Pharma Biotech

CHAUVIN ARNOUX
INDATECH

Indatech's softwares and the 21 CFR Part 11 standard

- Overview
- What is 21 CFR Part 11?
- Advantages of 21 CFR Part 11
- Compatibility of INDATECH's software with 21 CFR Part 11

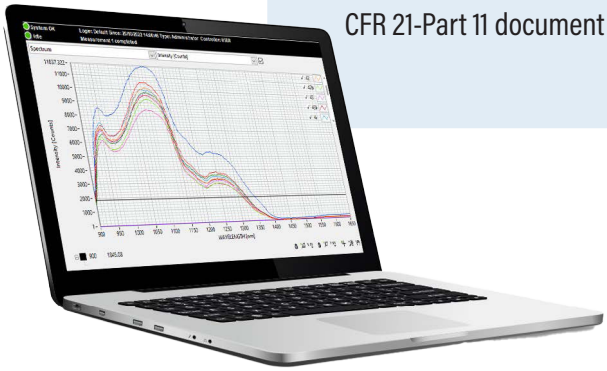
Measure up

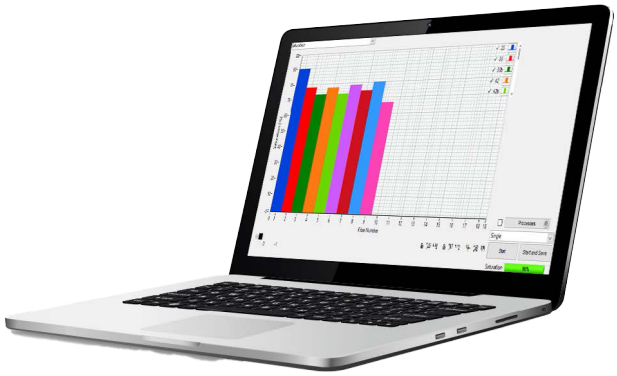
Overview

INDATECH's software solutions provide special features that allow customers to address the technical requirements of Title 21, Part 11 of the Code of Federal Regulations. This document describes the implemented features and how they should be used by customers in order to comply with the CFR 21-Part 11 regulations.

It is important to note that CFR 21-Part 11 states that it is not the equipment manufacturer's sole responsibility to meet the requirements. The entire manufacturing, inspection and record maintenance process must be validated according to the customer's standard operating procedures (SOPs) to comply with the regulations.

CFR 21-Part 11 document quotes are in *italics.*





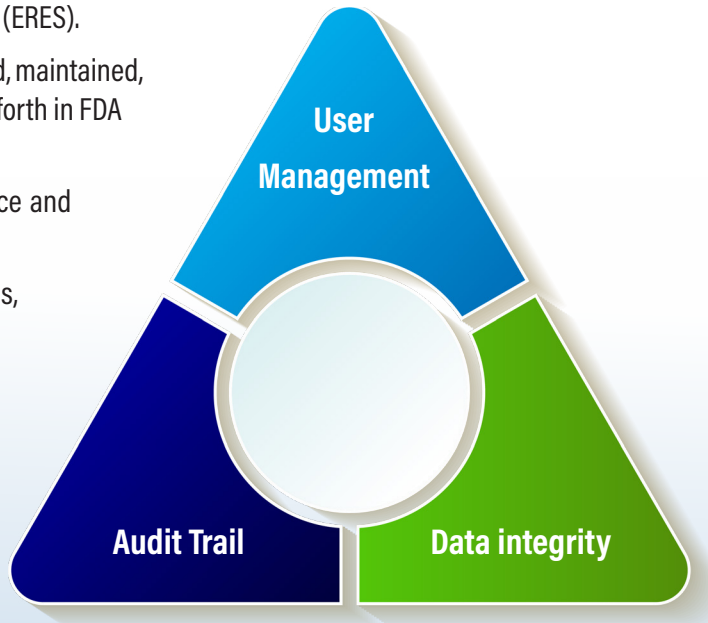
What is 21 CFR Part 11?

The United States Food and Drug Administration (FDA) 21 CFR Part 11 defines standards for the use of secure, reliable electronic records and electronic signatures (ERES).

The rule applies to records in electronic form which are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations.

All requirements under 21 CFR Part 11 are mandatory for medical device and pharmaceutical companies.

Indatech's Document Management System offers audit trail functions, reports, collaboration and approval for SOPs to assist your organization in meeting compliance standards.



▪ Advantages of 21 CFR Part 11

1. System Validation

▪ The main purpose of 21 CFR Part 11 is to ensure that your system is validated. The Indatech software provides a 21 CFR Part 11 compliant installation qualification (IQ) protocol and completed operational qualification (OQ) and performance qualification (PQ) reports.

▪ To better understand IQ, OQ, PQ, think of each by asking these questions:

- ▪ IQ: Is the software correctly installed?
- ▪ OQ: Is the software operating as expected, and do users understand its limits?
- ▪ PQ: Does the software reliably produce the correct result?

2. Full Data Security

▪ With a 21 CFR Part 11 compliant Indatech solution, you can ensure a better level of safety, protection, and integrity for the facts and data you keep and proportion on a daily basis.

3. Audit Trail

▪ Indatech's software incorporates an audit trail solution enabling organizations to meet FDA 21 CFR Part 11 requirements for the action log. Actions in the software automatically produce a log of the operation with timestamp, user information and values. This information is stored in an audit trail database and will not be deleted under any circumstances.

4. Data Integrity

▪ To maintain the reliability and credibility of the generated data throughout their life cycle, a checksum is added to the data file to detect errors in the transmission of data over time (on a data carrier) or in space (telecommunications). To detect errors, it is sufficient to perform the same operation on the data and compare the result with the original checksum.

5. Electronic record storage

▪ A non-editable file format can be generated and saved for all electronic records that can be signed.

▪ Indatech software comes with a broad range of key reports and quality metrics providing the capability to create custom reports which can be printed on paper or downloaded in electronic format.

▪ Electronic records are stored on the local hard drive of the PC running the software, using a specifically designed binary file format. INDATECH software allow users and reviewers to view the content of data files through a straightforward, configurable interface.

6. Authenticated signatures and control of user authorization

▪ Software is designed with security in mind, requiring a unique user name and password to gain access.

▪ Different modules and functions are controlled with a combination of roles and rights.

▪ Users and privileges are defined and managed by system administrators. An inactivity lock secures the program after a period of inactivity.

7. Version Control

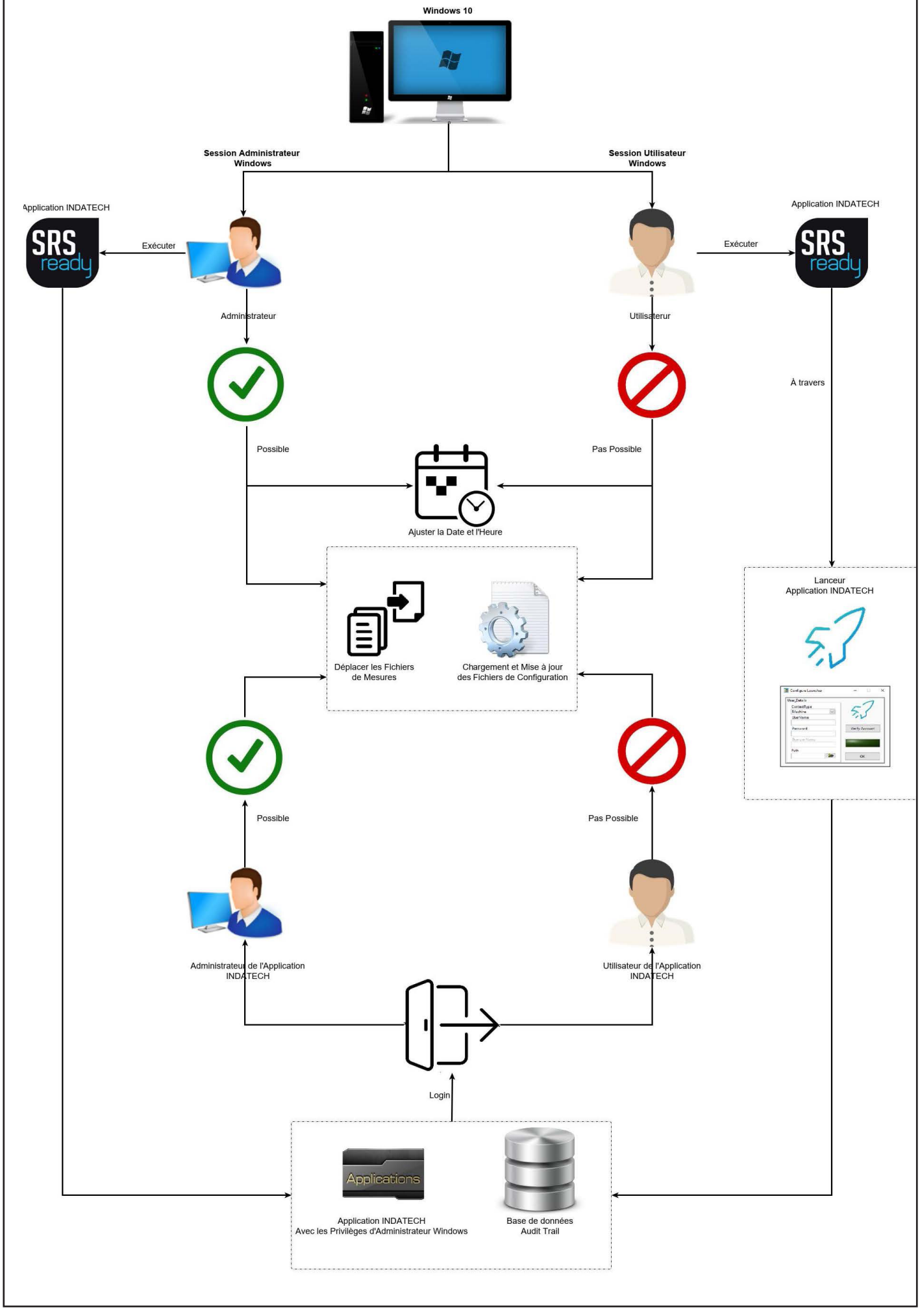
▪ INDATECH provides complete, version-controlled user documentation for the software. INDATECH also adheres to a quality management and change control system, and the system is fully documented. This includes software releases and documentation version traceability.

▪ All documents and their metadata, including previous versions, can be retrieved easily as the software stores all versions of all files without deleting or removing previous versions.

8. Closed system

▪ INDATECH's software solutions are designed as a closed system which can only be operated by authorized personnel

- ▪ Access Control to the system (Login and password)
- ▪ Electronic Records (File integrity)
- ▪ Audit Trail (Change and system history)


Windows 10
Session Administrateur Windows
Session Utilisateur Windows
Application INDATECH
Exécuter
Administrateur
Utilisateur
Application INDATECH
Exécuter
À travers
Possible
Pas Possible
Ajuster la Date et l'Heure
Déplacer les Fichiers de Mesures
Chargement et Mise à jour des Fichiers de Configuration
Lanceur Application INDATECH
Possible
Pas Possible
Administrateur de l'Application INDATECH
Utilisateur de l'Application INDATECH
Login
Applications
Application INDATECH
Avec les Privilèges d'Administrateur Windows
Base de données
Audit Trail

Compatibility of INDATECH's software with 21 CFR Part 11

Requirements	Solution
General provisions	
Sec. 11.3 Definitions	
(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. *(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.* *(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.*	INDATECH's software solutions are designed as a closed system, which can only be operated by authorized personnel *"who are responsible for the content of electronic records"*. Consequently, INDATECH's software meets the requirements of Section 11.3 of this document.
Electronic records	
Sec. 11.10 Controls for closed systems	
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	INDATECH's activities are compliant with the ISO 9001 requirements. The scope of certification covers the use of software development good practices and related documentation. INDATECH's software has been tested and validated according to a set of pre-defined, verifiable specifications. Customers are responsible for using our software in accordance with the provided user manual and documentation. Proper calibration procedures must be included systematically in the customer's SOPs. However, INDATECH's software solutions help users to perform a sequence of system verifications before any electronic data can be recorded (hardware checking, calibration checking, calibration procedure if necessary) ensuring measured data accuracy and reliability. INDATECH's software solutions also manage calibration scheduling and warn users before calibration data is out of date. If a single step in the verification process fails, no measurements can be performed by the software, thus preventing customers from measuring erroneous data. INDATECH's software solutions systematically verify that electronic records (data files) have not been altered by using a checksum algorithm. If a corrupted file is detected upon opening, users are informed which part of the data is not correct. The uncorrupted part of data can still be edited inside the software.

(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.	Electronic records are stored on the local hard drive of the PC running the software using a specifically designed binary file format. INDATECH's software solutions allow users and reviewers to view the content of data files through a straightforward, configurable interface. We strongly advise customers to set up a backup copy mechanism for INDATECH binary files. If any electronic record is altered during the copy process, it will be detected by our software at opening using a checksum algorithm.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	It is the customer's responsibility to ensure that its IT architecture can protect and store the recorded files.
(d) Limiting system access to authorized individuals.	INDATECH's software is accessible through a logon module at startup. Unique user ID and password combinations are associated with access levels for each authorized user. Users and privileges are defined and managed by system administrators. An inactivity lock secures the program after a period of inactivity.
(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.	Time-stamped audit trails of user actions are recorded into the same binary file as electronic records. Log data includes: ▪ Date and time ▪ User name and access level ▪ Description of the action(s) Security related data and actions, such as user login, electronic record saving or updating and system errors, are systematically logged in audit trails. Raw measurement data cannot be modified within INDATECH's software; only analysis and post-processed data may be updated. These updates are also logged in audit trails. Audit trails cannot be modified but only completed within the INDATECH software. Furthermore, logged data are protected from direct modification since they are encapsulated in a binary file. Any alteration of binary data files by direct access will be detected using a checksum algorithm. Finally, audit trails may be exported in PDF format for review purposes.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	INDATECH's software solutions preserve the data workflow through a pre-defined sequence of operations (hardware verification, calibration, measurement, data recording and display...). Data validity and integrity are checked automatically before and after each operation.
(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.	Multiple levels of security allow different parts of INDATECH software to be seen or updated by users with the appropriate credentials.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Devices connected to the PC running the system are automatically checked by INDATECH's software. Communication with devices is controlled first, then the identity of the devices is checked using serial numbers of hardware parts. This prevents the program from running on a device for which it is not intended. Finally, validity of data input from devices is verified during the calibration procedures.

(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.	INDATECH provides training during installation on the customer's site. At least one system administrator is fully trained by qualified INDATECH staff to use and maintain our system. It is then the responsibility of the customer to ensure that authorized users are properly trained and qualified to use INDATECH's software.
(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.	Customer SOPs should address the establishment of policies concerning personnel responsibility.
(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.*	Customers are responsible for the management and distribution of documentation internally. INDATECH provides complete, version-controlled user documentation for the software. INDATECH also adheres to a quality management and change control system, and the system is fully documented, including software releases and documentation version traceability.
Sec. 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 11.10, 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.	INDATECH software is a closed system. Consequently, additional requirements for open systems, such as *"document encryption and use of appropriate digital signature standards",* are not implemented.
Sec. 11.50 Signature manifestations	
(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).*	Every data related user action (acquiring, saving, updating) is logged in the audit trail with the aforementioned information (1-3). The last action and corresponding information performed on measurement data is also displayed next to graphical or numerical representations.
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.	Audit trails and measurement data are saved in the same binary file and cannot be edited separately.
Electronic signatures	
	The electronic signatures functionality is not implemented in INDATECH's software because it is a closed system.

906 211 719 - Ed. 2 - 05/2025 - LB - Non-contractual document.

FRANCE
Indatech
1900, Boulevard de la Lironde
34980 Montferrier-sur-Lez
Tél : +33 4 80 78 01 40
Fax : +33 4 80 78 01 42
sales@indatech.eu
www.indatech.eu

CHAUVIN ARNOUX
INDATECH