Using InTemp™ with 21 CFR Part 11 Systems

This document is intended to clarify how Onset Computer Corporation's InTemp mobile app and CX400 family of loggers are compatible within an environment where 21 CFR Part 11 is being employed.

Title 21 CFR Part 11 of the Code of Federal Regulations deals with the Food and Drug Administration (FDA) guidelines on electronic records and electronic signatures in the United States. Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable, and equivalent to paper records.

The following table shows how the 21 CFR Part 11 requirements can be addressed using InTemp in conjunction with the CX400 logger, the customer's mobile devices, and the customer's internal procedures.

Regulation Reference	Onset Comments
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:	
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	NIST-traceable temperature accuracy certification come standard with the CX400 loggers to assure customers that the hardware they are using will perform within the stated specifications. In addition, this document along with customer SOPs should be used to ensure consistency throughout the customer's process for maintaining a 21 CFR Part 11 system. The best way to ensure reliability and performance is through the proper use of the controls in Onset's InTemp application as laid out in the remainder of this document.
(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 primary data record resides in an embedded database in the app that only the app itself can access. Customers can export a secure PDF with document-level-permissions, which prevents editing of the PDF by an end user.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	InTemp stores the data files in a secure database, which can be accessed only from within the app. The customer systems must ensure that mobile devices are backed up regularly. The mobile device must have sufficient memory to allow for storage of data for the appropriate records retention period. The app will keep all data files unless explicitly deleted by a user.
(d) Limiting system access to authorized individuals.	Both Android and iOS provide their own locking mechanisms to prevent unauthorized individuals from accessing the data. In addition, the InTemp app and CX400 logger have the capability to add a passkey to the logger, preventing other mobile devices from connecting to or accessing the data on the device. The InTemp app will log a user out and require re-authentication each time the app is closed or backgrounded in the device.
(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 pertinent user events are stored in the logger, including connections, configurations, downloads, and periodic checks. In addition, the user is forced to log in to the app with an app-specific username and password. The events are included in the secure PDF, along with the user who performed each action, the time of the action, and the latitude and longitude of the action (assuming location services were enabled on the mobile device at the time).
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	A reminder feature in the app aids with performing periodic temperature checks on the logger.

Regulation Reference	Onset Comments
Sec. 11.10 Controls for Closed Systems (continued)	
(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.	Access to mobile devices running the app can be controlled by Android and iOS locking mechanisms, including biometric security. Customer procedures should be used to ensure only authorized users can access the mobile devices.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Every CX400 data logger has a unique serial number that is stored with the data file and uniquely identifies that data file as being generated by that logger.
(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.	User guides and online training are available to ensure the user has the information needed to operate the system.
(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.	InTemp app users are forced to log in to the app using a username (email) and password. Those values are stored in the logger and the secure PDF, and cannot be edited.
(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 is under version control.	Customers should follow their own guidelines for control when using any documentation, including user guides or SOPs for the CX400 or InTemp products. All Onset provided documentation is revision controlled. It is customers' responsibility to ensure they are using the most recent revision and that it is consistent with their internal SOPs, Training Documents, and other relevant materials.
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.	All PDF reports generated by InTemp are secured with document-level permissions that ensure changes cannot be made to the PDF.
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.	The secure PDF report generated by the InTemp app indicates the name, email, and company of the user who generated the report. In addition, all pertinent information about the logger and the deployment is contained in the report.
(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).	Not applicable.

Regulation Reference	Onset Comments
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.	The secure PDF is protected by document-level permissions embedded in the PDF report itself. These permissions cannot be edited by the end user.
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.	The actions performed on the logger are all contained in the secure PDF report, and the user who performed each action is listed in that report. Actions include: • Configuring and starting the logger • Daily checks of the logger • Downloading the logger • Generating the PDF report
(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.	Email address is used as a username, ensuring verification of the identity.
(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.	Not applicable.
Sec. 11.200 Electronic Signature Components and Controls	
Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	Organizations using the InTemp system should ensure that their users' iOS or Android devices are secured with a passcode or finger print ID.
(2) Be used only by their genuine owners	See above
(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.	No comment.

Regulation Reference	Onset Comments
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.	Customers should set up their iOS or Android devices to meet the requirements in this section.