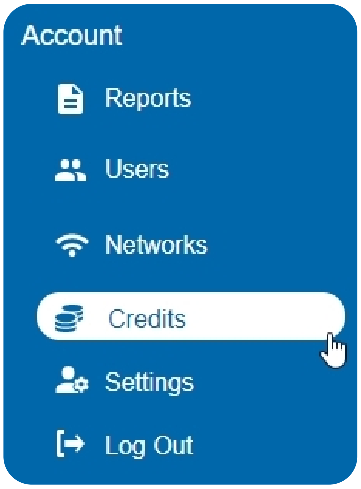
Remote Monitoring for Business

Title 21 Code of Federal Regulations Part 11



It is more important than ever for companies to automate their record keeping practices. 21 Code of Federal Regulations (CFR) Part 11B was developed by the FDA in 1997 to keep your records safe and secure in the digital age. Monnit takes great pride in making sure the readings delivered by our product lines are authentic, reliable and confidential.

iMonnit now has a 21 CFR Part 11B credit for purchase straight through the portal. Just find Credits in the main navigation menu and choose the "CFR" add-on for your iMonnit Premiere subscription.

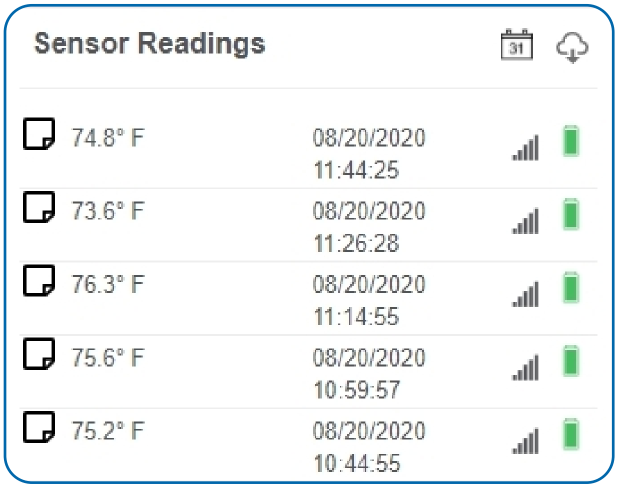
Systems assigned to work in regulated environments such as 21 CFR Part 11B are recognized for safeguarding sensitive information. Computer systems containing "records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations." [1] For example, a temperature sensor used to monitor ambient temperature in the waiting room for a healthcare institution does not require 21 CFR Part 11B approval. However, a temperature sensor monitoring an area where vaccines are stored at proper temperature ranges in the same institution will need to be part of a 21 CFR compliant system.

Electronic Record Authenticity Requirements

Authenticity requirements outlined by 21 CFR Part 11B include:

- System consistently performs as designed.
- System must have the capacity to identify invalid or altered records
- Sensor data is encrypted, stored redundantly and cannot be modified after recording
- Sensor data is logged and time-stamped
- All data is backed up over distributed databases

iMonnit, with CFR enabled, meets each of these guidelines. Sensors are available with traceable calibration certificates. The readings taken by sensors and stored on the online portal iMonnit cannot be changed in any way once the data is taken. Online data annotations can be added to track resources and remediation steps. All data is logged, time-stamped, and available under the history tab in iMonnit and available for export by scheduled report.



Sensor Readings

74.8° F	08/20/2020 11:44:25
73.6° F	08/20/2020 11:26:28
76.3° F	08/20/2020 11:14:55
75.6° F	08/20/2020 10:59:57
75.2° F	08/20/2020 10:44:55

Electronic Record Integrity Requirements

21 CFR Part 11B requirements are as follows:

- Sensor data can be graphed
- Sensor data is time stamped
- Sensor data can be exported in spreadsheet/text form
- Sensor data can be exported using a secure API

All sensor data is graphed and time stamped on iMonnit. These records can also be exported on the history tab while viewing that time tamped data. API calls can be accessed by going to https://www.imonnit.com/API.

[1] FDA (2018, July 12) Part 11, Electronic Records; Electronic Signatures - Scope and Application. http://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm

Change Log Audits

To view system changes, you can export logs that include:

- User
- Data
- Change

These are available for both sensor changes as well as Network changes.

Confidentiality Requirements

An application is considered confidential by 21 CFR Part 11B when it satisfies the below requirements:

- A username and password are needed for access
- Roles-based access can also be given to authorized users
- Logged data cannot be accessed by unauthorized users
- Customer data is separated by accounts

No data on iMonnit can be accessed by unauthorized users. Username and password combinations are not shared between other users. iMonnit is a secure cloud-based portal. Roles for multiple users on an account can be assigned by administrators right from their smartphone.

Accurate electronic records are important. Software applications used to store these records must be able to validate data, have an audit trail, copies of records, and be able to retain archived readings. Monnit supports these requirements, making it the right choice to automate company processes.

21CFR Requirement Checklist

✓ = Fully Compliant

◆ = Compliant with user control via SOPs (Standard Operating Procedures)

21 CFR Part 11 Requirement	Meets This Requirement?	Comments
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.	✓	The Cloud Software 21 CFR provides both Device and System Audit trails detailing user activities.
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.	✓	The Cloud Software 21 CFR can be used to generate complete copies of all records in both human readable and electronic form - which can be used for inspection, review and copying by the agency.

21 CFR Part 11 Requirement	Meets This Requirement?	Comments
c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	✓	The Cloud Software 21 CFR records are stored in a Database with controlled access, which are readily and securely retrievable using the data logger web user interface. Data is read-only and cannot be accessed in any other way. Each action to delete, print, export or add comments to data, is further controlled by the entry of an Approver’s credentials. The Approver must have sufficient privileges to perform the selected action.
d) Limiting system access to authorized individuals.	✓	Access to the Cloud Software 21 CFR is under user email and password control. Administrators grant access to chosen users only,and assign usage privileges to each. Assignable privileges include, the ability to view, print and export data.Key actions are further controlled by the entry of an Approver’s credentials. The Approver must have sufficient privileges to perform the selected action.
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.	✓	Cloud Software 21 CFR generates a System Audit trail, detailing all user activities. For more information on what is included in audit trail, please see table 1. Data cannot be overwritten or altered however, data and the System Audit can be deleted by an Administrator. All delete actions are recorded in the System Audit.
f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	✓	The Cloud Software 21 CFR is designed to ensure that the user is limited to performing one function at a time, and in the correct order.
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.	✓	Yes - please see Sec. 11.10 d).
h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	N/A	Not applicable to Cloud Software 21 CFR.
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.	✓ ◆	This is the user’s responsibility. The WiFi-21CFR device is supplied with a Quick Start Guide and online Help resources, and a thorough help file is included within the 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.	✓	This is the user’s responsibility. Users need to have their own Standard Operating Procedure.
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.	✓	This is the user’s responsibility. The WiFi-21CFR device is supplied with a Quick Start Guide, and a thorough help file is included within the software.

21 CFR Part 11 Requirement	Meets This Requirement?	Comments
2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	✓ ◆	The Cloud Software 21 CFR provides both Device and System Audit trails to record system changes and actions carried out. In-house procedures are the user's responsibility.

Section 11.50 Signature Manifestations

21 CFR Part 11 Requirement	Meets This 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;	✓	Yes - please see Sec. 11.10 e).
2) The date and time when the signature was executed;	✓	Yes - please see Sec. 11.10 e).
3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	✓	Yes - please see Sec. 11.10 e).
b) The items identified in paragraphs a1), a2), and a3) 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).	✓	Yes - please see Sec. 11.10 e).

Section 11.70 Signature/Record Linking

21 CFR Part 11 Requirement	Meets This 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.	✓	Yes - please see Sec. 11.10 e).

Subpart C - Electronic Signatures

Section 11.100 General Requirements

21 CFR Part 11 Requirement	Meets This Requirement?	Comments
a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	✓	Cloud Software 21 CFR users create their own password for their account. Each Sign-In Email address must be unique.
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 the user's responsibility. Users need to have their own Standard Operating Procedure.

21 CFR Part 11 Requirement	Meets This Requirement?	Comments
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.	✓	This is the user’s responsibility. Users need to have their own Standard Operating Procedure.
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, MD20857.	✓ ◆	This is the user’s responsibility. Users need to have their own Standard Operating Procedure.
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 the user’s responsibility. Users need to have their own Standard Operating Procedure.

Section 11.200 General Requirements

21 CFR Part 11 Requirement	Meets This 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.	✓	The Cloud Software 21 CFR uses Email and Password at Sign-In and Email and Password of an Approver, at the time key actions are being performed.
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.	✓	On the Cloud Software 21 CFR, each and every key action requires entry of both Email address and Password as the Approval signature.
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.	✓	On the Cloud Software 21 CFR, each and every key action requires entry of both Email address and Password as the Approval signature.
2) Be used only by their genuine owners;	✓	Please see Sec. 11.100 a).
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.	✓	Please see Sec. 11.100 a). Attempts made to Approve an action, by a user without a sufficiently high user privilege level, will be recorded in the System Audit.
b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N/A	

Section 11.300 Controls for Identification Codes/Passwords

21 CFR Part 11 Requirement	Meets This Requirement?	Comments
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.	✓	Please see Sec. 11.100 a).
b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	✓	An Administrator can change any user's registered Email address or password at any time. They can immediately deny system access to a user by permanently deleting the user and or temporarily change their password.
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.	✓ ◆	Users can be deleted or their privileges changed by an Administrator. In the event that a user forgets their password, a reset link can be sent to the user's registered email address. It is the user's responsibility to make sure this is covered in their Standard Operating Procedure.
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.	✓	Attempts made to Approve an action, by a user without a sufficiently high user privilege level, will be recorded in the System Audit.
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 the user's responsibility. Users need to have their own Standard Operating Procedure.

System Audit

All System Audit entries are Date/Time and contain the Full Name and Email address of the Signed-In User and the user giving Approval. The Approver must have the required privilege level to complete the operation.

If the user attempts to complete an action requiring Approval but has an insufficient privilege level, the attempted action is recorded in the System Audit.

Action	System Audit Entry	Approval Required	User Privilege Required
Devices:			
Archive/Clear/ Delete a device	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email List of Archived /Cleared / Deleted Devices - Names and MAC Addresses	✓	Administrator
Change Device Settings	None		Manage Devices
View Data:			
Other Sessions:			

Action	System Audit Entry	Approval Required	User Privilege Required
Export Device Audit	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Device Name and MAC Document ID	✓	Print & Export Device Data
Graph:			
Export	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Start & End Time / Date of data Document ID	✓	Print & Export Device Data
Print	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Start & End Time / Date of data Document ID	✓	Print & Export Device Data
Data:			
Add a Comment	Time/Date stamp Approvers Full Name & Email Signed-In user’s Full Name & Email Time/Date of data value Data Value(s) Comment	✓	Administrator
Export	Time/Date stamp Approvers Full Name & Email Signed-In user’s Full Name & Email Start & End Time / Date of data Document ID	✓	Administrator
Event Logs:			
Clear Log	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email List of Devices - Names and MAC	✓	Administrator
Export	Time / Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Start & End Time / Date of Log List of Devices - Names and MAC Document ID	✓	Administrator
Send This Log	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Start & End Time/Date of Log List of Devices - Names and MAC Recipient: Email Address Document ID	✓	Administrator
Reset Alarm	None		Manage Devices
New Device added (New Devices)	None		Manage Devices
Administration:			
Users:			
Create New User (pending user email address verification)	None		Administrator (Implied)

Action	System Audit Entry	Approval Required	User Privilege Required
Edit User: Full Name	None		Administrator (Implied)
Edit User: Email Address	None		Administrator (Implied)
Edit User: Password	None		Administrator (Implied)
Edit User: User Privileges	None		Administrator (Implied)
Delete User	None		Administrator (Implied)
Locations:			
Create New Location	None		Administrator (Implied)
Edit Location	None		Administrator (Implied)
Delete Location	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Name of Location(s) affected List of Archived/Cleared/Deleted Devices - Names and MAC Addresses	✓	Administrator (Implied)
Archive Location	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Name of Location(s) affected List of Archived/Cleared/ Deleted Devices - Names and MAC addresses	✓	Administrator (Implied)
Change users belonging to a location	None		Administrator (Implied)
System Audit:			
Delete part or all of the System Audit	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Amount of System Audit retained	✓	Administrator (Implied)
Export System Audit	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Audit period or Start & End Time/Date File Format Time Zone Document ID	✓	Administrator (Implied)
Settings:			
Change Auto Sign-Out time	Time/Date stamp Approvers Full Name & Email Signed-In user's Full Name & Email Old and New Auto Sign-Out time	✓	Administrator (Implied)
User Sign In	None		None
User Sign Out	None		None
Account:			

Action	System Audit Entry	Approval Required	User Privilege Required
Account Details:			
Account Name	None		Acct Administrator
Company Name	None		Acct Administrator
Address	None		Acct Administrator
Town/City	None		Acct Administrator
State/County	None		Acct Administrator
Zip/Postcode	None		Acct Administrator
Country	None		Acct Administrator
Time Zone	None		Acct Administrator
Automatically adjust daylight saving time	None		Acct Administrator
Billing Details			
Name	None		Acct Administrator
Address	None		Acct Administrator
Town/City	None		Acct. Administrator
State/County	None		Acct Administrator
Zip/Postcode	None		Acct Administrator
Country	None		Acct Administrator
Account type changed (Up/Downgrade)	None		Acct Administrator
My Settings			
Change Date format	None		None
Change Time format	None		None
Change Password	None		None
Change Email Address	None		None
Reduce the number of emails I get	None		None
Insufficient Privilege			
Approval Failed: Any Action requiring Approval	Time/Date stamp Full Name & Email entered Signed-In user's Full Name & Email Attempted Action	✓	Administrator

Example System Audit

SYSTEM AUDIT			
Audit Period	09/22/2020 00:00	to	9/23/2020 00:00
Account	ABC Company		
Date/Time	9/23/2020 00:00	Clear Device Data	
Signed-In User	User One (userone@example.com)	Approved by	Administrator (administrator@example.com)
Comments			
Date/Time	9/23/2020 00:00	Export Device Audit	
Signed-In User	User Two (usertwo@example.com)	Approved by	Administrator (administrator@example.com)
Comments			
Date/Time	9/23/2020 00:00	Approval Failed	
Signed-In User	User Three (usertwo@example.com)	Approved by	
Comments			

Table 1- Audit Trail Entries

Audit Entries	Software Audit	Session Audit
User Created	✓	
User Edited	✓	
User Disabled	✓	
User Logged In	✓	
User Logged Out	✓	
Failed Log In	✓	
Users Password Changed	✓	
Users Password Created	✓	
Software Settings Changed	✓	
Users Password Reset	✓	
Logger Initialized	✓	✓
Logger Stopped	✓	✓
Data Download	✓	✓
Comment Added/Edited	✓	✓
Data Approved	✓	✓
Data Un-Approved	✓	✓
Data Exported	✓	✓

MONNIT®

Monnit Corporation
3400 South West Temple • Salt Lake City, UT 84115 • 801-561-5555
www.monnit.com