ELPRO

WHITE PAPER

Could Poor Temperature Data Management be Putting Your GxP Facility at Risk for Data Integrity Violations?

we prove it.

How to Avoid Poor Temperature Data Management at Your GxP Facility

Data integrity remains a hot topic after recent headlines of data fabrication in the lab and new guidelines from regulatory agencies. It's an international issue that covers all of GxP, including GMP, GCP and GLP. Although a facility having intentionally falsified records is the type of juicy headline that makes the news, the fact of the matter is that 95 % of data integrity issues are actually unintentional and arise out of poor data management. If you're still manually writing temperature data or using chart recorders as part of your temperature monitoring activities, then you are familiar with how manual the process of recording and storing temperature data can be.

For years, the Food and Drug Administration (FDA) has stressed the significance of maintaining reliable data and has made it clear that data integrity lays the groundwork for supplying safe and effective medicines to patients. Now, the FDA, along with the Medicines and Healthcare products Regulatory Agency (MHRA) and World Health Organization (WHO) have taken lead roles in providing additional guidance on data integrity for the industry. Data integrity guidelines were released by the MHRA in 2015, and in 2016, guidelines are in draft form from the FDA and WHO, making it a good time to review how you handle your critical temperature / environmental monitoring data.

Why Monitoring?

Environmental monitoring plays an essential role in your GxP activities because the environments at which medicines, foods and consumer care products are manufactured, tested and stored can affect composition and efficacy. Even moderate changes in temperature, humidity or CO_2 can make experiments, manufacturing, laboratory, or distribution results unreliable. Refrigerators, freezers, stability chambers, storage areas and incubators are all examples of controlled environments utilized to ensure these sensitive products are maintained at specific conditions.

Regulators ask that you keep records of the temperature / environmental data to document that activities were performed under the appropriate environmental conditions. It will also ensure that all tests performed are reliable and repeatable. In the event of an excursion, deviation reports will demonstrate the corrective action taken to document whether or not the product was at risk.

Automated versus Manual

The FDA defines data integrity as «…the completeness, consistency and accuracy of data. Complete, consistent and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy and accurate (ALCOA).» There is a misconception that meeting data integrity expectations is easier with paper-based processes and that data integrity does not apply equally to paper as it does electronic records, however data integrity expec-

tations apply to all data collected. In fact, the WHO draft on data integrity notes that there is a need to modernize risk management practices with updated, current technology and states that data integrity risks are higher when processes are manual or paper-based.

WHO draft guidance states that data integrity risks are higher when processes are manual or paper based.

The data integrity guidance from the MHRA specifically warns against reverting from computerized systems back to paper, stating: «Reverting from automated, computerized to manual / paper-based systems will not in itself remove the need for data integrity controls. This may also constitute a failure to comply with Article 23 of Directive 2001 / 83 EC, which requires an authorization holder to take account of scientific and technical progress and enable the medicinal product to be manufactured and checked by means generally accepted scientific methods.»

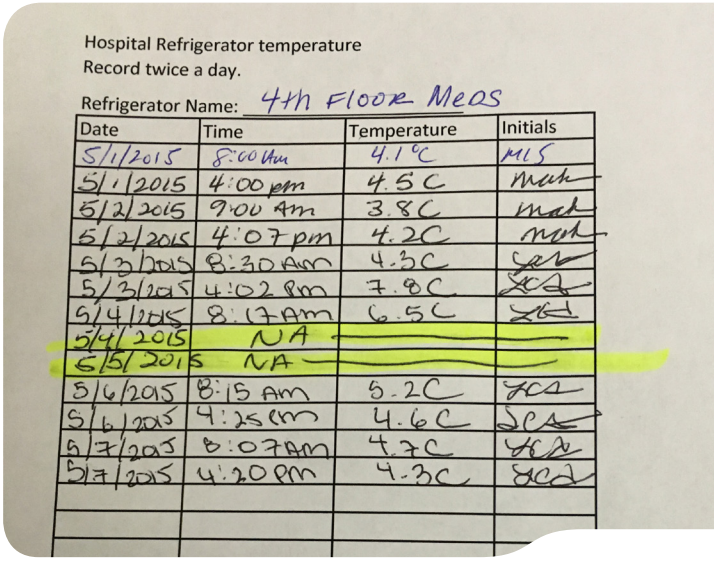
Efficient, Compliant and Practical Monitoring

Historically, monitoring has been achieved in several ways – from handwritten temperature logs to integrated networked data logging systems. First we'll define the most common practices for monitoring and map out the process to determine areas of risk as it relates to data integrity.

Handwritten Temperature Logs

These logs require personnel to manually check the equipment temperatures on a daily basis, often times twice daily. This may consist of a lab technician walking around with a notebook writing down temperatures. Some standard operating procedures (SOPs) require a minimum of four hours between the two checks, and in a busy lab, there are instances where it is difficult to allocate time to complete, which not only poses a risk to your process but isn't efficient from a business perspective, either. Also, what control is in place to protect this handwritten temperature data? What happens when you forget to check and record the temperature?

Other SOPs require that temperatures are checked in the morning and then again at the end of the day. The downfall is when the temperature is ok at the end of the day, but is in alarm the following morning. There is no point-by-point, time stamped temperature data to indicate exactly when the problem occurred, and how long temperature was in alarm. When this happens, most policies are to assume worst-case scenario. This could mean discarding product or losing days worth of time to produce test results.



Hospital Refrigerator temperature
Record twice a day.

Refrigerator Name: 4th Floor Meds

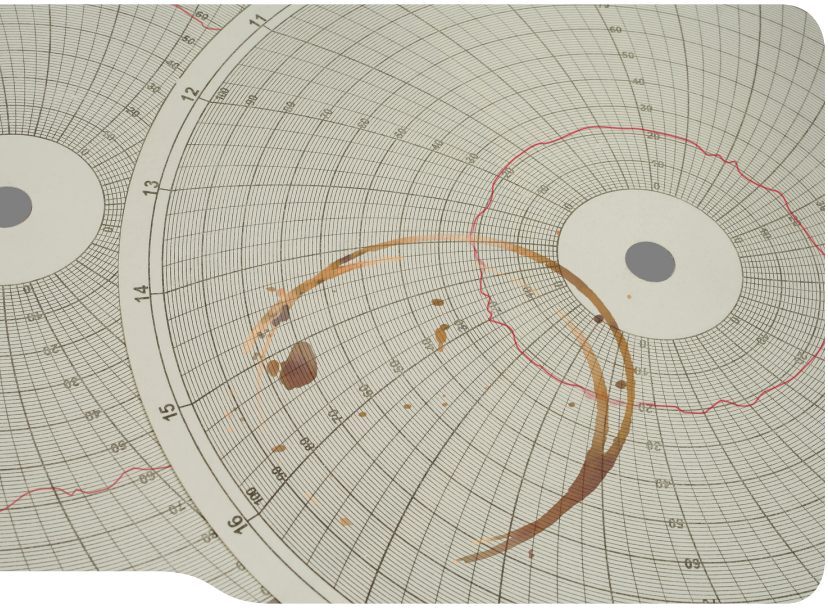
Date	Time	Temperature	Initials
5/1/2015	8:00 Am	4.1 °C	MLS
5/1/2015	4:00 pm	4.5 C	mak
5/2/2015	9:00 Am	3.8 C	mak
5/2/2015	4:07 pm	4.2 C	mak
5/3/2015	8:30 Am	4.3 C	[illegible]
5/3/2015	4:02 Pm	7.8 C	[illegible]
5/4/2015	8:17 Am	6.5 C	[illegible]
5/4/2015	NA		
5/5/2015	NA		
5/6/2015	8:15 Am	5.2 C	[illegible]
5/6/2015	4:25 Pm	4.6 C	[illegible]
5/7/2015	8:07 Am	4.7 C	[illegible]
5/7/2015	4:20 Pm	4.3 C	[illegible]

Once data is collected, where is it stored? Is the data then manually being transferred into a LIMS system? Any time data is handwritten and manually transferred to storage or even transferred to an electronic format, there is a chance that data can be omitted or changed. It's just the nature of manually processing data. As you think of your own procedures, identify steps like these where the potential for data integrity problems arise.

Chart Recorders

Chart recorders are still king in many GxP areas, and perhaps your organization has used these paper charts for your temperature monitoring activities for years. However, the process for changing out chart paper, checking temperature graphs, storing paper and writing deviation reports is very manually intensive, lending to human handling errors. Any notations or reporting made on these paper charts again requires the application of the ALCOA principle.

Additionally, an independent, designated archivist must store all the charts in protected and controlled area. What happens when an auditor asks for the temperature data of a refrigerator last year? How accessible is your temperature data in this format?



The chances of unintended data failure are higher with paper records. Take this example of a coffee ring on a chart recorder graph readout. Data must follow the ALCOA principle, and damage to the original file could put your data at risk.

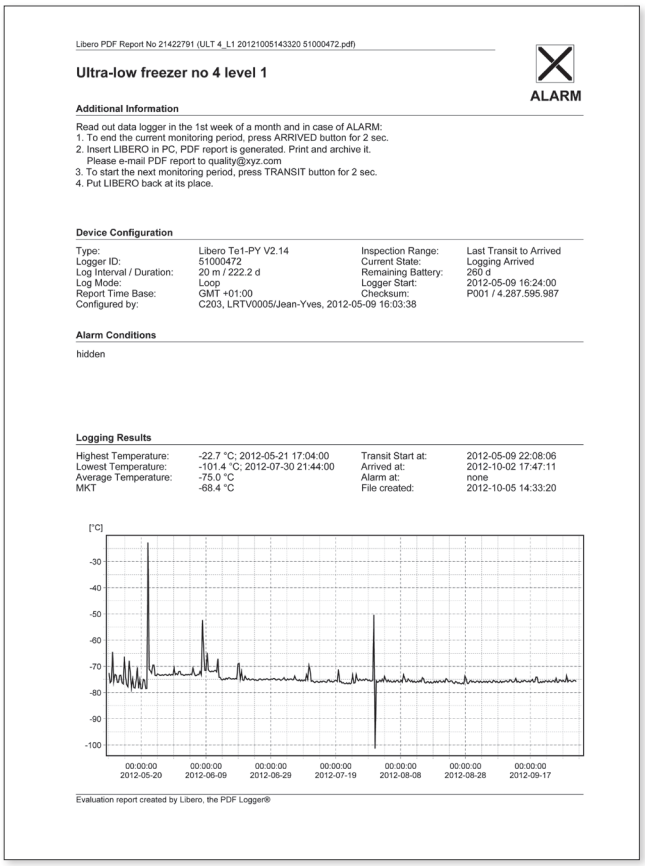
It's also worth noting that chart recorder technology is over 100 years old. New, modern technologies exist for monitoring that includes time stamped, point-by-point temperature data. The key to quality-based decision-making is data; however chart recorders can only provide the graph printout. A more robust temperature monitoring system would automatically collect and store temperature data in an electronic format, and would allow for alarm, analytics, and automatic archives.

So if handwritten and manual processes aren't the answer to safeguarding your data integrity practices, what kind of solution meets data integrity guidelines and also mitigates the chances of risk?

Independent Data Loggers

These loggers will collect temperature data and they normally include a built-in storage device. Data is time stamped, making it easier for data analysis. To retrieve data, they interface with a computer.

The upside to this solution is that data is collected and stored in an electronic format that is compliant with FDA 21 CFR Part 11. The downside is that the loggers have to be manually collected and connected with a computer to download data, which can be time consuming when there are many pieces of equipment.



Libero PDF Report No 21422791 (ULT 4_L1 20121005143320 51000472.pdf)

Ultra-low freezer no 4 level 1

ALARM

Additional Information

Read out data logger in the 1st week of a month and in case of ALARM:
1. To end the current monitoring period, press ARRIVED button for 2 sec.
2. Insert LIBERO in PC, PDF report is generated. Print and archive it.
   Please e-mail PDF report to quality@xyz.com
3. To start the next monitoring period, press TRANSIT button for 2 sec.
4. Put LIBERO back at its place.

Device Configuration

Type:	Libero Te1-PY V2.14	Inspection Range:	Last Transit to Arrived
Logger ID:	51000472	Current State:	Logging Arrived
Log Interval / Duration:	20 m / 222.2 d	Remaining Battery:	260 d
Log Mode:	Loop	Logger Start:	2012-05-09 16:24:00
Report Time Base:	GMT +01:00	Checksum:	P001 / 4.287.595.987
Configured by:	C203, LRTV0005/Jean-Yves, 2012-05-09 16:03:38		

Alarm Conditions

hidden

Logging Results

Highest Temperature:	-22.7 °C; 2012-05-21 17:04:00	Transit Start at:	2012-05-09 22:08:06
Lowest Temperature:	-101.4 °C; 2012-07-30 21:44:00	Arrived at:	2012-10-02 17:47:11
Average Temperature:	-75.0 °C	Alarm at:	none
MKT	-68.4 °C	File created:	2012-10-05 14:33:20

Evaluation report created by Libero, the PDF Logger®

Electronic records are far superior to handwritten records and chart readouts. This example of a data logger report shows device settings, high, low and average temperatures, and more.

Networked Data Loggers

A series of networked data loggers, sometimes known as a Central Monitoring System (CMS), will automatically collect temperature/environmental data and send the data to a central system on a computer or network, leaving the manual legwork out of the equation. Automatic archiving will ensure data is stored securely for future reference and meet data integrity guidelines

When 95 % of data integrity issues arise out of poor data management, then implementing a solution that is designed to intelligently manage data just makes sense.

for archive storage. For some organizations, the time saved from having dedicated technicians manually writing down temperature points or collecting and storing paper charts can add up to a significant cost savings.

Some networked systems provide analytical tools for reporting and statistics. Times / dates of temperature points allow for more in-depth data analysis. These systems are designed to send users a remote alarm notification in the event of an excursion so that action can be taken immediately. Some systems even allow for user-programmable alert notifications that can send notification of a problem before it happens. Systems may also allow you to query data, which is valuable during audits.

When 95 % of data integrity issues arise out of poor data management, then implementing a solution that is designed to intelligently manage data just makes sense.

A Checklist for Complying with New GxP Data Integrity Requirements

With so many networked data logging products on the market, how do you know which one to choose? When moving to an electronic method for monitoring, the key is traceability. It's not up to you to design a system that meets all of the data integrity guidelines – it's just up to you to find the right system that has been designed by experts in this field to meet these rigorous standards.

Use this checklist when searching for the right CMS for your needs:

Does the system include metadata?
Metadata is literally data about data. The FDA's draft guidance explains: «A data value is by itself meaningless without additional information about the data.» For example, the number 3 is meaningless without additional metadata, such as degrees in Celsius or Fahrenheit or date / timestamp for when the data was obtained.

Does the system offer an audit trail?
An audit trail is a critical component for any electronic system in GxP areas. You should never be able to manipulate or change data, and in the event that someone does try to change data, an audit trail should be enabled, which will work in the background to record all operations and events with user and time information captured – ensuring traceability. An audit trail is defined by the FDA as «a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record…the ‹who, what, where, when and why› of a record.» If your current system doesn't have an audit trail enabled, the MHRA guidelines state the expectation is for companies to have an integrated electronic system or validated audit software by 2017.

Will you own the data?

You should be able to keep the data throughout the entire lifecycle, and periodically review it. If you are considering a cloud or third-party storage service, consider in what format you will receive the data upon request. The data should be in its original format or a true copy. What happens if the system is down? The MHRA guideline states: «Where data and document retention is contracted to a third party, particular attention should be paid to understanding the ownership and retrieval of data held under this arrangement.» Guidelines also specify that you need to be able to access the data in a timely manner. This being said, the safest approach to temperature data storage is to have it stored on a redundant server. In terms of software type, the MHRA recommends a relational database because the «file structure is inherently more secure, as the data is held in a large file format which preserves the relationship between data and metadata.»

Can you assign user access / system administration roles?

It is critical to find a system that allows you to define user access rights. User access rights ensure that controls are in place against unauthorized changes. For example, when it comes to temperature monitoring, only certain individuals should be able to comment on or deactivate alarms. You must document the controls in place that activities are attributable to specific individuals. Depending on the size of your organization, it might be worth looking into a system that is sensor based, meaning you can assign access rights based on each sensor / monitoring point.

Can you validate the system?

All computerized systems need to comply with the requirements of EU GMP Annex 11 and GAMP5, and needs to be validated for its intended use and application. Ask the manufacturer if other GxP companies have validated the software in the past. This validation of software goes beyond a functional verification from the manufacturer – you must perform an installation, operation and performance qualification (IQ, OQ, PQ) to test the system and verify its operation. This will provide evidence that the software will perform as specified according to the manufacturer's specifications. This process can be timely, so it's also worth asking if the manufacturer can offer the software validation as a service after the installation.

Final Thoughts

As it relates to data integrity, the FDA suggests making a periodic risk-based assessment of your activities to help evaluate your existing policies and procedures. Try mapping your specific temperature monitoring workflows to identify areas of risk.

It's also important to note that risks change over time, so the same risks you had a couple years ago may not be the same as they are today, especially considering the new data integrity definitions and guidelines, and not to mention the increase in data integrity-focused audits. For example, perhaps five years ago you only had a couple pieces of equipment to monitor, and chart recorder monitoring posed very little risk to your operation. Now, with twenty pieces of equipment to monitor, the chance for human handling errors while processing these charts is greater. If you are still using paper or manual processes for your temperature monitoring activities, consider how an automated, computerized system will minimize data integrity risks and improve processes.

References

1. MHRA GMP Data Integrity Definitions and Guidance for Industry; Revision 1.1 and Final Release March 2015
2. World Health Organization Guidance on Good Data and Record Management Practice; Draft Release September 2015
3. U.S. Department of Health and Human Services Food and Drug Administration Data Integrity and Compliance with CGMP Guidance for Industry; Draft Release April 2016
4. NFS International – Data Integrity: The Fingerprint of a Company's Processes and Products; Webinar November 2015
5. FDA 21 CFR Part 11, Electronic Records; Electronic Signatures; Pharmaceutical CGMPS, August 2003
6. GAMP5: A Risk-Based Approach to Compliant GxP Computerized Systems; International Society for Pharmaceutical Engineering (ISPE), Updated 2008
7. European Commission: Annex 11 Computerized Systems; Volume 4 Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use