



Third-Party Electronic Visit Verification (EVV) Vendor Requirements:

To engage in the Nebraska Department of Health and Human Services (DHHS) EVV Program, third-party EVV vendors must meet the following minimum requirements:

- 1. Be compliant with the 21st Century Cures Act by electronically verifying the following:**
 - a. Individual receiving the service(s);
 - b. Individual providing the service(s);
 - c. Location of service(s) delivery;
 - d. Exact date of service(s) delivered;
 - e. Exact time the service(s) begin;
 - f. Exact time the service(s) end; and
 - g. Type of service(s) performed.
- 2. Allow authorized users to enter participant information, which includes:**
 - a. Name;
 - b. Address;
 - i. To be associated to each participant for verification purposes.
 - ii. Include, at minimum, street address, city, state, and zip code.
 - iii. Any additional addresses entered will not remove previously entered addresses from the system records.
 - c. Phone Number;
 - d. State Assigned ID (N-Focus ID)
 - e. Payer ID; and
 - f. Any other identifiers need to uniquely identify the participant for services and billing.
- 3. Allow authorized users to enter rendering provider (i.e. employee, caregiver, contractor, etc.) information, to include the following:**
 - a. Name;
 - b. Address;
 - i. Include, at minimum, street address, city, state, and zip code.
 - c. Phone Number;
 - d. Date of Birth;
 - e. Last four (4) digits of the social security number; and
 - f. Email Address

4. **User access will be controlled, so as to limit any unauthorized entry, manipulation, or review of EVV data, to include the following:**
 - a. The individual is not permitted to access the EVV system;
 - b. The individual is not authorized by the Medicaid and billing provider to enter information in the EVV system on behalf of that provider;
 - c. The individual is not permitted to see participant or agency provider data; and
 - d. Must be Health Insurance Portability and Accountability Act (HIPAA) compliant and provide appropriate security and privacy controls to protect personally identifiable information (PII) and protected health information (PHI) data.
 - i. Ensures all Protected Health Information (PHI) is encrypted at all times in transit and at rest.
5. **To ensure providers and provider agencies have EVV capability in all areas being serviced, the third-party vendor, at minimum, must utilize one (1) or more of the following:**
 - a. Mobile application which utilizes Global Positioning Systems (GPS) will be the primary method of collecting visit information;
 - i. Must operate in offline mode to capture visit data when cellular or Wi-Fi connectivity is unavailable.
 - b. Only when Mobile app is unavailable will the use of the participants landline to record the visit via Interactive Voice Response (IVR) be permitted; and
 - c. At a last resort, allow manual entry of visit information into the EVV system.
 - i. Must require authorized users to enter a DHHS approved reason for each modification or manual entry of verification data.
 - ii. In the instance where a visit is manually entered, the provider will be required to attest to the presence of hard copy documentation (i.e. timesheet).
6. **Must utilize unique sign in credentials for each user who accesses the system and retain information about any changes to electronically captured visit information.**
 - a. Only allow access to the system by properly credentialed users;
 - b. Only provider agency administrators will be allowed to manually edit visit data system of record/electronic log; and
 - c. Tracks all edits to data completed by administrators, recording user name and date/time stamp in an audit log.
7. **Be capable of retrieving current and archived data to produce reports of services delivered, tasks performed, participant identity, beginning and ending times of service, and date of services in summary fashion that constitute adequate documentation of services delivered. Any report shall include an explanation of codes utilized by the provider/vendor (i.e., Personal Care) and include the vendor/provider's identity by either name of vendor/provider and/or National Provider Identifier (NPI);**
8. **Maintain reliable backup and recovery processes that ensure that all data is preserved in event of a system malfunction or disaster. Data must be backed up, at a minimum, weekly, and retained for ten (10) years.**

9. Must support expansion of the DHHS EVV Program by allowing:

- a. Addition of potential future services;
- b. Addition of participants;
- c. Addition of tasks; and
- d. Addition of any requirements based on any applicable state or federal laws.

10. Providers and vendors shall:

- a. Accommodate more than one (1) participant and/or provider in the same home at the same phone number.
- b. Customize, collect, verify, document, and transmit specific provider services and visit tasks (i.e., bathing, meal assistance, etc.) delivered to each participant.

11. Verify components within the program requirements when the provider initiates visit verification and flag a visit for review when any required verification elements are missing, or if the recorded service location is not on a participant's list of approved locations.

12. Notify the provider if the visit data is incomplete or invalid when received.

13. Any training required for third-party EVV system functionality must be provided by the third-party EVV vendor. Tellus aggregator training will be provided by Tellus.

14. Third-party vendors must share client integration documents with Tellus.

15. Must meet published Tellus requirements in regards to integration messaging format, transport protocol, and security.

16. Is responsible for ensuring the quality of the data submitted to Tellus.

17. Must provision functionality for the monitoring and correction of any errors returned by Tellus, and a mechanism to resend corrected transactions.

18. Each third-party vendor will be required to electronically transmit EVV data to Tellus per Tellus' Third-Party Implementation Guide. A partial list of key requirements are as follows:

- a. Data format & layout to comply with Tellus Third-Party Integration Data Dictionary.
- b. Transmit data from all of your represented providers to a Tellus-hosted single SFTP directory or HTTPS end point.
- c. Manage error responses from Tellus, error resolution, and resubmission of failed transactions.
- d. Transmit at least visit created/scheduled and visit ended (completed, cancelled, etc.) status.
- e. Transmit changes in visit status within 60 minutes of change, 24x7.

19. Is able to electronically collect provider and participant authentication and confirmation of service delivery as part of EVV. Such confirmation will be delivered as part of the visit record to Tellus.

20. Must use only FIPS Pub 140-2-approved (or higher) encryption algorithms.

21. Must execute the Tellus Trading Partner Agreements, which includes a Non-Disclosure Agreement (NDA) and a Business Associate Agreement (BAA).

