NEMSIS Version 3 Compliance Policy

Date

November 23, 2022

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 Version 3 Dataset. 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 NHTSA version 3 dataset may be done, except as defined in this policy.

Policy

Any EMS data system can be labeled as "Compliant" at the "Collect Data" or "Receive and Process" level with the NHTSA Version 3 Dataset when the following conditions have been confirmed by the National EMS Information System (NEMSIS) Technical Assistance Center:

- *(v3.5.0)* The NEMSIS Version 3 State Dataset is used within the EMS data system as defined.
- The NEMSIS Version 3 Demographic Dataset is used within the EMS data system as defined.
- The NEMSIS Version 3 EMS Dataset is used within the EMS data system as defined.
- The NHTSA/NEMSIS Version 3 XML standard is used to export data from the EMS data system as defined.
- A structure within the EMS data system is in place to monitor and control changes within the EMS data system which would lead to inconsistency with the NHTSA Version 3 Dataset.

NEMSIS Compliance only applies to versions of the standard currently being accepted by the NEMSIS Technical Assistance Center for inclusion in the national registry. Once the NEMSIS TAC has closed a prior version of the standard, all compliance certifications for that version are considered expired. As of September 1st, 2021 the only current versions of the NEMSIS standard for which compliance certifications are offered are v3.4.0 and v3.5.0.

Procedure

An EMS data system can be labeled as "Compliant" at the "Collect Data" or "Receive and Process" level with the NHTSA Version 3 EMS Dataset by meeting the following conditions:

Collect Data

- *(v3.5.0)* The software is able to use information from a NEMSIS v3 State dataset for configuration.
- The full NEMSIS v3 Demographic standard is implemented in the user interface.
- The full NEMSIS v3 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 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 NEMSIS v3 Web Service standard.

Receive and Process

- The software is able to properly interoperate using the NEMSIS v3 Web Service standard.
- *(v3.5.0)* The full NEMSIS v3 State dataset standard is implemented in the user interface.
- *(v3.5.0)* XML Schema (XSD) validation is used when a StateDataSet record is finalized.
- *(v3.5.0)* Schematron validation is used for business rules when a StateDataSet record is finalized.
- *(v3.5.0)* Natural language expressions of StateDataSet validation warnings and errors are presented to the user.
- *(v3.5.0)* 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 is able to validate received data using multiple Schematron files (national, state, etc.).

Maintaining Compliance

In order to maintain data integrity and quality, the NEMSIS Technical Assistance Center only accepts EMS data from EMS software vendors that are tested and certified as a NEMSIS compliant product. Vendors that do not adhere to the Compliance Policy will lose their compliant status.

The recertification requirements in this section take effect on 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.

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 their email addresses be added to the NEMSIS Google Group, which will serve as the primary method of communication.

v3 Implementation Call Attendance Requirement

All vendors compliant on NEMSIS v3.4.0 or greater 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. 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 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 assumed 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 entire NEMSIS v3 Implementation Annual Meeting held each year. This in-person three-day meeting is normally held in the fall in Utah. The NEMSIS TAC will begin tracking a vendor's attendance at this meeting after they have attained their 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 initiate the compliance process within sixty (60) days prior to the start of the Annual Meeting may request, in writing, a one-time abeyance of this requirement if it is not feasible for their team to attend on short notice. This request is subject to approval by the NEMSIS Compliance Officer. A vendor is limited to a single request regardless of the various products they present for compliance.

Recertification Testing Requirement

All vendors compliant on NEMSIS v3.4.0 or greater are required to complete recertification testing within two years of their last testing date. The process for recertification testing is identical to the process for initial testing, so vendors are familiar with requirements. Any vendor who fails to complete recertification within two years of their last testing date will **lose their status as NEMSIS compliant**. In extenuating circumstances, the NEMSIS Compliance Officer may grant up to a thirty day extension of this deadline.

Probation

Vendors on probation will be denoted on the Compliant Software Testing Status page of the NEMSIS website. Links to the company's website will be removed.

In order to complete probation and return to the list of compliant products, a vendor must attend the following six v3 Implementation Calls held after they have been notified of probationary status.

Vendors may not be on probation for any two consecutive years. If a vendor completes probation, but then fails to meet recertification requirements for the following year, they will **lose their status as NEMSIS compliant**.
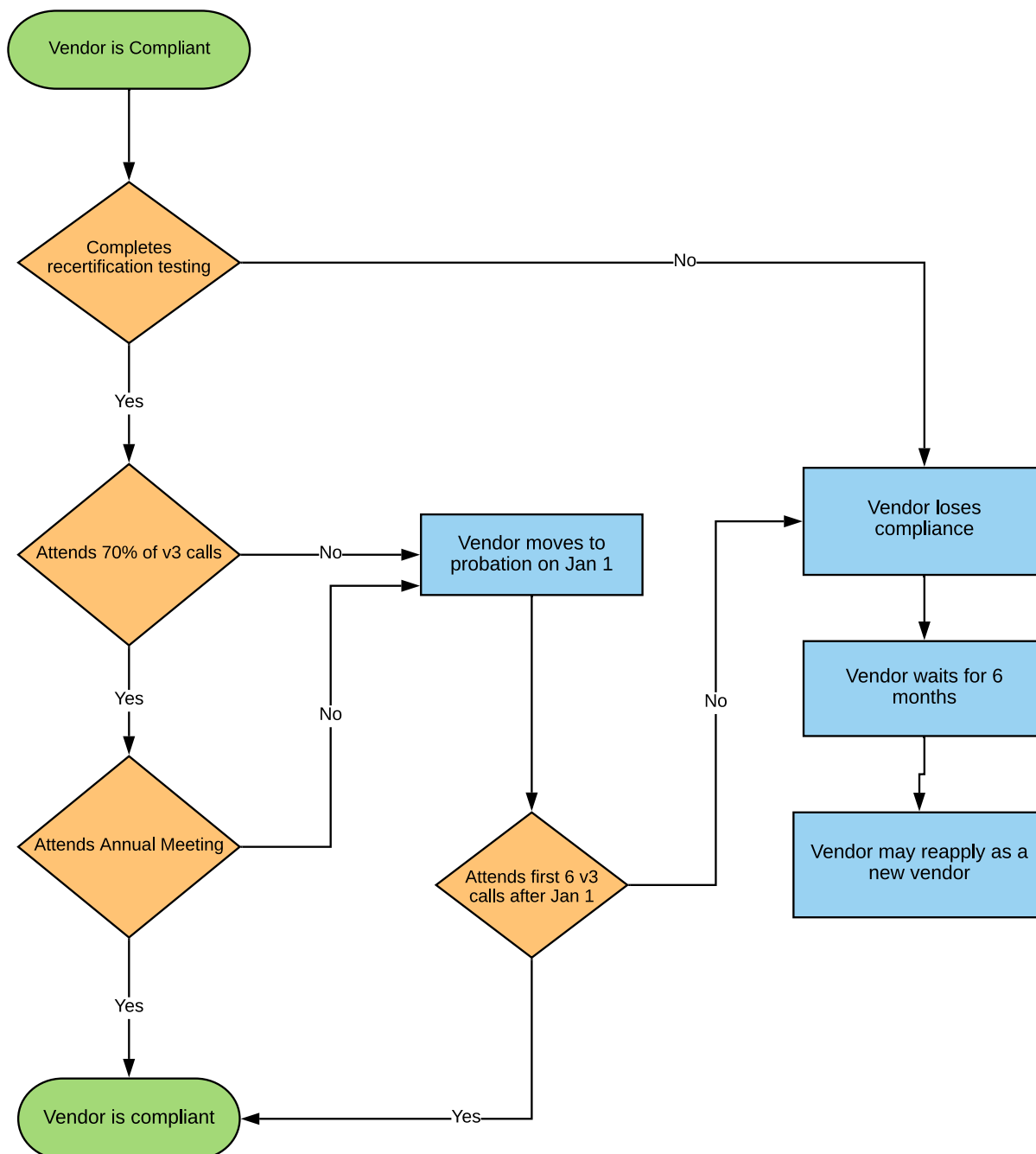
Losing Compliance

Vendors who lose their NEMSIS compliance will immediately be removed from the Compliant Software Testing Status page of the NEMSIS website. The NEMSIS TAC will also contact the states/territories in which they operate to inform state data managers and EMS directors of the vendor's loss of compliance. Non-compliant vendors must immediately discontinue 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 and then apply for and complete testing as if they were a new vendor.

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 days of the date of probation or loss of compliance. The request should include a detailed explanation and be sent to the NEMSIS Compliance Officer, Program Director, or Principal Investigator.

```
Vendor is Compliant
        │
        ▼
Completes ──────────────No──────────────┐
recertification testing                 │
        │                               │
       Yes                              │
        ▼                               ▼
Attends 70% of v3 calls ──No──▶ Vendor moves to      Vendor loses
        │              ┌──────▶ probation on Jan 1   compliance
       Yes             No                 │              │
        ▼              │                  ▼              ▼
Attends Annual Meeting │         Attends first 6 v3  Vendor waits for 6
        │              │         calls after Jan 1   months
       Yes             │              │    │            │
        ▼              │             Yes   No           ▼
Vendor is compliant ◀──┘                   │       Vendor may reapply as a
                    ◀──────Yes─────────────┘       new vendor
```

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.