21CFR Part 11 Demystified

MILLROCK TECHNOLOGY

Introduction

Do you produce an FDA regulated product? Do you use computerized systems to generate batch records? Do you submit data to the FDA in electronic formats? If so, you may have to comply with federal regulation 21CFR Part 11.

Technology has made a huge impact on every aspect of our lives making data and information increasingly accessible. With such advancements in information technology, the ability to access and manipulate data or electronic records, intentionally or unintentionally, has become a concern. Recognizing the issue, the FDA has developed and adopted regulations that address the need to manage and control electronic records for FDA regulated products. The standard is described in 21CFR part 11.

While this regulation has been made official for over two decades now, the FDA is starting to increasingly enforce the regulation and perform audits to ensure compliance with the regulation. Unfortunately, even after two decades of the regulation being in place, many entities are still unclear on who is required to comply. This paper is intended to clarify a few of the main points in the regulation as well as how to comply.

Scope of the Guidance

21 CFR Part 11 applies to electronic records and electronic signatures when an entity relies on the digital form of the data in lieu of the paper equivalent. There are a few categories of data that are considered within the scope of this code of regulation mainly:

- Records required by the FDA to be maintained under the predicate rule
- Records submitted to the FDA under the predicate rules
- Electronic signatures serving to be an equal substitution to handwritten signatures (wet signatures).

The key to the inclusion of all the above categories into the scope is that the electronic form of record or signature is the form relied on in lieu of the paper equivalent.

Requirements for Compliance

- Data Encryption and Storage
- Audit Trails
- Electronic Signatures
- User Password Levels

The intent of the regulation is to ensure that the electronic data is as reliable and accurate as its equivalent paper form. For this to be true, it is important that the entire process surrounding the generation the retention and the retrieval of such data supports this merit. In other words, even though the regulation seems to be heavily focused around the computer systems, it is not the computer systems that are compliant with the regulation; it is the entire process.

The properly designed computer systems and the infrastructure are merely tools that allow the process to be compliant. It is up to the user to ensure that the use of the system meets the regulatory requirements.

The regulation specifically outlines a few requirements that are typically necessary for compliance. However, the regulation leaves quite a bit of room for flexibility to allow the users to evaluate the necessity of each requirement as well as the necessity to introduce further procedures by the user.

Performance and Validation

The FDA identifies two types of computerized systems that can be used in a 21CFR part 11 compliant environments namely they are open systems and closed systems. Closed systems are defined by 21 CFR 11.3(b)(4) as "An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system" while open systems are defined by 21 CFR 11.3(b)(9) as "An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system." The difference between the two environments comes down to who has access to the computerized systems that generate, host, and retrieve the data. Both open and closed systems have similar requirements. However, the requirements for an open system are a bit more stringent when it comes to data protection.

The systems should be able to provide the same level of data accessibility to the users and the FDA as their equivalent paper format. In other words, the systems should be able to generate, retain, and make available, electronic records and signatures. Data is stored in encrypted format to prevent users from changing its content. The availability of the data managed by these systems must be at least equivalent of the paper form of the data. The data must be accessible for inspection and copying in a human readable format. Such performance must be validated for accuracy reliability and consistency.

Security – Audit Trails

The systems must be secured against unauthorized access and operation. The systems and procedures must ensure that all operations are done by authorized personnel through the proper input devices. In the case of an open system, additional measures should be considered such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

The systems must also be able to detect any alterations in the data and reporting such entries in audit trails that are retained for the lifetime of the original records. Such audit trails must be secure and indicate the date time and action taken by the operator to affect the records. Similar to the electronic records and signatures, the audit trails must be accessible in a human readable format for the purposes of review inspections and audits.

Electronic Signatures

The regulation clearly spells out several stringent requirements of an electronic signatures. While some the requirements are specific to the system, most of them are procedural requirements to ensure that the systems are used properly.

Both the systems and procedures need to ensure that the electronic signatures at minimum:

- Contain who the signer is when the signature was executed and why.
- The signature must be unique to each individual.
- Have two parts such as a username and a password.
- Each execution of the signature is linked to the appropriate record being signed.
- Each individual's identity must be verified prior to being granted the right to electronically sign records.

Additional Considerations

While not explicitly mentioned in the regulation, records must be retained for at least the same amount of time as their paper form equivalent. With the risk of hardware failures, and data loss it is important that an adequate back up procedure is in place to protect against loss of data. A proper back up procedure should at least ensure the integrity of the data, preserve any of the security features, and allow for easy restoration.

Use in Freeze Drying

- Each user is given a username and password with a user level that provides restricted access to sections of the system. Example user levels: Operator, Maintenance, Supervisor, Administrator.
- The freeze-drying protocol is entered step by step, where is step requires an electronic signature and the change is logged. The protocol or recipe is stored and available for use.
- When the protocol is initiated a batch log is created where all measurements, alarms, and changes are recorded in an encrypted file.
- Once the run is complete, a batch report can be printed in PDF format that includes the operator name, protocol, data measurements over time, graphic data, alarms, and a log of any adjustments made to the cycle.
- All batch records are stored and available for reference for later reporting.