
21 CFR Part 11 and the Cold Chain

Overview

Pharmaceutical and biotechnology pipelines contain an increasing number of temperature sensitive drugs where maintaining the proper temperature in the supply chain is a priority. Electronic temperature monitors have become the standard tool to ensure proper temperature was maintained. Because the time/temperature data collected during the shipment is often used for the accept/reject decision, the electronic record is a critical component to the cold chain.

The purpose of this document is to discuss how 21 CFR Part 11 impacts the cold chain and temperature monitoring. The paper will discuss the different approaches to comply with 21 CFR Part 11 and provide an evaluation criterion when selecting a Part 11 solution for cold chain temperature monitoring.

Temperature Records: Definition and Use

To ensure safe transport of temperature-sensitive pharmaceutical products many organizations use electronic devices known as temperature monitors. Temperature monitors measure and store the temperature experienced by the product during shipment. Temperature monitors are used in a variety of applications including the monitoring of research, clinical and finished goods while in-transit. They are also used to monitor the temperature of warehouses, coolers and other storage facilities.

Software applications extract the temperature data from the monitor and provide functionality for viewing, printing, saving, and analyzing. Organizations' operating procedures typically dictate whether the file is saved electronically or as a hard copy with related documentation. The temperature data collected by the monitor is a critical component to product integrity as it is the primary indicator of temperature exposure during transit or storage.

Temperature records – paper or electronic – must be maintained and readily available for the record retention period. Record retention periods vary based on the application and predicate rules. A temperature record created from the monitoring of a research sample would require a more lengthy record retention period than a temperature record created from monitoring a shipment of commercial pharmaceuticals. However, the majority of pharmaceutical applications dictate that temperature data collected must be readily available for a period of time after the shipment was received.

When a software application is used to extract the temperature data from a monitor, an electronic record is created. The temperature data can typically be saved in a variety of standard or proprietary formats. Regardless of the format, when the electronic record is created, it is governed by 21 CFR Part 11.

Common Approaches to Compliance

There are multiple approaches to record-keeping compliance regarding temperature records practiced in the industry. Following FDA's initiative on a risk-based approach to cGMP, the user organization should assess how temperature records are used and the evidence they provide on product safety, efficacy and quality. The results of this assessment and other business drivers, such as efficiency and data accessibility, will dictate the approach most appropriate for the user organization. Each of the following approaches has proved to be compliant with predicate rules and/or 21 CFR Part 11.

Each approach falls into three main categories:

- Paper Based Systems
- Client/Desktop System
- Central Repository System

Paper Based System

Maintaining a paper-based system for temperature records is an extension of widely accepted paper record management practiced in an organization. With a purely paper based system, an electronic record is never created and 21 CFR Part 11 does not apply.

When a shipment arrives, the temperature data is extracted from the monitoring device and printed. A printout often includes a graph view and tabular data. The hardcopy is initialed or signed and dated by the receiving personnel (per operating procedure) and a disposition recorded. A paper-based system can be cumbersome in the event of a temperature excursion. When an excursion occurs, the temperature data often has to be reviewed by other personnel in the organization – most often the product quality group. The product quality group must compare the temperature data to the product stability data to determine the impact on product efficacy. The temperature data must be in an electronic format to import into LIMS and stability data systems or, at a minimum, into Excel to complete the comparison. Performing these calculations by hand from the temperature data hardcopy is time consuming and error prone. When an electronic temperature record is created the regulations outlined in 21 CFR Part 11 apply. This is a significant limitation to pure paper-based systems.

Client/Desktop System

A Client or Desktop system maintains the electronic record created from the monitor as the shipment of record. With these systems, the temperature record is stored as a file on the desktop where it was downloaded. Organizations using this approach typically organize the file structure on the desktop to facilitate finding the records upon request. Common file structures used are based on geography – what origin was the shipment received, time – what week/month was the shipment received, identifier – what Order or Shipment Number was used to track the shipment. Some organizations also store temperature records based on the disposition that was made and store the record in the appropriate file folder – i.e., “Approved” or “Rejected”.

The Client/Desktop can be challenging when deployed in a large multi-national organization. By relying on the local PC for data storage and maintenance, the organization must institute the same procedures and file structure across all of its receiving locations. The organization must often rely on the local IT personnel (if they are available) to ensure that the data stored on the local PC is available for the record retention period. This would include backing up the data and ensuring the data remains in “readable” format during record retention. Long retention periods for research and clinical materials may dictate that a file is readily available for over a decade. In these situations, an organization would have to ensure that the data is available as well an application that can display the data when necessary.

Centralized storage on an organizations network is an alternative to file storage and maintenance that eliminates the need for consistent file structures on individual PCs. For organizations that are shipping product within their company, the Client/Desktop solution is an appropriate one. For organizations that are utilizing partners, such as Contract Research Organizations (CRO), Third Party Logistic (3PL) providers or Contract Packaging Houses, the Client/Desktop solution is not viable. In this situation, access to the organizations network would be required so that temperature data could be reviewed and stored correctly. An organization would have to build a robust access and authentication schema to determine who has what access to the organizations network. In many cases, separate “sites” would need to be deployed to control what partners have access to what data. Designing, administering and maintaining the infrastructure would become a burden to IT personnel. It also exposes the organization to potential intrusion to sensitive data stored on the network.

A Client/Desktop System approach is well suited for the very small organization in which monitors are downloaded on a single PC or in an environment that can be tightly controlled and the integrity of the file structure maintained.

Web-Enabled Database System

A web-enabled Database system provides an environment in which a temperature data is collected and saved centrally in a database using a web browser. In a browser-based application a user has access to the application directly through the web. The user does not have to install an application locally to collect and view the temperature data. This can be completed by navigating to the appropriate website and having the proper username and password to access the application.

Through the username and password, access to application functionality and data stored in the database can be restricted. A web-enabled system provides an environment that an organizations' partners can access without exposing the organization to network intrusion and sensitive data.

The centralized storage of the data also enables product quality to quickly access the data for analysis and comparison to stability data. Rather than emailing temperature data files across the organization, quality, packaging and other necessary parties can view the same temperature data at the same time. This eliminates the risk of redundant electronic copies of the same temperature data across an organization as it is emailed from one person to the next.

By storing temperature data in a database system, an organization can utilize the data in ways not possible with paper and client/desktop systems. Data can be analyzed in the aggregate to identify trends and/or highlight issues with particular distribution centers, carriers or routes that would not be apparent with the other systems. The database environment enables the combination of temperature data with metadata so that cold chain performance indicators can be tracked. For example, combining temperature data with container data enables packaging engineers to assess the performance of container design over a period of time. A logistics manager can assess the performance of their carriers as it relates to temperature control.

"Turn-Key" 21 CFR Part 11 Solutions Are Impossible

A number of organizations have advertised "Turn-Key" 21 CFR Part 11 solutions for various applications. A software application cannot ensure full Part 11 compliance alone. Documentation and adherence to procedures are critical to Part 11 compliance. Specifically, sections 11.10 (i), (j), (k) outline regulations involving training and documentation distribution that require procedural controls by the customer organizations. Vendors that indicate they can provide a "Turn-Key" 21 CFR Part 11 solution are incorrect.

Conclusion

The intent of the 21 CFR Part 11 regulations was to provide a common language and guidance on electronic record use in an organization. However, the regulation specifically avoids recommendations or inferences on solutions to compliance.

Selecting the most appropriate methodology for a temperature monitoring compliant system depends on the requirements of the user organization. No one solution applies to all. The selection process and ultimately the selected solution should be dictated by the decisions temperature records are used to make and the impact they have on product safety, efficacy and quality. A user organization can leverage vendor technology for technical controls, but procedural and administrative controls are critical to compliance and cannot be outsourced or omitted.

Temperature Monitoring Systems and 21 CFR Part 11 Compliance
Evaluation Matrix

The following matrix is a guide to selecting a temperature monitoring system that provides the technical controls for Part 11 compliance and indicates the procedural and administrative controls necessary for full compliance. In completing their evaluation, the user organization should conduct a GAP analysis between their current system for maintaining temperature records and a compliant system. A typical GAP analysis would include a thorough review of the current system against the regulation to determine what areas are currently compliant and which are not. A GAP analysis should also include any business requirements not met by the existing system.

Category	Regulation Reference	Evaluation Criteria
SYSTEM VALIDATION, TRAINING AND DOCUMENTATION	11.10 (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	<i>The software and hardware vendor(s) should produce a detailed validation package that includes the features designed in the system and evidence that those features function appropriately.</i> <i>The hardware and software vendor(s) should maintain a controlled environment for product development in which procedures are developed, routinely followed and regularly audited.</i>
	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 tasks.	<i>When selecting a temperature monitoring system ensure that the vendor(s) developers are properly trained in the relevant technologies and regulations (i.e., 21 CFR Part 11) related to the system.</i> <i>The vendor(s) should provide training for the system users and provide a detailed user manual describing system functionality. The vendor(s) should also maintain a Technical Support function that users can contact for support.</i>
	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.	<i>The customer organization should provide procedures and controls outlining for the users what an electronic signature represents in the system. In addition, the customer organization should provide information on the recourse for signature falsification.</i>
	11.10 (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.	<i>The vendor should provide documentation such as validation packages and user manuals. These documents should be maintained as part of the customer's document management system and controlled accordingly.</i>
SYSTEM ACCESS AND SECURITY	11.10 (d) Limiting system access to authorized individuals.	<i>Access to the temperature monitoring system should be controlled to authenticated users only. The vendor should provide functionality for user administration including system access and activities the users has available to them.</i>
	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.	<i>The temperature monitoring system should restrict access to activities via Username and Password. The vendor should provide functionality ensuring that access to data is secure and prevent unauthorized access. For web applications, the vendor should provide data encryption such as Secure Sockets Layer (SSL) at 128-bit encryption.</i>

<p>RECORD READABILITY AND DATA SOURCE</p>	<p>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. 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.</p>	<p><i>The vendor should provide functionality to print temperature data and related meta-data. In addition, the temperature data should be available for electronic export into a common readable file such as XML or .xls format.</i></p>
	<p>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.</p>	<p><i>The vendor should provide controls to ensure that data entered into the system is from a valid source and in the correct format. If certain steps should be performed before others, the application should control the sequence of steps.</i></p>
<p>DATA RETENTION AND BACKUP</p>	<p>11.10 (C) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><i>The type of temperature monitoring system dictates who is responsible for record retention. For a Client/Desktop system that relies on local storage on the PC, the customer must ensure that data is being backed up regularly and that data is readily retrievable upon request. The computer environment should be secure and maintained to prevent catastrophic failures in which data may be lost.</i></p> <p><i>For Web-Based Central Repository systems, the vendor shall provide a secure environment in which time/temperature and shipment data will be stored. Some solutions may include hardened Data Centers that provided guaranteed up-time and high Quality of Service (QoS).</i></p>
<p>SIGNATURE/RECORD LINKING</p>	<p>11.50 (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. 11.50 (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). 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.</p>	<p><i>The vendor shall provide functionality that captures the full name of corresponding to the electronic signature, the date and time the signature was executed and the meaning of the signature. An electronic signature would be used to sign the shipment disposition (i.e., accepted or rejected).</i></p>