

21 CFR Part 11: How Does It Affect Laboratory Automation Software Developers?

Robert M. Brown Jr., Code Refinery : rmbrown@code-refinery.com

ABSTRACT

Just what is "21 CFR Part 11"? Do I need to consider it when designing lab automation software?

Sure, I store data electronically, but my "official" copy is a signed hardcopy stored in my documentation control system, so Part 11 doesn't apply to me, right?

These and similar questions are being asked with increasing frequency during the development process for both off-the-shelf and custom lab automation software. This poster presents:

- 1) a brief overview of the FDA regulation concerning the use of electronic records and electronic signatures and
- 2) a guide for software analysts and developers.

Regulation Overview

Records are kept for a number of reasons. 21 CFR Part 11 (Part 11)¹ applies only to those records that are kept to meet other FDA regulations. Traditionally these records have been paper-based and stored in files or binders. When those records required signatures, the document was distributed to all parties on the signature list, and the signatures were stored along with the original.

Part 11 *does not* address what types of records should be kept, how long they should be kept, or who should sign them. It *does not* require that a company make the transition from paper to electronic files. It *does not* require that a company use electronic signatures or biometric identification. **What Part 11 does is provide the "criteria under which the FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures."**¹ In other words, if a company chooses to switch from paper records to electronic records, this regulation describes what must be done to satisfy an FDA audit.

Compliance Through Software?

One of the most important facts that a software developer should understand about Part 11 is that no single software application or set of applications can force an organization to be compliant. The job of the software developer is to provide the organization with the tools it needs to meet the regulation. The organization must then, among other things, configure the application, train users, maintain an emergency backup plan, limit system access, hold users accountable for electronic signatures, control system documentation, establish SOPs to prevent the reuse of electronic signatures, and certify that electronic signatures are legally binding before compliance can be achieved.

Most of the individual requirements in the regulation can be sorted into two categories, those that the organization must put in place and those that the software in question must implement. There are, of course, a number of requirements that can and should be sorted into both groups. The purpose of this presentation is to provide a high level view of those requirements the software developer must take into account to ensure that the organization gets the tools it needs.

Glossary²

Closed System – An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

Electronic Record – Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Signature – A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Handwritten Signature – The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

Open System – 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.

Software Design Considerations

Electronic records must be maintained in such a way that their authenticity, integrity and, if applicable, confidentiality are maintained. If a system is defined as "closed" (system access is controlled by persons who are responsible for the content of the records), then the following is a list of software development issues that must be considered.

- Records must be stored in such a way that they can be inspected, viewed, or copied by the FDA in both human readable and electronic form.
- Legacy data must still be readable or convertible if legacy hardware is not to be maintained. This must be taken into account when upgrading or replacing systems. Electronic records must be maintained for as long as the paper records that they replace.
- Secure, computer-generated, time-stamped audit trails must independently record operator activities that create, modify or delete electronic records without obscuring previously recorded data.
- Sequencing of process steps or events must be enforced whenever possible.
- Only authorized individuals must be allowed to use the system, sign a record, or alter an existing record.
- Time sequenced development and modification of all systems documentation must be logged via an audit trail.

If a system is defined as "open" (emailed records, internet-based applications, etc.), then the following items should also be considered.

- Document encryption may be necessary to maintain confidentiality.
- Digital signature standards may be used to ensure record authentic and integrity.

Signature considerations:

- The printed name of the signer, the date and time the record was signed, and the meaning of the signature (record reviewed, record approved, etc.) must be captured as part of any signature.
- Any human-readable form of a signed record must display this information.
- Any electronic or handwritten signature must be linked to its corresponding electronic record so that it cannot be copied and used to falsify another record.

References

- 1) Electronic Records: Electronic Signatures Final Rule, 62 Federal Register 13430 (March 20, 1997).
- 2) Guidance for Industry: 21 CFR Part 11: Electronic Records: Electronic Signatures: Glossary of Terms, Draft Guidance, Food and Drug Administration, Office of Regulatory Affairs, August 2001.
- 3) Guidance for Industry: 21 CFR Part 11: Electronic Records: Electronic Signatures: Validation, Draft Guidance, Food and Drug Administration, Office of Regulatory Affairs, August 2001.
- 4) Complying with 21 CFR Part 11: Electronic Records and Electronic Signatures, Part 2: GAMP Special Interest Group (21 CFR Part 11), 2001.
- 5) FDA Begins Roll-Out Of Electronic Records/Signatures Guidance, The Silver Sheet, Medical Device Quality Control Reports, Vol. 5, No. 10, F-D-C Reports, Inc., October 2001.

Electronic signatures do not have to be based on biometrics (retinal scan, fingerprint, etc.). Username/passwords can be used, but the following criteria must be met:

- At least two distinct identification components must be used.
- If a user signs multiple documents in a single session, at least one of the components must be used for each document.
- While a strict definition for a "single session" is not provided, the regulation does make it clear that if more than one document is signed, but they aren't signed in the same session, both components must be used to execute the signature.

While most controls for usernames and passwords are carried out with company SOPs and training, there are some related software design considerations.

- Each combination of username and password must be unique.
- Passwords should expire periodically.
- Safeguards should be implemented to detect and report usernames and passwords that may have been compromised. (Disable the combination and alert system administrators and/or management)

Conclusion

Part 11 is often discussed, but many times misunderstood. In its purest form, the regulation is a set of criteria that must be met by any company wanting to keep FDA required records in electronic form. The criteria may be divided into requirements that must be implemented by software developers and those that must be implemented by the organization. This poster presents a brief list of those that affect software developers. The referenced documents provide an excellent starting place to understanding this regulation and its implications. Additional guidance documents from the FDA and from the GAMP (Good Automated Manufacturing Practice) Special Interest Group are expected in 2002.