Statement on 21 CFR Part 11 Compliance

Change Log	
Version 1, January 7, 2020	Chris Riedel, CEO, ConnectSx
Version 1.1, June 30, 2021	Chris Riedel, CEO ConnectSx
Version 1.2, November, 2025	Chris Riedel, CEO, ConnectSx

Overview

The following document outlines ConnectSx, LLC's position on ConnectSx Platform compliance with FDA's CFR Part 11 of Title 21 of the Code of Federal Regulations, Electronic Records, Electronic Signatures. That ruling became law in March 1997, and outlines the requirements for the creation, modification, maintenance, archival, retrieval, and transmittal of electronic records, as well as the use of electronic signatures when complying with the Federal Food, Drug and Cosmetic Act or any other Food and Drug Administration (FDA) regulation.

While the ConnectSx platform and its various component applications provide value through direct document and record generation for medical device usage recording and device inventory chain of custody tracking, these data are, in many cases, replicated in other business systems and/or through other established business practices and processes. Nevertheless, we understand the importance of complying with 21 CFR Part 11 and have developed the following table to define the ways our specific platform addresses each of the relevant sections. As new features are added over time, this document will be updated to reflect any impacts or implications of those changes.

Definitions, as defined in 21 CFR Part 11

1. **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.
2. **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.
3. **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** is 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. **Open System** is 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.
6. **Open System "Controls"** must institute procedures and controls designed to ensure authenticity, integrity and as-appropriate confidentiality of electronic records from the point of their creation to the point of their receipt.
    a. All controls required for closed systems plus
        i. Document encryption
        ii. Digital signatures standards to ensure record authenticity, integrity and confidentiality

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

Subpart B - Electronic Signature

§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:

Section	21 CFR Part 11	ConnectSx Platform
§11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The end user/client organization is responsible for determining a system's suitability for use in regulated environments. The ConnectSx platform and all component applications are designed, developed, deployed, and updated using a consistent software development lifecycle (SDLC) methodology. Our SDLC includes standard defined processes for requirements gathering, functional specification, application development, quality assurance, deployment management, and code versioning. As a SaaS platform, it is not standard practice to make client-specific modifications. Limited configuration options are available at the account level and are set and maintained based on end user business requirements. Use and modification of these configurations is at the discretion, and under the control of the Client. New development and feature releases are documented and can be viewed by client organizations as needed. A demo environment is available for pre-release

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

		testing if required. Use of the Demo environment by the customer must be requested by the customer in advance of any scheduled release.
§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.	The ConnectSx platform contains information that can be filtered and viewed electronically (vial HTML or mobile device), exported in .csv format, printed in PDF format, and, where necessary, shared electronically between systems using standard RESTful APIs. It should be noted that not all information is available in all formats. APIs for data sharing require configuration between both client and ConnectSx systems and employ sufficient security controls to prevent data from being shared with unauthorized systems and applications.
§11.10 (c)	Protection of records to enable the accurate and ready retrieval throughout the records retention period.	ConnectSx provides roles-based authentication to ensure only authorized individuals are allowed access to the system and associated records. Nightly backups are executed to ensure data integrity in cases of service disruption. Backups are readily available for 30 days. At 30 days, backups are stored in nearline storage. At 90 days backups are stored in coldline storage. At 750 days, backups are deleted. Our standard backup retention policy is 2 years. PDF and CSV export of data are available. Not all export mechanisms are available for all record types. The Client is required to establish internal back-up protocols to ensure records are protected for the duration of their own retention period, as defined in their internal SOPs.
§11.10 (d)	Limiting system access to authorized individuals.	The ConnectSx platform limits access using a roles-based authentication

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

		model. Mobile applications further employ 2-factor authentication using biometric or pin-based methods. Web applications use a timeout mechanism tied to token-based authentication. Once a ConnectSx user is authenticated, the role of that user ID is checked and verified to ensure they are granted only the appropriate access. All user IDs are unique and tied to individual email addresses. Access is revoked for suspended or deleted accounts. Previously mentioned time-outs and 2-factor authentication protocols are implemented to prevent unauthorized users from accessing idle records. It should be noted that it is beyond the scope of the platform to prevent users from sharing login credentials with unauthorized individuals.
§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 of at least as long as that required for the subject electronic records and shall be available for agency review and copying.	The ConnectSx platform captures identity information of the user creating and updating data across the system. Our audit trail includes username, ID, and timestamp(s) for created and last updated. Certain functional elements also record granular activity types beyond creation, update, or deletion. Information can be exported via .csv download. In depth log information can be provided as needed by customer request. Specific logging requirements can be explored on a per-case basis.
§11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.	The ConnectSx platform and associated applications employ standard workflow for the creation and execution of all records. Users are forced to comply with workflow rules using defined steps, required data, and validation checks on

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

		submission of data to the system database. User failure to comply results in system warnings and data submission failure, with appropriate error messaging.
§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.	The ConnectSx platform limits system access to authorized individuals using roles-based authorization, based on the principle of least privilege. Users only have access to documents that fall within their scope of authority, as determined by the Client. Mobile users are required to re-authenticate after timeout using 2-FA methods including biometrics or PIN code. Web users are forced to log in after a 75 minute idle timeout. It should be noted that it is beyond the scope of the platform to prevent users from sharing login credentials with unauthorized individuals.
§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.	The ConnectSx platform uses data validation to ensure the input formats match system expectations for information, on a per-field or data component basis. Invalid data formats are rejected from the system and the user is informed of the results via system error dialogues. It should be noted that it is beyond the scope of the platform to prevent users from inputting incorrect data if using the appropriate data format.
§11.10 (i)	Determination that persons who develop, maintain, or use electronic record/ electronic signature systems have the education, training, and experience to perform their assigned	It is the responsibility of the Client to develop internal policies and procedures related to training and compliance on systems used to generate and maintain records.

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

	tasks.	ConnectSx will provide Client with appropriate training and training materials as part of system implementation that can be shared with appropriate users, based on internal Client policies and procedures.
§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.	It is the responsibility of the Client to develop internal policies and procedures related to accountability and responsibility for electronic signatures. The ConnectSx platform helps Clients guard against the falsification of records by creating an audit trail and inventory chain of custody that can be used to validate and verify changes in records over time.
§11.10 (k)(1)	Use of appropriate controls over systems documentation including: Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	It is the responsibility of the Client to develop internal policies and procedures related to controlled access to system manuals, knowledge base articles, and other ConnectSx-provided documentation.
§11.10 (k)(2)	Use of appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	All documentation provided to Client by ConnectSx is version controlled, with comprehensive revision histories. It is the responsibility of the Client to develop internal policies and procedures related to controlled access to system manuals, knowledge base articles, and other ConnectSx-provided documentation.
§11.30	Controls for Open Systems - must institute procedures and controls designed to ensure authenticity, integrity and, as appropriate, confidentiality of electronic records from the point of their creation to the point of their receipt. All controls required for closed systems	ConnectSx uses Google Cloud infrastructure for our services, encrypting all information in transit and at rest. SSL is used for all web traffic, including traffic to and from our application APIs. Mobile devices employ 2 factor authentication for access after idle

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

	Document encryption Digital signatures standards to ensure record authenticity, integrity and confidentiality	timeout or application switching. Web applications use token-based authentication with 75-minute timeouts. Additional controls can be discussed if business needs warrant.
§11.50(a) (1-3)	Signed electronic records shall contain information associated with the signing that clearly indicates all 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.	Electronic records generated by the ConnectSx platform contain the following information: 1. If using physical signatures: a. Typed name of the signer b. Label of role of individual signing i. E.g. "Manufacturer Representative" or "Provider Representative" c. Handwritten signature i. Mobile and Web Device compatible 2. User name of the last person updating 3. Timestamp of last record update 4. The ability to add notes and comments to records being updated. Because the documents are created in individual accounts, and within individual workflow contexts, meaning is expressly implied. The meaning of the signatures are further defined by the account type and user role assigned to the individual account.
§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).	Electronic signatures are stored in ConnectSx platform infrastructure. Digital artifacts are stored in the database and associated with the digital record. Names and signatures captured via finger-sign on mobile and web devices are associated with the appropriate records and are viewable on the

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

		associated PDF version of the record and in the Web Console.
§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.	Every signature is automatically linked to its corresponding document at the time of signing. There is no capability for removing or copying signatures by ordinary means. Substantive usage record changes are required to secure new signatures at the time of modification.

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

Subpart C - Electronic Signature

§11.100 General Requirements

§11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The ConnectSx Platform requires a unique user ID, tied to a unique email address. Any signatures created inside of a user account will be unique to that user. Emails cannot be reused for other accounts. Further, each event record requiring a signature forces the user to implement their signature new for each unique case. It should be noted that it is beyond the scope of the platform to prevent users from sharing login credentials with unauthorized individuals.
§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.	Identity is verified when a user logs into the system using their unique email address and password combination. It is the responsibility of the Client to establish policies and procedures to verify the identity of individuals being given access to use the system. It should be noted that it is beyond the scope of the platform to prevent users from sharing login credentials with unauthorized individuals.
§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.	It is the responsibility of the Client to notify FDA of their intention to use electronic signatures for regulated data capture and maintenance.

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

§11.100(c)(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 Fisher Land Rockville , MD 20857.	
§11.100(c)(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.	
§11.200(a)(1)	Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	All ConnectSx platform applications require a unique username tied to an individual email and a unique password for each username. Passwords are case-sensitive and require a combination of upper, lower case, and numeric characters Mobile devices use biometric or PIN-base methods to provide a second factor for access when sessions time out. Web applications use token-based methods to expire user sessions and do not provide methods for circumventing timeout after expiration due to inactivity.
§11.200(a)(1)(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.	Initial login to any of the ConnectSx platform applications requires a username and password. Document creation in a single session tie signatures to the logged in user. It should be noted that it is beyond the scope of the platform to prevent users from sharing login credentials with unauthorized individuals.
§11.200(a)(1)(ii)	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each	

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

	signing shall be executed using all of the electronic signature components.	
§11.200(a)(2)	Electronic signatures that are not based upon biometrics shall be used only by their genuine owners.	It is beyond the scope of the platform to prevent users from sharing login credentials with unauthorized individuals.
§11.200(a)(3)	Electronic signatures that are not based upon biometrics shall 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.	
§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.	ConnectSx uses FaceID and FingerPrintID for iOS mobile devices. The specific protocol used is determined by user preference and device compatibility. ConnectSx does not control any changes to these security mechanisms, and relies solely on the device manufacturer to ensure mobile security integrity of their individual protocols.
§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.	ConnectSx user IDs are tied to unique email addresses, ensuring at least one unique element for all user accounts. Users are further "invited" to the system by a Client admin, providing an additional layer of oversight of usernames. It should be noted that it is beyond the scope of the platform to prevent users from sharing login credentials with unauthorized individuals.
§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).	ConnectSx does not currently implement password expiration policies. We do, however, enforce 'strong' password policies. It is up to the Client to institute a policy and procedure for internal password requirements and

© Copyright 2025, ConnectSx, LLC | www.connectsx.com

		management. Password expiration policies may be instituted in the future, and if so will be documented here. It should also be noted that admins can deactivate (suspend) user access at any time, preventing them from accessing the system for any reason, including suspicious activity.
§11.300(c)	Following loss management procedures to electronically de-authorize 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.	ConnectSx is a SaaS platform and does not include devices that bear or generate identification codes or passwords. It is the responsibility of the Client to manage lost or stolen credentials. New passwords can be generated by the individual user on-demand, and requires they have access to the existing user email account on file.
§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.	The ConnectSx platform ensures users are authenticated and verified before providing access to the system. User lockout after multiple unsuccessful login attempts and revocation of access to terminated users is also enabled. Admins in the system can deactivate users at will, where deactivation immediately revokes access to the system for the implicated user.
§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 properly and have not been altered in an unauthorized manner.	ConnectSx is a SaaS platform and does not include devices that bear or generate identification codes or passwords.

Sources

CFR - Code of Federal Regulations Title 21

© Copyright 2025, ConnectSx, LLC | www.connectsx.com