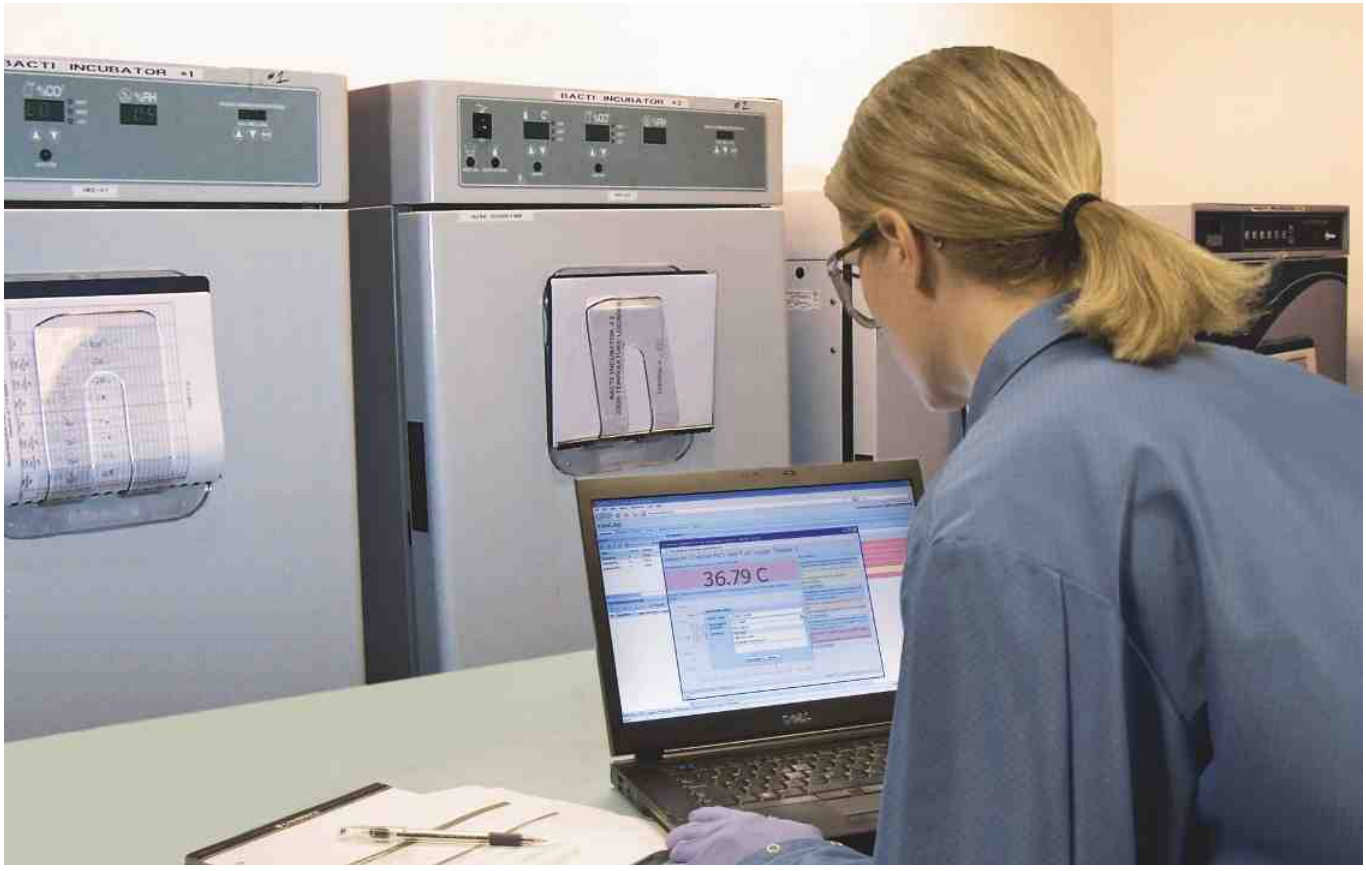
VAISALA / WHITE PAPER

How the Vaisala Continuous Monitoring System Aids Compliance with Title 21 CFR Part 11 and EU GMP Annex 11



Introduction

Two crucial regulatory guidelines that describe the proper use of computerised systems to perform GMP-related activities are the Food and Drug Administration's Title 21 CFR Part 11 and the EU GMP "Annex 11: Computerised Systems" published by the European Commission as part of EudraLex. This white paper analyses the requirements of Part 11 and Annex 11 as they apply to environmental monitoring and validation, and outlines how Vaisala's Continuous Monitoring System software viewLinc helps firms meet the requirements of both.

Scope & Principles

The geographical reach of 21 CFR Part 11 and Annex 11 is as follows: Part 11 applies to manufacturers who seek the FDA's market approval to sell pharmaceuticals, biologics, nutraceuticals, and medical devices within the United States. Meanwhile, Annex 11 applies to manufacturing operations wishing to distribute the same products within the European Union. Both Part 11 and Annex 11 outline broad technical and procedural controls that can be used in creating and storing electronic data used in GMP-mandated records. Annex 11 is one of nineteen supplementary requirements of the EU GMP guide. The revisions to Annex 11 from 2011 align the EU GMPs with the quality guidelines Q8-10 (published by the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use). These changes are reflected within this white paper.

Part 11 applies to the creation, modification, archival, retrieval, and transmission of any electronic records necessitated by the FDA's predicate rules. Annex 11 is a little broader in that it addresses the principles and proper use of computer systems used to execute GMP-required tasks. 21 CFR Part 11 states that the FDA's view is that the risks of falsification, misinterpretation, and change (without leaving evidence) within the GMP-environment are greater with electronic records than paper records, and therefore specific controls are required. By comparison, Annex 11 alludes more broadly to the automation of processes with computerised systems. The concern of both Part 11 and Annex 11 is to reduce any risks to product quality that could result from automation within manufacturing environments.

According to 21 CFR Part 11, Subpart A Section 11.1 – Scope:

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and written signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.[1]

The scope of Part 11 encompasses any electronic record that has been created in compliance with FDA regulations. Part 11 also applies to electronic records submitted to the agency in accordance with the Federal Food, Drug, and Cosmetic and the Public Health Service Acts. Applicable within this scope are "… such records [that] are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means."[2] This means that, while documents must comply with Part 11, they need not be specifically listed in any GMP regulation or guidance. If the record exists first in paper format, it is not considered an "electronic document." The transmission of the paper version electronically, by email in a scanned copy or a PDF, does not supersede the paper record, or render it "electronic."[3]

A key difference between 21 CFR Part 11 and Annex 11 is that most of Part 11 is about electronic records and electronic signatures (ERES) and Annex 11 does not address electronic signatures in detail.

Instead, Annex 11 concerns computerised systems, including software and hardware components that combine to perform a function in a GMP environment. Such applications should be validated through qualification processes. Additionally, Annex 11 stipulates that computerised systems that replace manual operations should not result in any decrease in product quality, process control, or quality assurance. Nor should there be an increase of risk in a process where computerised systems are used.[4]

The Vaisala CMS software viewLinc is a "hybrid system", because it uses electronic records with the expectation that when a signature is required, the record will be printed and signed. Records printed from viewLinc are generated in a PDF so that they can be imported to a system designed to implement electronic signatures. Since viewLinc does not use electronic signatures, they will not be discussed in this paper.

The environmental data collected by viewLinc are stored as electronic records that can then be used to prove that regulated products have been stored within the correct ranges of multiple environmental parameters (i.e. temperature, humidity, CO_2, differential pressure, etc.).

It should be noted that although viewLinc software helps users meet the requirements of both 21 CFR Part 11 and Annex 11, the ultimate responsibility for compliance rests with persons responsible for the content of electronic records and with those responsible for the use of computerised systems. Similarly, the responsibility for compliance with the requirements of paper records lies with those responsible for the records' content.

Regulatory Inspections

Both Part 11 and Annex 11 stipulate that systems and components used to create electronic records must be available for regulatory inspection. Under Part 11, "Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection." Likewise in Annex 11: "Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request."[5]

In application this means that the electronic records generated by viewLinc must be backed up and maintained, as with any automated system. To ensure that no historical data is lost when system users update viewLinc, Vaisala maintains compatibility with preceding versions of the software. However, we suggest that as a best practice, firms archive a copy of the version used to create the electronic records as a backup reference.

System Controls & Security I

Annex 11

Under Annex 11 there are three sections that focus on system controls and security. Essentially, data integrity is part of risk management and as such, controls designed to ensure correct data must be in place. Controls include: built-in data checks (within the software and/or with a manual procedure) and permission-based user access to designated personnel only. In the terminology of Annex 11, Vaisala's CMS software viewLinc constitutes an application installed on a system owner's platform, making Vaisala a "third party provider of commercially available software."

In addressing the security features and procedures that make a commercially available software compatible with the requirements of Annex 11, the EMA takes a risk-based approach and expects firms to weigh both data integrity and system security in terms of any risks associated with a process executed by a computerised system. The following sections from Annex 11 illustrate the balance that must be found between efforts expended to ensure system controls are in place and the level of risk a particular system is meant to mitigate.

> "Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks…
>
> "Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons…
>
> "The extent of security controls depends on the criticality of the computerised system."[6]

In Annex 11, the security of the system, the data, and the access control of operators is addressed in the following passages:

> "Data should only be entered or amended by persons authorised to do so. There should be a defined procedure for the issue, cancellation, and alteration of authorisation to enter and amend data, including the changing of personal passwords.
>
> "When critical data are being entered manually …there should be an additional check on the accuracy of the record which is made.

> "The system should record the identity of operators entering or confirming critical data...
>
> "Any alteration to an entry of critical data should be authorised and recorded with the reason for the change. Consideration should be given to building into the system the creation of a complete record of all entries and amendments (an "audit trail")."[7]

In alignment with these guidelines, the viewLinc CMS software produces files in a proprietary format using a checksum technique to detect invalid or altered records. In addition, the software employs several layers of access control, including Windows OS built-in authentication. All data recorded by devices that connect to viewLinc are captured in the data logger file. Users who are granted a level of access by a system administrator can never disable or modify the content, or the way data is written to the electronic record. Once the data is recorded by the device (and during recording), files cannot be edited or deleted. In addition, any changes made to data logger operating parameters in the middle of a recording session results in the creation of a completely new electronic record.

System Controls & Security II

21 CFR Part 11

For 21 CFR Part 11, data security is partly addressed in the sections that outline what the FDA refers to as "closed systems" and "open systems." The term closed system has different meanings in different contexts. For the purposes of Part 11, a closed system is "an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system." The viewLinc software is a "closed system" because data files cannot be modified under any circumstances and only authorized persons can gain access to the system. All files created by viewLinc are secure and any attempts to change a file would be recorded by the system's audit trail, which captures all interactions with the system, including the clearing of the memory in a recording device.

According to Part 11, Subpart B "Section 11.10 Controls for closed systems" procedures and controls must be in place to ensure the "authenticity, integrity, and, when appropriate, the confidentiality of electronic records." Records need to be protected from retraction or falsification. Controls can include:

- System validation to indicate expected function
- The ability to generate complete copies
- Record protection for retrieval purposes
- Limited access to records
- Time-stamped audit trails that are unmodifiable and available for review
- Sequential recording that is linear, unmodifiable, and complete
- Authority checks on access and signatures
- Tamper-proof devices to ensure data validity

- Proper training of personnel involved in Part11 tasks
- Written policies that include responsible individuals who use electronic signatures.

In addition to these examples of controls for closed systems, there must be controls over system documentation that include record distribution, the use of the system's operational documentation, and change control procedures.

Within viewLinc, copies of data recorded by sensor-equipped devices are made available by copying the raw data files or by setting up a "PDF printer" to export graphs into PDF (this requires Adobe Acrobat or a similar Portable Document Format printer). Because viewLinc is a hybrid system, the electronic records it generates must be printed and signed. The *records* are electronic, but the *signature* is manual (hence the term "hybrid"). Records are protected for retrieval with viewLinc's reporting and exporting functions and the software does not allow modification of records under any circumstances, by any individual, authorized or not, including step sequences taken by a user.

Access to records is limited by the software's access control, which as already stated, uses the built-in authentication method of Windows OS.

Audit Trails

In response to Part 11's requirement for sequential recording, viewLinc creates an audit trail comprising all data logged in the CMS devices. The system applies a checksum function to all files generated by the system to ensure data integrity. In addition, any changes made to a data logger's operating parameters while it is active results in the creation of a completely new electronic record.

Each CMS device (i.e.: data logger, transmitter) holds electronic data in non-volatile EEPROM memory. Once data has transmitted from the device to the software, the media it is stored on, the backup strategy, and retrieval procedures are the responsibility of the system's users.

The Vaisala CMS is an off-the-shelf commercial system based on the creation of secure database files that cannot be modified without rendering the database completely unusable. Its devices are also

physically tamper-resistant. The software follows a proprietary protocol for communicating with its devices and positively identifies each device, determining the integrity of the data as part of its process. Additionally, historical files are encrypted.

Validation

Part 11

Guidance surrounding validation is contained in both 21 CFR Part 11 and Annex 11, ("Section 11.10 Controls for closed systems", and "Project Phase, Validation", respectively). As with any validation procedure, the intent is to show that a system performs as expected. The FDA considers validation a procedural control to ensure that a closed system can create accurate records, with confidentiality when required by GMP.

> "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."[8]

In its document titled: "Part 11, Electronic Records; Electronic Signatures – Scope and Application"[9] the FDA outlines its enforcement strategy regarding validation under Part 11 and suggests that the predicate rule requirements guide firms' decisions on the extent of their validation efforts.[10] Basically, the effect that a system has on a firm's ability to meet the requirements of GMP should correlate to the validation of that system. As with all data germane to predicate rule requirements, the "accuracy, reliability, integrity, availability, and authenticity" of the records should be verified according not only to the rule, but also to the demands and parameters of your application. We recommend a risk assessment document that can serve as justification for the scope and depth of validation procedures.

Annex 11

Annex 11 guidance refers more specifically to validation in its section "Project Phase, Validation."[11] This section outlines validation expectations including the life cycle of validation documents, change control records, deviation reports, GMP-related system inventories, User Requirements Specifications (URS), risk assessment, quality management systems, supplier assessment, test environments and data integrity through migration processes. The scope of Annex 11's validation guidance exceeds that of Part 11 in its inclusion of IT infrastructure as an element requiring qualification.[12] Further, validation must conform to Operation Qualification standards and be performed in the environment in which the system will be used. This means that system providers cannot offer pre-validated systems, but can perform installation and operation qualifications once the system is installed.

Validating Vaisala's CMS

Although validation, along with all other system operational procedures, is the responsibility of the firm, Vaisala offers validation protocols including Installation (IQ) and Operation Qualification (OQ). These documents contain detailed protocols for testing the functions of the viewLinc software and include columns for those executing protocols to signify success or failure and to note any deviations observed.

A Vaisala validation technician can perform the IQ/OQ execution on Vaisala's CMS. We can also perform a mapping study of your environment in selected regions. For information, refer to:

www.vaisala.com/en/lifescience/serviceandsupport/Pages/default.aspx

Personnel

Part 11

21 CFR Part 11 contains less guidance than Annex 11 on who is qualified to use GMP-related systems. In Part 11, the authorized persons are defined by the context; that is, the system they use rather than their role in the firm. In "Definitions" the access of personnel to a system, in addition to their responsibility for the content of that system's electronic records, defines a Closed system. In the same section "Open systems" are described as those which do not necessarily have access control by personnel responsible for the content of electronic records.[13] However, both Open and Closed systems must employ procedures to ensure "the authenticity, integrity, and, as appropriate, the confidentiality of electronic records."

Under "Controls for Closed Systems" we find guidance to ensure that personnel have the requisite skill and access to perform GxP-related tasks with a system, stating that "procedures and controls shall include the following:

(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.

(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."[14]

Annex 11

Annex 11 lists examples of relevant personnel: "Process Owner, System Owner, Qualified Persons and IT."[15] Similar to Part 11, Annex 11 also requires adequate training and access controls mediated by system administrators.

Vaisala CMS Access Control & Training

The viewLinc software contains ten levels of rights that determine what data a qualified person can see and what software functions they can use. The system administrator(s) also define access controls at the level of the locations being monitored. Vaisala offers remote and onsite training for system users and administrators to aid in proper system deployment and use.

Conclusion

Part 11 and Annex 11 were both introduced to address the key differences between computerised and manual systems and to make electronic records equivalent to paper records as evidence of the proper execution of GMP-related tasks. Today, most environmental monitoring systems used in GxP compliant firms are inherently aligned with the requirements of both the "Elevens." However, the risk of non-compliance with regulatory guidance comes not from the systems themselves, but in how they are implemented, used, and maintained.

Both Part 11 and Annex 11 provide broad guidance for and approaches to risk-based management of records created with computerised systems. In response to the requirements of both, Vaisala's CMS software viewLinc allows firms to achieve compliance with comprehensive validation protocols, multiple layers of security, fail-safe audit trail capabilities and a system designed for regulated environments.

References

1. See 21 CFR Part 11, “General Provisions, Sec. 11.1 Scope”, http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.1
2. Ibid.
3. Ibid. See: (b) under Scope: “However, this part does not apply to paper records that are, or have been, transmitted by electronic means.”
4. See Annex 11 “Principle”: http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf
5. Ibid. See Suppliers and Service Providers (3.4)
6. Ibid. See Data (5), Security (12.1), and (12.2)
7. See Annex 11, Eudralex Volume 4, from the European Commission DGIII-E-3 (1998) http://ec.europa.eu/health/files/eudralex/vol-4/pdfs-en/anx11_en.pdf
8. See 21 CFR Part 11, Subpart B – Electronic Records, Sec. 11.10 Controls for closed systems http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11&showFR=1
9. “Part 11, Electronic Records; Electronic Signatures – Scope and Application” http://www.fda.gov/regulatoryinformation/guidances/ucm125067.htm
10. The Agency provides further validation guidance in sections 4.8 and 4.10 of this document: “General Principles of Software Validation; Final Guidance for Industry and FDA Staff” http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085281.htm
11. See Annex 11, “Project Phase, 4. Validation” http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf
12. Ibid. “Principle”
13. 21 CFR Part 11 “Sec. 11.3 Definitions” http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11&showFR=1
14. Ibid. “Sec. 11.10 Controls for Closed systems”
15. See Annex 11, “General, 2. Personnel” http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf