VAISALA

White Paper

www.vaisala.com

Managing GxP environmental systems to ensure data integrity

In this paper, we provide an overview of data management best practices for life science systems and an overview of regulatory expectations. We offer eight recommendations for establishing and maintaining good practices for data integrity.

More than Bytes and Signatures

As efforts to ensure the quality and safety of drugs increase, so does the amount of data generated by those efforts. Over the last few years, global regulatory scrutiny has turned to providing guidance on preserving the integrity of data. Throughout life science industries — pharmaceutical, medical devices, and biotechnology research and production — regulatory guidance and enforcement strategies are being re-evaluated with a focus on data integrity. With increasing awareness of data collection and storage, there comes increased awareness of gaps between industry practice and existing technology. Although there are new strategies available for data management, companies can find changes hard to implement in terms of updating systems and behavior.

Data integrity: Related regulations

Data integrity requirements are core elements of basic GMPs, and are broadly addressed in the FDA's Title 21 CFR Part 11 and the EU's GMP Eudralex Volume 4, Chapter 4 and Annex 11. However, with increasing automation based on computerized systems, as well as the globalization of operations and the increasing cost of bringing products to market, new guidance was needed to clarify regulatory expectations around the creation, handling, and storage of data.

Thanks to the publication of enforcement actions such as GMP non-compliance reports, warning letters, import alerts, and notices, it is evident that regulators are targeting data integrity failures during inspections. Subsequent enforcement actions have led to the withdrawal of supply across multiple markets, product recalls, consent decrees, and reputational damage for the firms involved. With increased targeting of data integrity from regulators, it is now crucial that everyone involved in GxP-regulated activities understand correct data management practices.

Principles and Practice

In essence, data integrity means that data collected and stored must be original, complete and traceable. Several regulatory agencies have defined the term "data integrity." In the UK, the Medicines and Healthcare products Regulatory Agency (MHRA) defined data integrity in their 2015 document: "MHRA GMP Data Integrity Definitions and Guidance for Industry" as the degree to which all collected data are "complete, consistent, accurate, trustworthy, reliable… throughout the data lifecycle."

For their 2016 draft guidance for industry "Data Integrity and Compliance with CGMP" 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)."

The acronym ALCOA is used by the FDA, MHRA, the World Health Organization and others to outline expectations on records, including paper-based, electronic, and hybrid records (systems that use both paper and electronic records). ALCOA is a useful guide to remembering key points of data management for GxP compliance. ALCOA stands for:

A = Attributable to the person generating the data
L = Legible and permanent
C = Contemporaneously recorded
O = Original or a true copy
A = Accurate

The WHO added some extra definitions to ALCOA in their working document "Guideline on data integrity" expanding the acronym to ALCOA+. In addition to original emphasis of ALCOA principles, the "+" highlights the importance of the attributes of being complete, consistent, enduring and available.*

Thus, *ALCOA+* is now the goal for every piece of GMP information – information that can impact the purity, efficacy, and safety of products. ALCOA+ is the standard by which data integrity is evaluated. In practice, this means that companies must maintain control over all intentional and unintentional changes to GMP data, including the prevention of data loss or corruption.

Data Management Challenges

Regardless of the methods used to gather and store data — manual, automatic, or a combination — there are always opportunities for failure. Manual processes entail obvious points of possible failure: operators can forget to record information, record incorrect values, lose records, or even intentionally falsify data. The risks associated with computerized systems are more technical. For both manual and automated methods, regulatory agencies have described the regulatory expectations in their guidelines and draft documents.

A review of enforcement actions proves that many companies are misinterpreting guidance documents. Other industry stakeholders try to help with more explicative documents. For example, the European Compliance Academy (ECA) published an article specifying data integrity failures that caused one company to receive an FDA Warning Letter. Observations included:

- Failure to exercise sufficient controls over computerized systems to prevent unauthorized access or changes to data, and to provide controls to prevent omission of data.
- The computerized system lacked access controls and audit trail capabilities.
- All employees had administrator rights and shared one user name.
- Electronic data could have been manipulated or deleted without traceability.
- Raw data were copied to a CD and then deleted from the hard drive. Data copied were selected manually without assurance that all raw data was copied before being permanently deleted.

Each of these deviations could have been addressed by systems and methods including:

- Unique usernames and passwords
- A durable and inerasable audit trail or event log
- Separate administrator and user access rights
- Good standard operating procedures (SOPs)
- Oversight and regular review of processes

** See also: WHO Technical Report 996, Annex 5, "Guidance on good data and record management practices"*

Key areas of data integrity control

There are seven functional areas consistently mentioned in regulations and guidance on data integrity. Here we review these key areas, focusing on how they apply to environmental monitoring applications.

Quality Risk Management[1]

- Understand the potential impact of all data on product quality and patient safety.
- Understand the basic technologies used in your data processes, and their inherent limitations.
- Implement systems that provide an acceptable state of control that is matched to risks and criticality of the process in question.
- Identify and document points of risk for unauthorized or untraceable deletion or amendment, as well as opportunities for detection through routine reviews.
- Schedule and perform periodic risk assessments as technology and processes change.
- Provide technology training to ensure existing technologies are used to their full potential.

Audits & Internal Inspections[3]

- Create detailed review processes for inspection findings, non-compliance reports, and Warning Letters.
- Perform routine in-house data audits, including: audit trails, raw data and metadata, and original records.
- Schedule regular review of system user access rights.
- Report audit results to senior management and other relevant stakeholders.

Personnel[2]

- Document and communicate roles and responsibilities.
- Provide technical support for systems administration.
- Assign responsibility for data throughout its entire lifecycle.
- Encourage a workplace culture that supports issue reporting.
- Implement systems that can identify and minimize potential risks.
- Create behavioral controls for personnel, procedural controls for processes, and technical controls for technologies.
- Analyze the root causes of compliance failures in order to fix them systemically.
- Authorize appropriate access privileges for each system.

Training

- Provide regular training, and document training completion including personnel identities and dates.
- Ensure training is matched to different roles involved with data - including quality assurance, quality control, production and management - with an emphasis on Good Documentation Practices.
- Store training documentation where it is easily retrievable by those involved with regulatory and 3rd party inspections.

Documentation

- Implement and require Good Documentation Practice (GDocP) in all written documents and SOPs.
- Follow relevant regulations when creating and reviewing documents. For example, CFR Title 21, Part 211 "Current Good Manufacturing Practice for Finished Pharmaceuticals" Subpart J - Records & Reports.

Data Life Cycle

- Implement change management and control of incidents and deviations.
- Ensure corrective and preventive action (CAPA) processes and procedures.

Vendors/Providers

- Ensure providers have qualified and trained personnel.
- Review providers' quality management systems.
- Note compliance to standards such as ISO 9001, or ISO 17025.
- Perform regular checks of providers' systems and services; audit where necessary and/or allowable.
- Review contracts, technical agreements, and quality agreements.

[1] A key document in this area is ICH Q9. This guideline from the ICH Expert Working Group provides a methodology for a risk-based approach to data management, including recommendations.

[2] Personnel management directs and controls how companies function to achieve business goals. Focusing on personnel ensures that resources are allocated to the functions that support recommended practices and promotes accountability among all levels of management and staff.

[3] If a hybrid system is in use (both paper and electronic data are generated), the original data should also be checked routinely in addition to trend data, reported documents, or PDF files.

Eight Ways to Ensure Data Integrity in monitoring systems

The following recommendations give an overview of how to maintain data integrity for computerized systems.

Perform Risk-based Validation

- Validate only systems that are part of GxP-compliance. Ensure protocols address data quality and reliability.
- In some cases, it's cost-effective to have the system vendor perform qualification and validation of the systems. To help decide between in-house or purchased validation service, use the ISPE's GAMP5 (Good Automated Manufacturing Practice) categorizations to determine the validation complexity of your system.
- Account for all electronic data storage locations, including printouts and PDF reports during validation.
- Ensure your quality management system defines the frequency, roles and responsibilities in system validation.
- Your validation master plan must outline the approach you will use to review meangingful metadata, including audit trails, etc.
- Your validation master plan should require periodic re-evaluations of every validated system.

Change Control

- Ensure system software updates are designed to comply with changing regulations, especially when implementing new features.
- Collaborate with providers to stay informed about changes and update your systems accordingly.
- Select systems that are easy to update and validate upon the addition of new hardware or other system inputs.

Audit your Audit Trails

- An audit trail must be an inerasable record of all changes made to data in a system. To be useful in GxP compliance an audit trail must answer: Who? What? When? And Why?
- Define the data relevant to GxP and ensure any changes to this data will be recorded by an audit trail.
- Assign roles and schedules for testing the audit trail functionality.
- The depth and frequency of an audit trail review should be based on the complexity of the system and its intended use.
- Understand what audit trails comprise: discrete event logs, history files, database queries, reports or other mechanisms that display events related to the system, electronic records or raw data contained within the record.

Select Appropriate System and Service Providers

- Ensure your providers are familiar and fluent with the relevant regulations.*
- Systems must be fit-for-purpose. Compare your User Requirements to system Functional Specifications prior to acquisition to prove the suitability of a candidate software for any GxP application.
- Learn about your suppliers' organizational culture and maturity relating to quality and data management. Ask what systems are in place to ensure data integrity and audit those systems if possible.

Qualify IT & Validate Systems

- Validated systems require an IT environment that has been fully qualified.

Plan for Business Continuity

- Ensure disaster recovery planning is in place.
- Your plan should state how quickly functions can be restored, as well as the probable impact of any data lost.
- Look for software and systems that can record and store data redundantly to protect it from loss during power outages or network downtime.
- Employ solutions such as UPS (Uninterrupted Power Source), battery-powered, standalone recorders or devices that can switch to an alternate power source when required. E.g. data loggers that can also be battery powered.

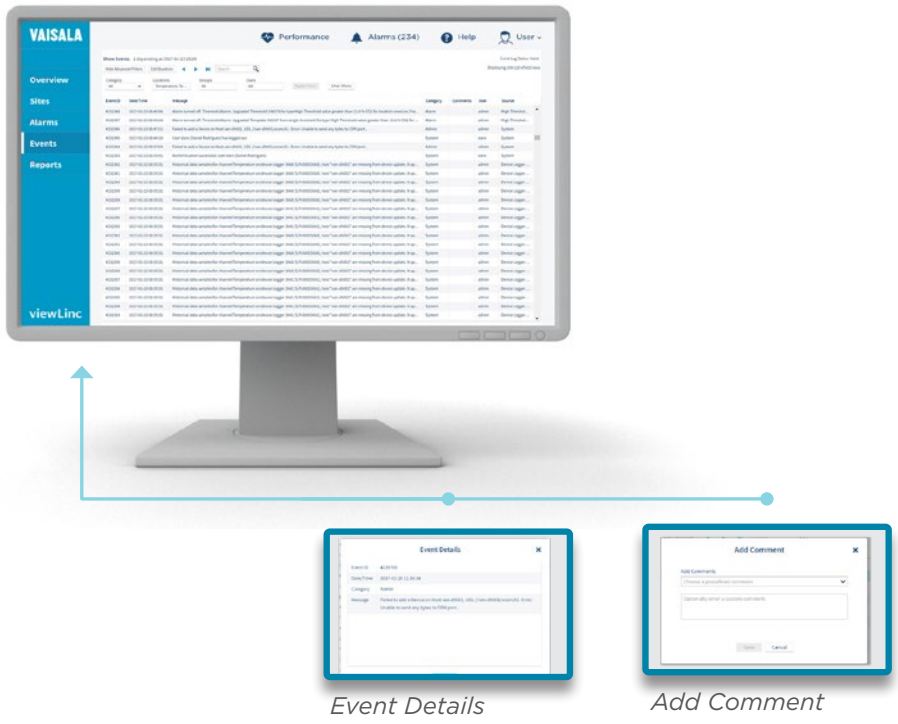
Be Accurate

- Verify system inputs. For example, an environmental monitoring system requires regularly calibrated sensors.
- For networked systems, test that data are coming from the correct location.
- Select systems that provide alarm messages in case of communication failure, device problems, or data tampering.

Archive Regularly

- Backup and save electronic data, including metadata, to a secure location on a regular schedule.
- Verify relevant GxP Data can be readily retrieved during internal audits.
- Electronic archives should be validated, secured and maintained in a state of control throughout the data life cycle.

** See also: EU GMP EudraLex Annex 15, Section 2, Documentation including VMP 2.6: "Where validation protocols and other documentation are supplied by a third party providing validation services, appropriate personnel at the manufacturing site should confirm suitability and compliance with internal procedures before approval."*



Event Details *Add Comment*

Monitoring software should show all events within the system, including: threshold and device alarms, messages sent (Emails or SMS), User login/out, automated report generation, devices added, etc.

Data Integrity in Environmental Monitoring

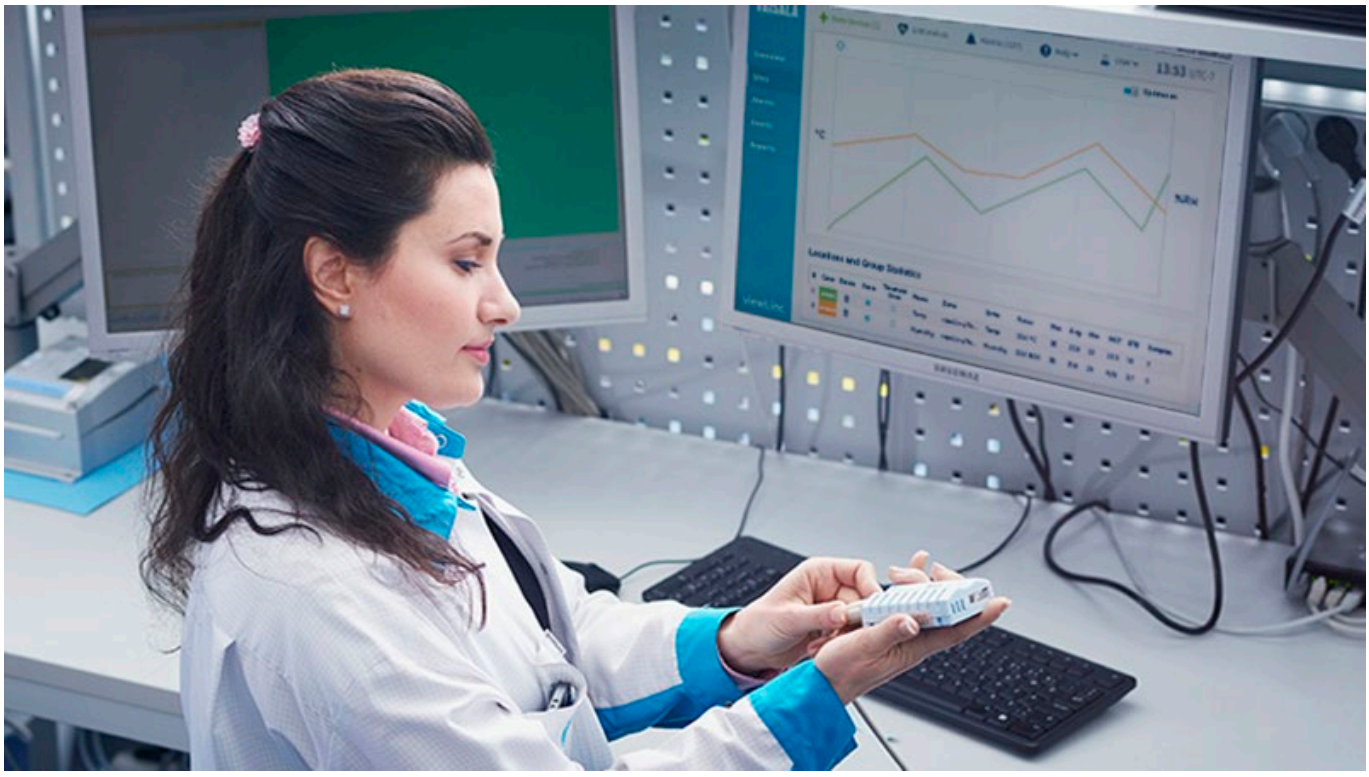
Vaisala understands the diligence and attention that is required to ensure data integrity. As a manufacturer of environmental measurement and monitoring systems used in GxP applications, our customers turn to us for assistance to protect their data. Vaisala is invested in understanding the relationship between computerized systems, network functionality, device efficacy and data integrity. We continuously develop our system software with the goal of ensuring data integrity for our customers. Here we outline several features of viewLinc that guarantee reliable, complete, and accurate data.

New Generation, Same Data Integrity

Vaisala's proprietary VaiNet wireless technology is a wireless device connectivity option for the viewLinc Continuous Monitoring System. The VaiNet data loggers system include several security features, which are designed to ensure data integrity in GxP-regulated applications. VaiNet provides secure connectivity between data loggers and access points with a licensed ISM (Industrial, Scientific and Medical) protocol. With radio band frequencies that vary depending on global location, VaiNet relieves already overburdened Wi-Fi networks that are often difficult to secure. Vaisala used the LoRa™ modulation technique to create wireless data loggers with wired reliability. VaiNet's highly modulated CSS (Chirp Spread Spectrum) signal achieves ranges of 100 meters or more in typical manufacturing environments. The unique modulation is highly reliable, yet requires less power for data transmission. The result is a long-range signal that is readable only by Vaisala network access devices within a VaiNet network, and superior protection of data integrity.

viewLinc & VaiNet Features

- Access to the system is controlled by individual login IDs, user names and passwords.
- User-specific rights and access control permissions create different authority levels, fulfilling the regulatory requirement for segregation of duties.
- viewLinc includes device checks to guarantee the origin of the data and validation alarms to guarantee the validity of data.
- Only viewLinc, not users, can create data records, and these are uneditable and inerasable.
- Creation and modification of data and system parameters is recorded by an audit trail shown in viewLinc's "Event" view.
- Calibration data is stored in each device, and in the software, ensuring accuracy specifications of devices are also tracked.
- Reports are created in secured PDF files that cannot be modified.
- All graphs, system reports and environmental reports are easy to read, fulfilling the requirement of human readable copies of data.
- All measurements are synchronized against the system server clock so it's easy to compare data sets across time zones.
- The viewLinc software can be used in multiple time zones simultaneously without compromising the data because all records are based on UTC (Coordinated Universal Time).
- Thorough system documentation helps with qualification, validation and future usage of the system (User Requirement Specification, Functional Specification, Design Qualification, Traceability Matrix, Risk Assessment, Validation Protocols and Reports).
- Metadata is easy to find and provides contextual information on all data.



Two additional security features further enhance data integrity: data encryption and data authentication. Data encryption means that specific code is required to read and understand transmitted information. In VaiNet, the original data is transmitted between data loggers and the network access point (VaiNet AP10) and cannot be intercepted by a non-VaiNet device. Data loggers encrypt the data before transmission, and only the access point can decrypt this data. Encryption is performed with proven AES-128 technology (AES = Advanced Encryption Standard) and data authentication uses CMAC technology (Cipher-based Message Authentication Code). Authentication ensures that data is coming from the correct source and the origin of the sent message is always identified and tracked.

Data integrity by design

Risks to data integrity are reduced by implementing correct data management practices that include behavioral, procedural, and technological controls. In environmental monitoring applications, there are common scenarios that entail expensive risks: an undetected compressor failure could destroy the entire contents of a fridge or freezer. These chambers may be storing irreplaceable samples from research in a crucial stage of development. If the monitoring system includes remote alarming, the costs of an equipment or process failure are mitigated. Even when equipment failure is not immediately catastrophic, accurate and reliable data is sent in an alert through email or SMS will indicate a problem.

Data integrity is about more than compliance with regulations; it is about protecting research and products for human use. In GxP applications, data often represents a significant investment in development, clinical trials, donated tissue, and the hopes of patients for a new therapy or drug. The data represent assets that require fail-safe, trustworthy systems and practices that ensure product safety. The devices, software, infrastructure, processes, and operating procedures must all be aligned to ensure that data are complete, consistent, accurate, and exemplifying the characteristics of ALCOA+.

To learn more, see our webinar on data integrity.

VAISALA

Please contact us at
www.vaisala.com/contactus

www.vaisala.com

Scan the code for more information