PPR: 21 CFR Part 11

Paperless Process Recorder and Legendary™ Application Guide for FDA 21 CFR Part 11

Anderson-Negele Paperless Process Recorder (PPR) with Legendary™ software is designed to meet the requirements of 21 CFR Part 11 application, however the responsibility to implement the equipment properly and validate the system remains with the Client. The blue text of this document explains how the Paperless Process Recorder (PPR) and Legendary™ cloud software meets the requirements of this Code of Federal Regulation.

Part 11 - ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

All following gray Sub-parts are included in part 11

Subpart A - General Provisions

Sec. 11.3 – Definitions (4) Closed System:

Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

The PPR and Legendary™ software constitute a closed system as the Client is responsible for appointing and maintaining an active Legendary™ Administrator. The Client's Legendary™ Administrator is responsible for managing and controlling access to the systems.

Subpart B - Electronic Records

Sec. 11.10 – Controls for closed systems:

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

Creation, maintenance, and transmission of electronic records is automatically handled by PPR and Legendary™.

PPR's data storage scheme securely stores the database used to generate chart images within PPR's internal memory. The Internal memory is not directly accessible to customers and thus may not be overwritten or modified. The PPR's internal database is password protected, requiring Anderson-Negele software developer credentials to view or edit the database. These credentials and the source code within the system are considered Intellectual Property and will not be shared with Clients.

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Validation by end-user or a third party acting on behalf of the end-user may be required.

Validation of recorder accuracy performance by the Client, Inspectors or 3rd party may be required upon commissioning, and periodically thereafter.

Records viewed directly through Legendary™ or the PPR can only be created, revised and uploaded by PPR, thus are unalterable. Supporting documents can be uploaded by Legendary™ users in a designated location but Legal records cannot be added, edited, or deleted by the Legendary™ software user.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

At the end of each record period and upon updates to a record e.g., adding information, the PPR will automatically generate an image file of the record data in human readable format. All record image revisions generated by the PPR are automatically synced to the Legendary™ software when connected.

Records can be downloaded and printed at will by Clients.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Record images cannot be altered in either the PPR or Legendary™ software. Record images are backed up within the PPR for a minimum of 2 years. Process data and annotations are stored on the PPR for up to 7 years.

For redundancy the removable microSD storage contains the last 100 days of the latest revision of each PPR Record Image, as well as the last 100 days of 24-hour backup records.
Each version of all record images created by any PPR are available indefinitely in the Legendary™ software to authorized users.

(d) Limiting system access to authorized individuals.

Any annotation or information added to a PPR record by an individual requires user identification and authentication with PIN. Only authorized users can make configuration and calibration changes to the PPR.

Physical jumpers and tamper evident sealing covers are available to physically restrict configuration and calibration changes.

PPR access and Legendary™ user access is limited to users configured and maintained by the Clients' System Administrator.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

All annotations are recorded with operator initials, along with the date and time when they were created or edited. A log of all annotation details is automatically created for annotations added from Legendary™ within the record page.

Records cannot be deleted by any Legendary™ user nor directly through the PPR user interface.

All configuration and calibration changes are automatically logged by the system and available in the System Activity log via PPR or Legendary™.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

No specific sequence required during normal operation of PPR, but each annotation and system changes are allowed only after entering correct credentials and may be dependent on J9 jumper position.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

The Client bears responsibility for establishing and maintaining and executing system authority checks. The Clients' Legendary™ Administrator is capable of granting & restricting user access to the PPR, Legendary™ and various permission levels within the system.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

The PPR has built-in broken sensor and over- and under-range detection.

Internal communication protocol validates each communication between input cards and central processing system.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Anderson-Negele has published the required documentation to train PPR and Legendary™ users and Administrators. Such documentation can be found here.

The Client is responsible for creating and executing the applicable training programs for their team.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

The Client is responsible for creating and executing the applicable policies with their team of users.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

The documentation including instructions on installation, configuration, operation and administration of PPR and Legendary™ are available here. The operating manuals are subject Anderson-Negele's change control process.

Sec. 11.10 – Controls for closed systems:

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;
(2) The date and time when the signature was executed; and
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

When an approval (signature) is added to a PPR record, the PPR will regenerate the record image to include the full name of the user who signed the record, date and time the action was executed, and responsibility of the user as defined by the responsible group in the record approval workflow.

When annotations are added to a PPR record the unique initials of the user who added the annotation will automatically be added to the annotation entry text along with the time and date the annotation was added.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout)

All information defined above is included in the record image regardless of how that image is viewed, e.g., at the PPR, online, or printed out.

Sec. 11.70 – Signature/record linking:

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

PPR & Legendary™ does not support handwritten signatures at this time.

The electronic signature added to a record is simply the user's first and last name, along with their role (when approving a record image). Users are required to provide credentials with PIN or Password authentication before a signature can be added to a record. There is no way for a user to remove a signature from a record revision previously generated by the PPR.

Subpart C - Electronic Signatures

Sec. 11.100 – General Requirements

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

When setting up users in Legendary™ the system requires each user to have a unique username and Initials. The Client is responsible for developing, executing, and maintaining procedures to ensure that credentials are not shared amongst their team members.

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

The Clients' Legendary™ Administrator is responsible for verifying the identity of all users in their system during the user creation process.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

The Client is responsible for this requirement when applicable.

Sec. 11.200 – Electronic signature components and controls

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

When using the PPR, a user is required to select their name from the user list and enter their PIN for every signature.

When using the Legendary™, a user is required to enter their Username and their Password to gain access to the system before signing any records. The user will not be required to re-authenticate if subsequent actions are continuously performed within 60 minutes.

(2) Be used only by their genuine owners; and

The Client is responsible for developing, executing, and maintaining procedures to ensure that credentials are not shared amongst their team members.

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals

Users with the Legendary™ Administrator role are not capable of signing as an approver in the PPR/Legendary™ record approval workflow. Users with non-Administrator Legendary™ Roles are not capable of user administration, thus the collaboration two individuals (with Administrator and non-Administrator roles) would be required to falsely sign any PPR records.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

The PPR and Legendary™ do not support biometric identification at this time.

Sec. 11.300 – Controls for identification codes/passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

User access to PPR and Legendary™ are controlled by Usernames, not user codes. These requirements are not applicable.