FDA Regulation 21 C.F.R Part 11

Document Owner: Andrew Forsyth

Effective Date: 18th June 2025

Version: 1.1

Document Approver: Andrew Forsyth

Introduction

Organizations regulated by the U.S. Food and Drug Administration (FDA) must follow a variety of Good Practice (GxP) standards - such as Good Laboratory Practice (GLP), Good Clinical Practice (GCP) and Current Good Manufacturing Practice (cGMP). When an FDA-regulated company relies on an electronic system for record-keeping or electronic signatures, that system must comply with 21 C.F.R. Part 11 (simply “Part 11”).

This paper explains how Processity can equip life-science companies to obtain - and keep - Part 11 compliance. It begins with a high-level overview of the rule and then answers common questions about both general provisions and specific subsections.

Part 11 safeguards the integrity of electronic records and signatures. It governs any FDA-required record that is created, modified, stored, archived, retrieved, or transmitted electronically, as well as any electronic document submitted to the agency under a governing statute (often called the “predicate rules”).

For example, medical-device manufacturers must document customer complaints. If they choose an electronic system for this task, that system must follow Part 11. Other similar record-keeping requirements in life-sciences can be streamlined through compliant electronic solutions. In practice, Part 11 applies whenever:

- Electronic records replace paper records required by predicate rules;
- Electronic records accompany paper records but are relied on to conduct regulated activities; or
- Records - or electronic signatures that stand in for handwritten signatures or initials - are sent to the FDA in electronic form.

Although the FDA does not currently enforce every clause in Part 11, any unmet provision can still be enforced through its underlying predicate rule. Requirements the agency is actively enforcing include:

- Restricting system access to authorized users only;
- Using operational system checks;
- Implementing authority checks;
- Deploying device checks;
- Ensuring personnel who develop, maintain, or use the system have appropriate education, training, and experience;
- Maintaining written policies that hold individuals accountable for actions taken under their electronic signatures;
- Exercising strong controls over system documentation; and
- Providing robust controls for electronic signatures.

In short, companies must demonstrate that electronic data are accurate, secure from alteration, and reliable substitutes for paper records. Under a shared-responsibility model, Processity delivers the capabilities that help organizations meet those obligations. The remainder of this

document addresses common questions about how Processity supports customers in satisfying Part 11 requirements while using our Products.

How Processity Can Assist

Shared Responsibility

We approach the shared responsibility model as a partnership with customers. Whilst we provide tools to assist customers, and can provide assistance with their implementation, our customers are responsible for meeting these GxP requirements.
We follow and are audited against SOC2 requirements for good practice in the Software Development Lifecycle. This includes compulsory security training, RBAC, restrictions on source code access, segregation of duties, peer review of code, source code management, QA, application change/release management, patch and vulnerability management, infrastructure protection and monitoring, and other common security and quality controls.
For the avoidance of any doubt, the customer is ultimately responsible for compliance with all FDA requirements, including Part 11.

Signature manifestation and Signature/Record Linking (21 CFR Part 11.50 and 11.70)

Processity Data History

Processity Data History provides a detailed audit trail of what changes were made to data on Salesforce, by whom, and when. This detail is captured with millisecond precision, and includes subsequent changes to data triggered by the original user or system action. Changes to fields are captured in the background regardless of whether the user initiating the change has visibility of the changed data, however display of this audit trail is restricted to only those fields to which the user does have access.

In comparison to platform options:

- Track Unlimited Fields and Objects, vs:
    - 20 fields in Standard Field History
    - 60 or 100 fields with Shield
- Track most types of fields. Platform options only tell you they changed but no before & after values
    - Multi-picklist
    - Rich Text
    - Long Text
    - Roll-up-Summary

    - Auto-number
    - Formulas (where deterministic)
- Track changes from all user types, with Salesforce security model respected for display of field values

Operational system checks (21 CFR Part 11.10(f))

Processity Data History

As above, this provides a high-fidelity audit trail of exactly what has changed as part of process execution.

Processity

Processity provides powerful process intelligence capabilities. It takes data from Processity Data History (and other configurable audit data including Shield Field Audit Trail and Standard Field History) and reconstructs the processes being followed by users, including assessing conformance to a defined “correct” process.

This is a powerful tool in auditing process execution and compliance, and that the processes being followed match the documented policies and procedures.

Validation of configured Salesforce solution

As above, Processity can be used to provide objective evidence that the combination of the system and the user actions are behaving as intended - following the correct process, with the correct effect on its data. This greatly simplifies the activity of validating the configured Salesforce solution.

Documentation of Process Design and Execution

Processity’s automated process documentation capabilities provide a streamlined and automated way of clearly documenting the processes as implemented and executed by users, not just the intended process. The conformance capabilities then assure customers that the documented and executed processes are aligned.

Conclusion

Processity and Processity Data History provide enhanced capabilities for FDA regulated entities to assist them in their fulfillment of the obligations surrounding auditing user behaviour and system changes. This assurance is present at a detailed field-by-field change-by-change level, at the level of analysing individual processes, and the aggregated level of ensuring that systems are correctly documented and conformance levels are maintained.