepted into the national data repository outlined in the policy below. The term compliance (or "compliant") may only be used by an EMS data system or EMS software vendor if the terms of this policy are met in full. No marketing of any EMS data product as being compliant with the NEMSIS dataset may be done, except as defined in this policy.

Policy

Any EMS data product can be labeled as "Compliant" at the "Collect and Send" or "Receive and Process" level with the NEMSIS Dataset when the following conditions have been confirmed by the NEMSIS Technical Assistance Center (TAC):

- For version 3.5.0 and later, the NEMSIS Dataset is used within the EMS data system as defined in the XSD and Data Dictionary.
- The NEMSIS Demographic Dataset is used within the EMS data system as defined by the XSD and Data Dictionary.
- The NEMSIS EMS Dataset is used within the EMS data system as defined in the XSD and Data Dictionary.

- The NEMSIS XML standard is used to export data from the EMS data system as defined in the XSD and Data Dictionary.
- The EMS data system monitors and controls modifications within the EMS data system to prevent changes that would be inconsistent with the NEMSIS Dataset standard.

NEMSIS Compliance only applies to versions of the national data standard currently being accepted by the NEMSIS TAC for inclusion in the national data repository. Once the NEMSIS TAC has closed a prior version of the standard, all compliance certifications for that version are considered expired. For questions regarding current NEMSIS standard versions, please refer to the NEMSIS website or contact the NEMSIS TAC helpdesk.

Procedure

An EMS data system can be labeled as "Compliant" at the "Collect and Send" or "Receive and Process" level with the National Emergency Medical Information System (NEMSIS) Dataset by meeting the following conditions:

Collect Data

- For versions 3.5.0 and later, the software is able to use information from a current NEMSIS State dataset for configuration.
- The full current NEMSIS Demographic standard is implemented in the user interface.
- The full current NEMSIS emergency medical services (EMS) standard is implemented in the user interface.
- The software has implemented the NEMSIS TAC Defined Lists for all elements where they are applicable.
- The software is capable of implementing custom elements. As a part of the testing process, custom elements will be provided in the test cases.
- XML Schema (XSD) validation is used when a Demographic record is finalized.
- XML Schema (XSD) validation is used when an EMS record is finalized.
- Schematron validation is used for business rules when a Demographic record is finalized.
- Schematron validation is used for business rules when an EMS record is finalized.
- The software is able to validate data using multiple Schematron files (national, state, etc.).
- Natural language expressions of validation warnings and errors are presented to the user.
- The software is able to properly submit data using the current NEMSIS Web Service standard.

Receive and Process

- The software is able to properly interoperate using the current NEMSIS Web Service standard.
- For version 3.5.0 and later, the full NEMSIS v3 State dataset standard is implemented in the user interface.
- For version 3.5.0 and later, XML Schema (XSD) validation is used when a StateDataSet record is finalized.
- For version 3.5.0 and later, schematron validation is used for business rules when a StateDataSet record is finalized.

- For version 3.5.0 and later, natural language expressions of StateDataSet validation warnings and errors are presented to the user.
- For version 3.5.0 and later, the software is able to send State data, including change log notes.
- The software is able to receive Demographic and EMS data.
- The software is able to send Demographic and EMS data—full dataset and national elements only.
- XML Schema (XSD) validation is used when Demographic and EMS data are received.
- Schematron validation is used for business rules when Demographic and EMS data are received.
- The software can validate received data using multiple Schematron files (national, state, etc.).

Major Version Release

A major version is denoted in the first two leftmost numbers. For example, a change in the version number represented as v3.4.0 updated to v3.5.0 would be a major version change. A major release can contain but is not limited to the following:

- Not backward compatible without translation
  - Any document created in the old version may not be valid in the new version.
  - Any document created in the new version may not be valid in the old version.
  - Requires states to move before local agencies.
- Changes can include:
  - XML structure changes
  - Data type changes within an element
  - New attributes to the standard
  - New Required or Mandatory elements
  - Deprecation of Mandatory elements
  - Section changes
  - Schematron rule changes from warning to error
  - Usage changes to Required or Mandatory
  - Usage changes to Optional
  - Removal of elements
- Any change that creates a more restrictive structure.
- Compliance testing is required.
- Vendors will be required to complete compliance testing with the latest version after a major version release.

Minor and Critical Patch Version Release

A minor version is denoted in the third number after the first two. For example, a change in the version number represented as v3.5.0 updated to v3.5.1 would be a minor version change. A critical patch will reflect the date and critical patch number and will be denoted after the third decimal in the version number. For example, a change in the version number for a critical patch from critical patch three 3.5.0.211008CP3 to critical patch four 3.5.0.230317CP4. A critical patch is a change that is immediately necessary and will not have a set schedule.

A minor release can contain but is not limited to the following:

- Backward compatible without translation.
    - Any document created in the old version would be valid in the new version.
    - Any document created in the new version may not be valid in the old version.
    - Requires states to move before local agencies.
- Changes can include:
    - New values to an existing element
    - Deprecation of values to an existing element
    - New optional attributes to an existing element
    - New Recommended or Optional elements
    - Changing elements from Required to Recommended
    - Schematron rule changes from error to warning
    - Removing schematron rules
    - Enhancements of the data dictionary
    - Schematron verbiage changes to warning or error messages
- No XML structure change.
- Any change that creates a more permissive structure.
- Compliance testing will begin in the year following the minor release.
    - Any vendor testing in the year after a minor release, whether for initial or recertification, will be testing on the new minor version. For example, if v3.5.1 were released in 2024, then compliance testing for v3.5.1 will be in the 2025 test cases for compliance.

Maintaining Compliance

In order to maintain data integrity and quality, the NEMSIS Technical Assistance Center accepts data from state and territories Receive and Process EMS software vendors that are tested and certified as a NEMSIS compliant product. The NEMSIS TAC does not accept data directly from Collect and Send EMS software vendors.

The recertification requirements in this section are effective after January 1, 2021. This section describes what actions are taken if a vendor fails to meet the requirements and how they can return to good standing for compliance. Vendors that do not adhere to the Compliance Policy will lose their compliant status.

It is the responsibility of the vendor to maintain current contact information with the NEMSIS TAC. The TAC recommends that multiple vendor points of contact are established and the respective email addresses be added to the NEMSIS Google Group, which will serve as the primary method of group communication.

v3 Implementation Call Attendance Requirement

All vendors compliant with the NEMSIS v3.4.0 standard or later NEMSIS data standards are required to attend 70% of the twice-monthly v3 Implementation calls held each year. This requirement begins as

soon as the vendor has successfully completed compliance testing. The NEMSIS TAC tracks vendor attendance on every call. All vendors are required to join the v3 Implementation calls within ten minutes of the call starting. Any vendor joining past that point will not receive credit for the v3 Implementation call. Attendance for the entirety of the meeting is expected. Vendors shall not use unattended accounts to attend v3 Implementation calls. It is the responsibility of every vendor to ensure that the attendees' name and the company they represent are clearly identified on the participation list during each call. Vendors can monitor their participation on the NEMSIS website here.

For vendor companies with more than one compliant product, while we welcome a representative for each product team, we only require one representative per company for call attendance. It is expected that any pertinent information will be communicated among product teams.

At the end of each calendar year, any vendor who has fallen below the 70% attendance requirement for that year will be put on probation.

Annual Meeting Attendance Requirement

All vendors compliant on NEMSIS v3.4.0 or greater are required to attend the general sessions of the NEMSIS Annual Meeting held each year. This meeting will be held once a year in Utah. The NEMSIS TAC will begin tracking a vendor's attendance at this meeting after the vendor has attained initial compliance certification. At the end of each calendar year, any vendor who failed to attend this meeting will be put on probation.

Vendors who will complete the compliance process within thirty (30) days prior to the start of the Annual Meeting will be expected to attend the annual meeting. If there are extenuating circumstances, a compliant vendor may request, in writing, a one-time abeyance of this requirement. Please note, this request is subject to approval by the NEMSIS Compliance Officer and approval is not assured. A vendor is limited to a single request regardless of the various EMS software products that are submitted for NEMSIS compliance.

Recertification Testing Requirement

All software products compliant with the NEMSIS v3.4.0 standard or later NEMSIS data standards are required to complete recertification testing within two years of the "Compliant Since" or "Recertification Date", whichever is later, listed on the NEMSIS.org website status tracking page. The recertification testing applies to the latest version of each software product a vendor has listed on the status tracking page. The process for recertification testing is similar to the process for initial testing, so vendors are familiar with the requirements.

Any software vendor that institutes a major software version update to a previously NEMSIS compliant software product, will need to complete the recertification process within six months or by the scheduled recertification date, whichever comes first.

Any software vendor who fails to complete recertification of a software product by the two-year deadline of the most recent certification date will **lose that software product's status as NEMSIS compliant**. This policy extends to each version of the NEMSIS standard actively being tested and accepted by the NEMSIS TAC. In extenuating circumstances, the NEMSIS TAC may grant up to a thirty-day extension of this deadline. An email request for an extension including a thorough explanation

must be submitted to the NEMSIS Help Desk and must be provided at a minimum of thirty (30) days prior to expiration. Please note, approval is not assured.

If an extension is granted, the software product will be removed from the v3 Compliant Software Testing Status page. When completed successfully, the software product will be reinstated on the v3 Compliant Software Testing Status page as appropriate.

Sunsetting NEMSIS Versions

Initial compliance applications will not be accepted twelve months prior to the end date of a sunsetting NEMSIS version. An email request for an exception including a thorough explanation must be submitted to the NEMSIS Help Desk. The NEMSIS Compliance Officer will review and decide based on the request explanation. Please note, approval is not assured.

Recertification compliance applications will not be accepted 6 months prior to the end date of a NEMSIS version. An email request for an exception including a thorough explanation must be submitted to the NEMSIS Help Desk. The NEMSIS Compliance Officer will review and decide based on the request explanation. Please note, approval is not assured.

If there is a software program that has a compliance expiration within 90 days of the end date of a NEMSIS version, an extension may be requested by the vendor to extend the expiration date of their compliance to the end date of the expiring NEMSIS version. An email request for an exception including applicable EMS software names and dates must be submitted to the NEMSIS Help Desk. The NEMSIS Compliance Officer will review the request.

Probation

Any vendor or EMS software product that does not continuously meet the compliance requirements including the recertification timeline, v3 Implementation call attendance, and NEMSIS Annual Meeting attendance will be placed on probation denoted on the Compliant Software Testing Status page of the NEMSIS website.

In order to complete probation and return to good standing, the EMS software product vendor must correct the issue that resulted in probationary status and attend the following six v3 Implementation calls held after they have been notified of probationary status.

An EMS software product may not be on probation for any two consecutive years. If an EMS software product completes probation, but then fails to meet any of the recertification requirements for the following year or fails to meet the compliance maintenance requirements, the software product will **lose status as NEMSIS compliant**.

Losing Compliance

EMS software products that lose NEMSIS compliant status will immediately be removed from the Compliant Software Testing Status page of the NEMSIS website. The NEMSIS TAC will notify the states/territories in which they operate to inform State Data Managers and EMS Directors of the vendor's loss of compliance. Non-compliant software products and/or vendors must immediately discontinue the use of relevant NEMSIS compliance logos and statements in the marketing of their products.

Regaining Compliance

A vendor who has lost NEMSIS compliance for any reason can become compliant again by completing a six-month waiting period from the date of non-compliance, then apply for and complete testing as if they were a new vendor. When a NEMSIS version is sunsetting, the Sunsetting Policy supersedes the ability to regain compliance.

Appeals Process

If a vendor wishes to appeal the designation of probation or loss of compliance, they may submit their written request, via email, within thirty (30) days of the date of probation or loss of compliance. The request should include a detailed explanation and be sent to the NEMSIS Help Desk which will be relayed to the NEMSIS Compliance Officer for review.

Disclaimer

The NEMSIS TAC can only verify the user interface, files, and documentation as provided by the EMS software developers. The NEMSIS TAC reserves the right to remove any EMS software which has obtained NEMSIS v3 Compliance through this policy from the list of Compliant EMS Software, maintained on the official NEMSIS website if it is determined that the EMS software developer provided false information or subsequently makes changes to the software version after compliance status was granted that results in the software falling out of compliance with the NEMSIS standards.

All appropriate requirements contained in this document must be completed for a product to be considered NEMSIS compliant. In rare circumstances, a product may be considered NEMSIS compliant (with qualification) if a levied legal injunction or restriction prohibits the inclusion of a software feature associated with the NEMSIS compliance requirements.

Any EMS system, state, or territory using this compliance validation as a part of a contract pricing or request for proposal should either request additional documentation from the EMS software developer (specifically of test cases which have been used in the validation of the software) or test the software using a series of test cases reflective of the EMS data elements which will be implemented by the EMS system.