Priority Tools for Compliance with FDA Title 21 Code of Federal Regulations Part 11

Introduction

FDA Title 21 CFR Part 11, which deals with electronic records and electronic signatures, requires an audit of the ERP system used by the audited company. The certification process audits the company itself, and how it employs the software; it does not certify the software directly.

This document serves to outline the various tools available in ***Priority*** to enable compliance with components of CFR Part 11 that must be addressed by the ERP platform.

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:

Requirement	Comments
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Priority has built in tools for validating data entered by users, that the customer can employ to assure only valid data is entered into the system. Priority Software's QA process has thoroughly verified that creation and modification of data is accurately captured in the system. Priority has multiple checks and self-tests that ensure that partial records are not committed to the database, and that data integrity is maintained. All data are protected to prevent unauthorized access and alteration.
(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.	***Priority*** stores data in a relational database in electronic form, and can easily be viewed through the ***Priority*** interface. ***Priority*** offers a number of ways to view and export record data,: • In addition to displaying data in the graphical user interface, electronic records include programs for creating customizable printouts and reports. • There are several report generators that allow users to create reports based on data in relevant electronic records. • Data can also be exported from a record into other formats.

	Only authorized users can use the data export features.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	All records created in ***Priority*** are stored securely in a database. ***Priority*** supports automated backup of all records in the system. Restoring data from backup is simple, by use of a dedicated program that restores both data and configuration settings.
(d) Limiting system access to authorized individuals.	Users can only access the system using their unique username and password. Passwords are stored and secured in the database in encrypted form, further securing the system. Additionally, organizations can elect to implement external identity management using identity provider services over the OAuth2 standard (such as Google, Microsoft, Okta, etc.). This allows for additional layers of verification used by the identity provider, such as two factor authentication (2FA).
(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.	Records include a change log that tracks modifications (add, delete, modify) and a log of statuses that provides an audit trail of the users who changed the status of the document (e.g. approved a transaction). Each log contains a computer generated timestamp with the user that made the change. All logs are built into the system and cannot be tampered with. These logs are available for review at all times. The logs can be backed up in the same way other data is backed up.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	All documents in Priority are manageable through a graphical business process management (BPM) interface. The customer can define the flow of the process and the users that may advance the process, including conditions that must be fulfilled before progressing to the next stage. Furthermore, for all records, the customer can define additional warning and error messages that will appear when certain conditions are met. The customer is responsible for maintaining the process and ensuring that it meets all requirements.
(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.	***Priority*** requires users to login with a unique username and password. The customer may choose to configure password complexity and duration to ensure passwords are changed on a regular basis. Accounts can be disabled by the administrator. Additionally, organizations can elect to implement external identity management using identity provider services over the OAuth2 standard (such as Google, Microsoft, Okta, etc.). This allows for additional layers of verification used by the identity provider, such as two factor authentication (2FA). ***Priority***'s privilege management enables highly granular control over what actions a user can perform. Each user can be assigned permissions on an individual basis, or they can be assigned a user group based on skill set, that determines their permissions.

	Permissions can be assigned separately for each feature in the system, down to read/write permissions for individual fields, protecting data from unauthorized access or modification. Users can only update/modify/ delete records based on these permissions. Additional security checks can be added by system administrators to prompt the user to enter a password when attempting to update a certain field. This will prevent a user from updating data on another user's computer.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	**Priority** is a web-based software solution that can be distributed via the customer's corporate Intranet. After it is installed, external access by devices must be controlled through firewall and VPN administration. Access to **Priority** may be opened up to third parties that are part of an extended secure network controlled by the customer.
(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.	**Priority's** privilege management tool enforces that only users with specific roles may perform certain actions. Also, business rules can be set up to further restrict actions to specific users. In the HR module, it is possible to maintain employee's training and certification. Generally, it is the customer's responsibility to ensure that their employees are qualified to perform their tasks.
(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.	This is a procedural requirement relevant to customers and is not related to functionality in **Priority**.
(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.	Priority Software provides official documentation for operation and maintenance of **Priority**, which the customer can then distribute among the appropriate employees. Priority Software's official documentation is version controlled, and changes are recorded. It is the customer's responsibility to ensure that official documentation is distributed to their personnel and is accessible to authorized individuals. They are also responsible to maintain and distribute private documentation for their own internal processes.

11.30 – Controls for open systems.
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 1'1.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Priority is a closed system. Access to **Priority** is permitted to authorized users only.

11.50 - Signature manifestations.

Requirement	Comments
(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. (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).	Each modification by a user will automatically generate a signature consisting of the username (which links to the full name of the user), and the date and time in which it was carried out. These items are a part of the record and can be included in the printout or display of the record.

11.70 - Signature/record linking.

Requirement	Comments
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.	The electronic signature is comprised of username and password. Each record that is modified contains documentation of the username. This data is computer generated and read only, therefore cannot be changed or copied in any manner. User passwords are maintained in **Priority** in an encrypted format to protect from unauthorized use.

11.100 – General Requirements.

Requirement	Comments
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Users can only access the system using their unique username and password. **Priority** enforces the uniqueness of each username in the system. Even when a username is deactivated, a user account with the same username cannot be created. Additionally, organizations can elect to implement external identity management using identity provider services over the OAuth2 standard (such as Google, Microsoft, Okta, etc.). This allows for additional layers

	of verification used by the identity provider, such as two factor authentication (2FA).
(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.	This is a procedural requirement relevant to customers and is not related to functionality in **Priority**.
(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.	This is a procedural requirement relevant to customers and is not related to functionality in **Priority**.

11.200 - Electronic signature components and controls.

Requirement	Comments
(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.	Users can only access the system using their unique username and password. Additionally, organizations can elect to implement external identity management using identity provider services over the OAuth2 standard (such as Google, Microsoft, Okta, etc.). This allows for additional layers of verification used by the identity provider, such as two factor authentication (2FA).
(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	A unique username and password are both required for the first log in to the system. In addition, the system can be configured to automatically log users out of the system if they have been idle for a certain period of time (timeout). Users will be required to re-enter their credentials to log back in (username and password). Every system function executed after the first sign in is recorded with the individual’s username.

executable by, and designed to be used only by, the individual.	Additional security checks can be added by system administrators to prompt the user to enter a password when attempting to update a certain field. This will prevent a user from updating data on another user's computer.
(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.	Users are required to enter both a username and password each time a new session is initiated.
(2) Be used only by their genuine owners; and	This is a procedural requirement relevant to customers and is not related to functionality in **Priority**.
(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.	Only the genuine owner of a username and password can use the electronic signature associated with that user. The customer can set in place procedures that ensure that if a system administrator is going to perform actions that might infringe on the authenticity of the signature (by resetting an electronic signature or logging in as another user), such actions must be with the oversight of another individual.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	***Priority*** does not support electronic signatures based on biometrics, and as such the requirement pertaining to them is not applicable.

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:

Requirement	Comments
(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.	Priority enforces the uniqueness of each username in the system. Even when a username is deactivated, a user account with the same username cannot be created. If external identity management is used, this requirement will pertain to the identity provider instead of Priority.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The system manager can set a password policy for the system, requiring users to change their password after a certain period of time has elapsed. The manager can also specify complexity and length requirements for new passwords. If external identity management is used, this requirement will pertain to the identity provider instead of Priority.
(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	If the administrator suspects a certain user account has been compromised, said account can easily be deactivated, automatically revoking all permissions in the system.

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.	***Priority*** can be configured to lock out a certain username from logging into the system if too many failed attempts to log in with that account are made. If external identity management is used, this requirement will pertain to the identity provider instead of Priority. Several tools are available for the system administrator to review actions performed by users within the system. If the administrator suspects a certain user account has been compromised, said account can easily be deactivated, automatically revoking all permissions in the system.
(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.	This is a procedural requirement relevant to customers and is not related to functionality in **Priority**.

Summary

For over 30 years, ***Priority*** has supported manufacturing and industry, including in regulated industries. ***Priority*** offers a core set of features that allow compliance with the guidelines of FDA Title 21 CFR Part 11, including security, process and privilege management, electronic signatures, logging and auditing.