Therma°

21 CFR 11 Compliance

Section 11.10 Open Systems Controls

21 CFR 11 Requirement	Manner of Adherence	Compliant?
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.	Retain both Device and System Audit logs detailing all system activities. Logs are routinely reviewed and confirmed across all systems.	✓
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 electron records.	Companion software 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.	✓
c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Cloud records stored in a database with controlled access, which are readily and securely retrievable.	✓
	Sensor data is read-only and cannot be accessed in any other way.	✓
	Each action to update, print, export, or add comments to data is controlled by entry of	✓

✓ - Fully compliant

⚠ - Compliant with user control via SOPs (Standard Operating Procedures)

	an Approver’s credentials. Must have sufficient credentials to perform selected action.	
	Records protected by encryption to ensure accuracy, incorruptibility, and (where applicable) confidentiality.	✓
	Internal procedures for Data Backup and Recovery, Data Archiving, and Disaster Recovery/Business Continuity.	✓
d) Limiting system access to authorized individuals.	Access under user account/password control.	✓
	Admins grant access to chosen individuals only, and usage privileges to each as needed. Key actions further controlled by entry of Approver’s credentials. Administrators can be notified of unsuccessful login attempts via email/text/alert/etc.	✓
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.	Automatically records System Audit logs detailing all user activities.	✓
	Data cannot be overwritten/altered ,but can be deleted by an Administrator. Delete actions recorded in system audit.	✓
f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	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.	See 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.	Document how data is input into the system. If data is being collected from another external system, describe the connection to that source and how the system verifies the identity of the source data.	✓
i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have	User’s responsibility.	✓⚠

the education, training, and experience to perform their assigned tasks.		
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.		✓⚠
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.		✓⚠
k) 2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	System provides both Device and System Audit logs to record system changes and actions carried out. In-house procedures are the user's responsibility. Users need to have their own Standard Operating Procedure.	✓⚠

Section 11.50 Signature Manifestations

21 CFR 11 Requirement	Manner of Adherence	Compliant?
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 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).	As in 11.10 (e) above.	✓

Section 11.70 Signature/Record Linking

21 CFR 11 Requirement	Manner of Adherence	Compliant?

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.	As in 11.10 (e) above.	✓

Section 11.100 Electronic Signatures General Requirements

21 CFR 11 Requirement	Manner of Adherence	Compliant?
a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Users create their own password for their account following required password standards. Each username 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.	✓⚠
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. 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.		✓⚠

Section 11.200 Electronic Signatures Components and Controls

21 CFR 11 Requirement	Manner of Adherence	Compliant?
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.	Username and Password at Sign-In and Username 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.	Each and every key action requires entry of both username 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.		
2) Be used only by their genuine owners; and	See 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.		✓
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 11 Requirement	Manner of Adherence	Compliant?
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.	See 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 username 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	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	✓⚠

or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	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.	✓⚠