Managing GxP Environmental Systems to Ensure Data Integrity

In this paper, we provide some history of data management for life science systems and an overview of new regulatory expectations, including changes to guidance. We then 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. As a result, global regulatory scrutiny over the last few years has turned to providing guidance on preserving data quality. Throughout the life science industries — pharmaceutical research, manufacturing, medical devices and biotechnology — guidance and regulatory enforcement strategies are being re-evaluated with a focus on data integrity. With increasing awareness among inspectorates of problems inherent to data collection and storage, there comes increased awareness of gaps between industry practice and existing technology. Although there are solutions and control strategies available for compliant data management, pharmaceutical companies can find change hard to achieve, both in terms of updating systems and behavior.

Enforcement Action on Data

Data integrity requirements have been addressed in the FDA's Title 21 CFR Part 11 and the EU's GMP Eudralex Volume 4, Chapter 4 and Annex 11. This is so far unchanged. 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's 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

Data integrity means that all data collected and stored must be correct, traceable and reliable. 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 extent to which all collected data are "complete, consistent and accurate throughout the data lifecycle."

For their 2016 draft guidance for industry "Data Integrity and Compliance with CGMP" the FDA defines it 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

Full documents: MHRA GMP Data Integrity Definitions and Guidance for Industry and Data Integrity and Compliance with CGMP**

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

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 document "WHO Technical Report Series 996 Annex 5*, Guidance on good data and record management practices" expanding the acronym to *ALCOA+*. In addition to original emphasis of ALCOA principles, the "+" includes the attributes of being complete, consistent, enduring and available.

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

Data Management Challenges

Regardless of the methods of gathering and storing data — manual, automatic or a combination — there are 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 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.

*Full document: WHO Technical Report Series 996 Annex 5, Guidance on good data and record management practices**

However, a review of enforcement actions proves that many companies are misinterpreting guidance. Other industry stakeholders try to help with more explicative documents. For instance, the European Compliance Academy (ECA) published an article specifying data integrity failures that caused one German 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
- An inerasable audit trail or event log
- Separate administrator and user access rights
- Good standard operating procedures (SOPs)
- Oversight and regular review of processes

** See references at the end of this paper for links to sources.*

From Principles to Practicable

There are seven functions and knowledge areas touched upon consistently in regulations and guidance on data integrity. Here we review these key areas, focusing on how they are applied 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 process criticality and risks.
- Identify and document points of risk for unauthorized deletion or amendment, as well as opportunities for detection through routine reviews.
- Schedule and perform periodic risk assessments.
- Provide training to ensure you are using existing technologies to their full potential.

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.
- Reward proper conduct and analyze the root causes of compliance failures in order to fix them systemically.
- Authorize individuals and grant appropriate privileges for each system.

Documentation

- Implement Good documentation practice (GdocP) in all written documents and SOPs.
- Refer to relevant regulations when creating and reviewing documents. For example, CFR Title 21, Part 211 "Current Good Manufacturing Practice for Finished Pharmaceuticals" Subpart J - Records and Reports.

Data Life Cycle

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

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 spot-checks of system user access rights.
- Report audit results to senior management and other relevant stakeholders.

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.
- Store training documentation where it is quickly retrievable by those involved with regulatory and 3rd party inspections.

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, 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.* *See references at the end of this paper for links to sources.*

[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] *For the recommendation to review original records an example is germane. 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.*

Data Management Tools: Eight Ways to Ensure Data Integrity

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.
- Schedule periodic re-evaluations after your initial validation.

Select Appropriate System and Service Providers

- Ensure your providers are fluent with the relevant regulations.*
- Systems must be fit-for-purpose. Get proof of a software's efficacy for the application it will be used in.
- Learn about your suppliers' organizational culture and maturity relating to data management. Ask them what systems are in place to ensure data integrity and audit those systems if possible.

Audit your Audit Trails

- An audit trail must be an inerasable record of all data in a system, including any changes that have been made to a database or file. To be useful in GxP compliance an audit trail must answer: Who? What? When? And Why?
- Define the data relevant to GxP and ensure it's included in an audit trail.
- Assign roles and schedules for testing the audit trail functionality.
- The depth 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.

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 upon the addition of new hardware or other system inputs.

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 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.

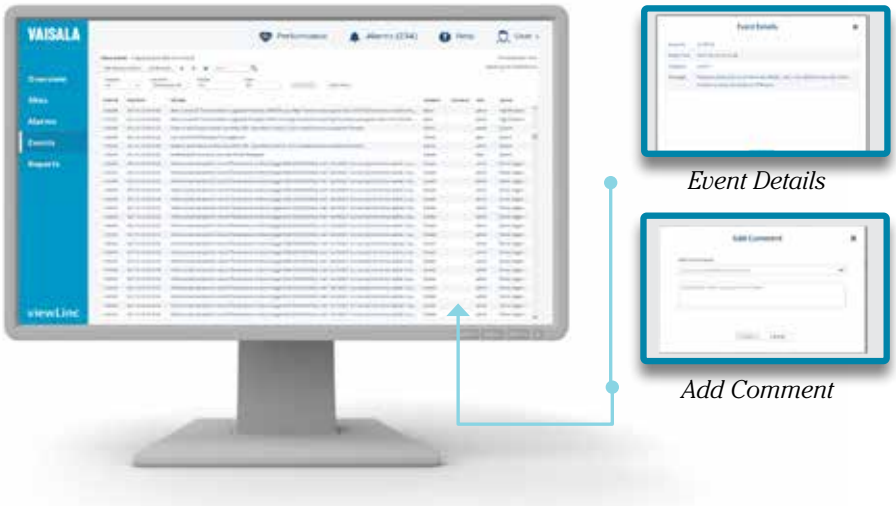
Be Accurate

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

Archive Regularly

- Backup and save electronic data on a pre-set schedule and to a secure location, including metadata.
- Verify the retrieval of all of data during internal audits.
- Electronic archives should be validated, secured and maintained in a state of control throughout the data life cycle.

** See EU GMP EudraLex Annex 15: "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."*



viewLinc shows all events within the system, including: threshold and device alarms, messages sent (Emails or SMS), User login/out, automated report generation, devices added, and more…

Data Integrity in Environmental Monitoring

As a manufacturer of environmental measurement and monitoring systems, Vaisala is invested in understanding the relationship between computerized systems, network functionality, device efficacy and data integrity. Over the past decade we've continuously developed our monitoring system software with the goal of ensuring data integrity. 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 recent addition to the viewLinc system and includes all of Vaisala's current data loggers' security features, which are designed for GxP-regulated applications. However, the VaiNet technology assures secure connectivity between loggers and access points with a specially licensed ISM (Industrial, Scientific and Medical) protocol. With radio band variants of 868 MHz and 915 MHz depending on global location, VaiNet allows monitoring devices to transmit independently of over-crowded Wi-Fi networks. Vaisala licensed Semtech's LoRa™ (Long Range) modulation technique to create a device that operates wirelessly with wired-equivalent data recording. VaiNet uses a modulated version of CSS technology (Chirp Spread Spectrum) to achieve ranges 100 meters or more in typical warehouses based on wideband, noise-like signals that are highly reliable, yet require less power for data transmission.

The result is a long-range signal that is readable only by Vaisala devices within a VaiNet network. 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 AP) 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.

** See Application Note and webinar*

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.
- Acquisition, changes, modifications, and deletion of data are 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's server clock so it's easy to compare data sets.
- 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, Traceability Matrix, Risk Assessment, validation documentation and reports).
- Metadata is easy to find and provides contextual information on all data.

Conclusion

By implementing correct data management practices that include behavioral, procedural and technological controls, the risks of flawed, incomplete or erroneous data are mitigated. For many viewLinc users in GxP-regulated applications there are common scenarios that entail expensive risks. An undetected compressor failure overnight or on a weekend 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. With an automated monitoring system in place, the assets are safeguarded. Even when equipment failure is not immediately catastrophic, accurate and reliable data sent in an alert through email or SMS will indicate that a problem is imminent.

Data integrity is about more than compliance with regulations; it's about protecting life-saving research and products for human use. In GxP applications, data often represents significant investments 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 patient 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+.

References and Further Reading

- EU GMP EudraLex Volume 4, Annex 11: Computerized Systems (2011)
- EU GMP EudraLex Volume 4, Annex 15: Qualification and Validation (2015)
- EU GMP Eudralex Volume 4, Chapter 4. Documentation (2011)
- European Compliance Academy (ECA), GMP News 22/06/2016, German Company receives FDA Warning Letter for Data Integrity Issues
- FDA 21 CFR Part 11, Electronic records, electronic signatures (1997)
- FDA Draft Guidance, Data Integrity and Compliance with CGMP, Guidance for Industry (April 2016)
- ICH Q9, ICH Harmonized Tripartite Guideline, Quality Risk Management, 9 November 2005
- ISPE GAMP 5. A Risk-Based Approach to Compliant Computerized Systems (2008)
- MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015
- MHRA GxP Data Integrity Definitions and Guidance for Industry, Draft version for consultation, July 2016
- PIC/S, Draft Guidance, PI 041-1 (Draft 2), Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments. 10 August 2016
- WHO Technical Report Series 996 Annex 5, Guidance on good data and record management practices (May 2016)

To learn more about data integrity in your controlled environments, see our webinar on this topic:

Vaisala.com/webinar-central/data-integrity-for-pharma

About the Author: *Piritta Maunu brings many years in biotechnology to her role as a Life Science Industry Expert in Vaisala. She has worked in quality management, R&D and GMP production. Piritta holds a M.Sc. in Cell Biology and is an instructor of General Biology.*

VAISALA

Please contact us at
www.vaisala.com/requestinfo

Scan the code for more information

www.vaisala.com