Ennov and FDA 21 CFR Part 11

MKG.LB.0299.000
Application date: 20/03/2019

An Ennov white paper

Summary:

The 21CFR Part 11[1] is a set of regulatory requirements issued by the FDA[2] in order to specify the conditions to be met by an organization willing to comply with the FDA standards concerning management of records and electronic signatures. Management of data has to follow these requirements so that electronic records (resp.) electronic signatures are considered to be equivalent as paper records (resp. handwritten signatures on paper). The 21CFR Part 21CFR11 was published in 1997; since there were different ways to understand it, several guidelines were published afterwards[3], but do not offer a complete clarification yet.

The Ennov software suite includes native features that facilitate management of records and secured signatures. The system implementation is then based on configuration with no need to perform development.

This document lists the 21CFR Part 11 requirements and presents how Ennov understands their impact on its software and how it complies with them.

All our products are designed, developed and validated in order to be 21CFR Part 11 compliant. However, the client has to make sure the software implementation follows appropriate procedures and methods. Ennov delivers all the software documentation (both technical and functional) and can also provide a complete validation kit detailing all the tests related to the different qualification phases.

About Ennov:

Ennov is a software vendor specialized in document and business process management solutions for the life sciences industry. We focus on four product lines: Quality, Regulatory Affairs Clinical Trials and Pharmacovigilance. Our primary concern is to deliver a highly configurable system that improves operational performance in compliance with regulatory standards. No training is required for end-users; this guarantees a quick return on investment and a strong satisfaction level. Our clients include large corporations, especially in the medical / pharmaceutical sector. Ennov is ISO 9001:2015 certified by SGS for all its operational processes, and regularly audited by clients.

Confidentiality Statement:

This document is strictly confidential; it is communicated to Ennov clients and/or persons directly in charge of validating the Ennov software solution. Communication to any third party is forbidden.

---

1 "Code of Federal Regulation", Part 11 of Title 21, named: "Electronic Records; Electronic Signatures".

2 Food and Drug Administration

3 The latest guideline (*Guidance for Industry – Part 11: Electronic Records; Electronic Signatures – Scope and Application*) was issued in August 2003.

1 Definitions

These definitions are those provided by the FDA.

(1) **Act** means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) **Agency** means the Food and Drug Administration.

(3) **Biometrics** means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) **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.

(5) **Digital signature** means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) **Electronic record** means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) **Electronic signature** means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) **Handwritten signature** means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) **Open system** means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

2 Application scope of the 21CFR Part 11

2.1 Records concerned

The 21CFR Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted to the FDA.

It does not apply to paper records that are, or have been, transmitted by electronic means (for example by fax).

2.2 Acceptance criteria

If electronic records and electronic signatures comply with the 21CFR Part 11 standard, the FDA considers they are equivalent to paper records and handwritten signatures on paper.

The FDA accepts electronic records that comply with the 21CFR Part 11, unless a paper version is explicitly required.

Hardware, software, data, controls and system documentation have to be available for an FDA inspection.

Note: considering the definitions provided by the FDA (presented above), Ennov is a closed system.

---

3 General principles of Ennov implementation

3.1 Electronic signature

Prior to each signature, Ennov requires entering again the personal login and password.

The following information is saved at the time of signature:

- the complete name of the signatory,
- the identification of the signed record,
- the meaning of the signature (workflow step label),
- the date and hour.

The legal name or complete name, the date / hour and the meaning of the signature can be displayed on all visible forms of the record.

The time-stamping (local and GMT) displays: the year in four digits; the month; the day; the hour, minutes and seconds.

The meaning of a signature corresponds to a workflow step label.

3.2 Workflow management

Ennov includes a workflow engine that controls the sequencing of predefined tasks for each process. Workflow steps, deadlines and responsibilities are configured in the system based on the rules you define. Then, data entry or modification is possible only by authorized persons at each workflow step.

3.3 Traceability

Ennov guarantees all data are saved and stored according to the specifications of the entity that implements the software. The administrator defines which information can be modified at each workflow step for active records, and the archival duration for closed records. These features are standard in Ennov.

The additional Ennov 21CFR Part 11 module provides an audit trail that logs in a separate database all modifications performed in the main database. The audit trail records the following information:

- nature of the modification (previous value / new value / reference number of concerned record),
- date and hour (local / GMT),
- first name / family name of the user.

4 Detailed analysis: electronic records and electronic signatures

This chapter specifies for each item how Ennov responds to the FDA requirement concerning electronic records and electronic signatures, as stated in the 21CFR Part 11.

Note: in the following table, you will find the following information:

- **in the first column, the text of the FDA requirement in the 21CFR Part 11**

- **in the second column, indication of the responsibility to meet the requirement:**
  - **'P' stands for "Procedure"**
  - **'S' stands for "System"**
- **in the third column, how Ennov understands the requirement**
- **in the fourth column, a short description of the Ennov features that meet the requirement**
- **in the fifth column, indication of the compliance level:**
  - **'Y' stands for "compliant"**
  - **'N' stands for "not compliant"**

'N/A' stands for "not applicable".

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
B-11.10.a - Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	PS	The system has to detect invalid or altered records.	Management rules are implemented in the Ennov set up to control the validity of all records (for example: if a mandatory field is missing, an error message will be displayed). Ennov relies on a relational database (such as Oracle or MS SQL Server) where all data, metadata and configuration elements are secured. This prevents any alteration of the electronic records.	Y
B-11.10.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	S	Records have to be available: - either on the screen - or in paper format - or in electronic format, via an export delivered to the FDA auditor. FDA accepts records in PDF format.	Ennov enables: - to search records and export them in CSV or XML format - to generate regulatory reports in PDF or XML format	Y

[4] Responsibility = (P)rocedure or (S)ystem

[5] Compliant

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
B-11.10.c - Protection of records to enable their accurate and ready retrieval throughout the records retention period.	PS	Records have to be protected during the legal retention period.	Records are stored in a database hosted on a secured server, for which a back-up is performed regularly according to the corporate procedures. No records can be destroyed during the local retention period.	Y
B-11.10.d - Limiting system access to authorized individuals	PS	The system has to prevent access of non authorized persons.	Ennov relies on the authentication mechanism of the corporate information system (NTLM, LDAP, Kerberos, SSO…). Within the application, access level is determined by the Ennov profile management utility. Each Ennov user has to be declared in the address book and cannot connect to the system unless the authentication is validated. The format and validity rules of passwords are those defined in the corporate information system. Ennov logs failed connection attempts and blocks the user account after a configurable number of authentication failures. User profiles are clearly defined in Ennov configuration utilities and can be audited when needed by an external expert. Ennov is a Web-based application. A session time-out is implemented so that after a	Y

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
			configurable duration with no activity in the system, a new authentication is necessary.	
B-11.10.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.	S	There is a need for a time-stamped audit trail recording all actions performed by users that have an impact on the stored data. An audit trail is a mechanism that stores the detail of all operations performed in the database. The system has to include an audit trail feature for each GMP[6] record and each action performed by the operator. This audit trail has to be stored for the same duration as the records it relates to. The audit trail has to be available for audits by the agency.	The Ennov audit trail displays the name of the user who performed the action, an accurate description of the action, the motive (i.e. the workflow step), the date and hour (both local and GMT). Once a line has been added to the audit trail, it cannot be modified nor deleted. The audit trail is created in incremental mode, following the chronological order. A new audit trail entry cannot crush existing information. System events that are recorded in the audit trail are the following: - Creation of a record, - Modification of a record (in this case values before and after the modification are traced), - Deletion of a record. It is possible to search the audit trail in order to provide the accurate information needed	Y

6 Good Manufacturing Practices

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
			by the agency. They can be exported in CSV and XML formats. The audit trail information is included in the regular back-ups since it is stored in the same database as the live data.	
B-11.10.f - Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	PS	The system has to control (when it is relevant) the correct sequencing of steps or operations (i.e. the workflow).	This is a standard Ennov feature: workflows are defined in the system as sequences of steps; Each step has to be processed by a person or a group of persons (designated based on rules set in the configuration utilities).	Y
B-11.10.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.	PS	The company has to control authorized interventions on the records (creation, modification, deletion). Direct access to stored data has to be controlled, as well as direct interventions on the supervised process.	Only authorized persons can enter the system (after going through the authentication process). Access level is determined by the user profile. Access rights definition is handled in Ennov configuration utilities (administrators set up authorizations for each action in the system).	Y
B-11.10.h - Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	PS	All actions have to be secured and traced, with supervision mechanisms for each process. Each action can be performed by authorized persons only. Some of these actions have to be checked or validated by other authorized persons. All this is recorded in an audit trail (see B-11.10.e).	Ennov can determine: - the origin of a data entry (name of the issuer), - the origin of an operational instruction (traceability of the process). Failed connection attempts are logged. The user account is blocked after a configurable	Y

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
		Besides, it is necessary to log failed connection attempts by non authorized users.	number of authentication failures. A notification email is then sent to the administrator. Only the administrator can unlock the account.	
B-11.10.i - Determination that persons who develop, maintain, or use electronic record systems have the education, training, and experience to perform their assigned tasks.	P	The persons who develop / maintain / use the Ennov software have to follow an initial training and then regular refresher training sessions while gaining experience to perform their tasks in the most professional way.	The Ennov personnel is trained and experienced for all the missions related to the software development and implementation at clients. Ennov is regularly audited by clients. The company is ISO 9001:2015 certified for all its operational processes, including the entire product lifecycle. Ennov transfers knowledge on its products to the clients (both for using/configuring and operating each software module).	Y
B-11.10.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.	PS	The company has to implement written guidelines and make sure employees are aware of their responsibility for all actions performed under electronic signature, which will discourage any misuse and falsification.	Ennov enables to define a session time-out (the duration is configurable). Signing a document electronically is possible only if the user knows his/her personal login and password. The rules concerning password format and validity are implemented in the corporate authentication system.	Y
B-11.10.k - Use of appropriate controls over systems documentation including:		The documentation of the system has to be controlled.		

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	P	Distribution and access to the system documentation have to be controlled.	The reference guide is delivered in PDF format and accessible to all Ennov users. It includes a complete description of the system features (both for users and administrators) illustrated by screenshots. Additional documentation is delivered to selected persons concerning the system operation and maintenance.	Y
(2) - Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	P	The system documentation is written and updated according to procedures that include an audit trail.	The Ennov quality system is regularly audited by clients. The company is ISO 9001:2015 certified for all its operational processes, including activities related to the software documentation.	Y
B-11.30 - 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 § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary	S	Access to open systems has to include additional security mechanisms such as encryption or digital signature.	In this case, additional controls can be implemented as options: - an encryption system during all the working session - a strong authentication relying on a certificate.	Y

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
under the circumstances, record authenticity, integrity, and confidentiality.				
B-11.50.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.	S	Signed electronic records have to display the legal name or the complete name of each signatory, the date and hour of the signature and its meaning.	The time-stamping (local and GMT) displays the year in four digits, the month, the day, the hour, the seconds. The meaning is the label of the workflow step (as defined in Ennov). The complete name of the signatory is displayed in the signature.	Y
B-11.50.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).	S	The information mentioned in requirement 11.50.a. has to be considered as an integral part of the electronic record and displayed in all readable forms of the record.	This information can be consulted, printed and exported with the other data of the record. In Ennov, the configuration of the workflow enables to prevent the modification of any signed data.	Y
B-11.70 - 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	S	The link between the signature and the record it refers to cannot be broken.	The signature contains the identification of the signed record and the date of the signature. It cannot be dissociated from the concerned record. When printing signed records through the system, the printed documents contain all the information that enables to determine with certainty which	Y

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
			electronic records are concerned by the signature.	
C-11.100 a - Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	S	A signature has to be: - personal, - unique for each person in the system at any moment, - non reusable, - non transferrable.	Management of passwords relies on the corporate authentication system (passwords are not defined in the Ennov software).	Y
C-11.100 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.	P	The identity of the persons using electronic signatures has to be checked.	This requirement concerns the trusted certificate authority that delivers digital keys.	N/A
C-11.100 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.	P	Users have to confirm they consider their electronic signature is equivalent to their handwritten signature in a letter sent to the FDA.	This requirement concerns the client.	N/A

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
(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.				
C-11.200 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. (2) Be used only by their genuine owners; and	S	For non biometric signatures, the system includes at least two distinct identification components (such as a login and a password) to control electronic signatures. When an authorized user performs a series of signatures during an interrupted period of controlled activity in the system, only one component of the electronic signature is required, provided the first signature was validated with both components. The security level has to make it impossible to sign when you are not authorized, unless the authorized person communicated his/her password to you. The company has to guarantee the identity of the persons capable to sign electronically through the system.	Signatories have to be registered in the Ennov internal address book. Each user has a personal login to connect to Ennov, while the password is managed in the corporate authentication system. In case several records are signed by the same user during an interrupted period of controlled activity in the system, Ennov requires entering both identification components for each signature (i.e. the login and the password). The right to sign electronically is configured by the administrator for each user profile.	Y

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
(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.				
C-11.200 b Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	PS	The system has to be designed to guarantee that electronic signatures relying on biometrics cannot be used by any person apart from their owners.	This requirement concerns the biometric identification system interfaced with Ennov.	N/A
C-11.300 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:				
C-11.300 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.	S	The system has to guarantee each login / password combination is unique.	Management of passwords is not handled within Ennov; it relies on the authentication mechanism of the corporate information system.	N/A
C-11.300 b - Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	PS	Management of passwords controlling electronic signatures has to respect the criteria specified in the client's procedure in terms of format, validity duration and renewal.	Management of passwords is not handled within Ennov; it relies on the authentication mechanism of the corporate information system.	N/A

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
C-11.300 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.	PS	The system has to include the possibility to deactivate temporarily or definitely the identification process in place (card or token) in case of loss. It has to be possible to replace a card or a token (if it has been lost). The system administrator can revoke a signature.	This requirement concerns digital signatures using cards, tokens or biometric systems.	N/A
C-11.300 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.	S	The system has to detect and log unauthorized attempts to use electronic signatures.	Ennov logs unsuccessful signature attempts, including the name of the user and the date/hour. Three unsuccessful attempts deactivate the possibility to sign records in the system (this number is configurable). Only the administrator can unlock the account so that it can sign again. The system enables to display the log information detailing signature attempts. An automatic notification is sent to the administrator in case failed electronic signature attempts are detected repeatedly.	S
C-11.300 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	P	The equipments that enable to generate identification codes or passwords have to be tested periodically.	This is controlled through procedures that have to be implemented by the client: - a validation of the system is performed when activating a card or a token	N/A

21CFR part 11 requirement	R[4]	Ennov understanding	Ennov feature	C[5]
properly and have not been altered in an unauthorized manner.			- a validation of the system is performed at least once a year for cards or tokens	

Ennov US

Phone: **+1 (833) 366-6887**
Mail: contact-us@ennov.com

- **Ennov California**
  75 E W Santa Clara St. – suite 700
  San Jose, CA 95113, USA

- **Ennov North Carolina**
  223 S West St. – suite 1000
  Raleigh, NC 27603, USA

- **Ennov Missouri**
  518 Felix St.
  St Joseph, MO 64501, USA

Ennov Europe

Mail: contact@ennov.com

- **Ennov France (headquarter)**
  251 rue du Faubourg Saint Martin
  75010 Paris, France
  Phone: **+33 (0)1 40 38 81 38**

- **Ennov UK**
  5 Eaton Court Road, Colmworth Business Park
  Eaton Socon St Neots Cambridgeshire PE19 8ER – UK
  Phone: **+ 44 1 480 21 22 23**