

NEMSIS Version 3 Compliance Policy

Date

September 18, 2015
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)

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.

NEMESIS TAC Version 3 Policy

NEMESIS Compliance only applies to versions of the national data standard currently being accepted by the NEMESIS TAC for inclusion in the national data repository. Once the NEMESIS TAC has closed a prior version of the standard, all compliance certifications for that version are considered expired. For questions regarding current NEMESIS standard versions, please refer to the [NEMESIS website](#) or contact the [NEMESIS 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 (NEMESIS) 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 NEMESIS State dataset for configuration.
- The full current NEMESIS Demographic standard is implemented in the user interface.
- The full current NEMESIS emergency medical services (EMS) standard is implemented in the user interface.
- The software has implemented the NEMESIS 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 NEMESIS Web Service standard.

Receive and Process

- The software is able to properly interoperate using the current NEMESIS Web Service standard.
- For version 3.5.0 and later, the full NEMESIS 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.

NEMSYS TAC Version 3 Policy

- 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 is able to validate received data using multiple Schematron files (national, state, etc.).

Maintaining Compliance

In order to maintain data integrity and quality, the NEMSYS Technical Assistance Center accepts data from state and territories Receive and Process EMS software vendors that are tested and certified as a NEMSYS compliant product. The NEMSYS 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 NEMSYS TAC. The TAC recommends that multiple vendor points of contact are established and the respective email addresses be added to the [NEMSYS Google Group](#), which will serve as the primary method of group communication.

v3 Implementation Call Attendance Requirement

All vendors compliant with the NEMSYS v3.4.0 standard or later NEMSYS 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 NEMSYS TAC tracks vendor attendance on every call. It is the responsibility of every vendor to ensure that their name and the company they represent are clearly identified on the participation list during each call. Vendors can monitor their participation on the NEMSYS 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 NEMSYS v3.4.0 or greater are required to attend the general sessions of the NEMSYS Annual Meeting held each year. This meeting will be held once a year in Utah. The NEMSYS 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.

NEMESIS TAC Version 3 Policy

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 NEMESIS 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 NEMESIS compliance.

Recertification Testing Requirement

All software products compliant with the NEMESIS v3.4.0 standard or later NEMESIS data standards are required to complete recertification testing within two years of the “Compliant Since” or “Recertification Date”, whichever is later, listed on the NEMESIS.org website [status tracking page](#). The recertification testing applies to 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 NEMESIS compliant software product, will need to complete the recertification process.

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 NEMESIS compliant**. This policy extends to each version of the NEMESIS standard actively being tested and accepted by the NEMESIS TAC. In extenuating circumstances, the NEMESIS 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 [NEMESIS 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 NEMESIS Versions

Initial compliance applications will not be accepted twelve months prior to the end date of a sunseting NEMESIS version. An email request for an exception including a thorough explanation must be submitted to the [NEMESIS Help Desk](#). The NEMESIS 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 NEMESIS version. An email request for an exception including a thorough explanation must be submitted to the [NEMESIS Help Desk](#). The NEMESIS 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 NEMESIS version, an extension may be requested by the vendor to extend the expiration date of their compliance to the end date of the expiring NEMESIS version. An email request for an exception including applicable EMS software names and dates must be submitted to the [NEMESIS Help Desk](#). The NEMESIS 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 NEMESIS Annual Meeting attendance will be placed on probation denoted on the [Compliant Software Testing Status](#) page of the NEMESIS 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 NEMESIS compliant**.

Losing Compliance

EMS software products that lose NEMESIS compliant status will immediately be removed from the [Compliant Software Testing Status](#) page of the NEMESIS website. The NEMESIS 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 NEMESIS compliance logos and statements in the marketing of their products.

Regaining Compliance

A vendor who has lost NEMESIS 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 NEMESIS version is sunseting, the Sunseting 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 [NEMESIS Help Desk](#) which will be relayed to the NEMESIS Compliance Officer for review.

Disclaimer

The NEMESIS TAC can only verify the user interface, files, and documentation as provided by the EMS software developers. The NEMESIS TAC reserves the right to remove any EMS software which has obtained NEMESIS v3 Compliance through this policy from the list of Compliant EMS Software, maintained on the official NEMESIS 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 NEMESIS standards.

NEMESIS TAC Version 3 Policy

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