REGULATORY COMPLIANCE ON SALESFORCE

FDA 21 CFR Part 11 & Salesforce: What Medical Device Manufacturers Need to Know

A practical guide to electronic records, electronic signatures, and validated Salesforce environments for regulated device manufacturers.

Medical Devices | Pharma | MedTech | Diagnostics | Combination Products

Table of Contents

01 - Executive Summary

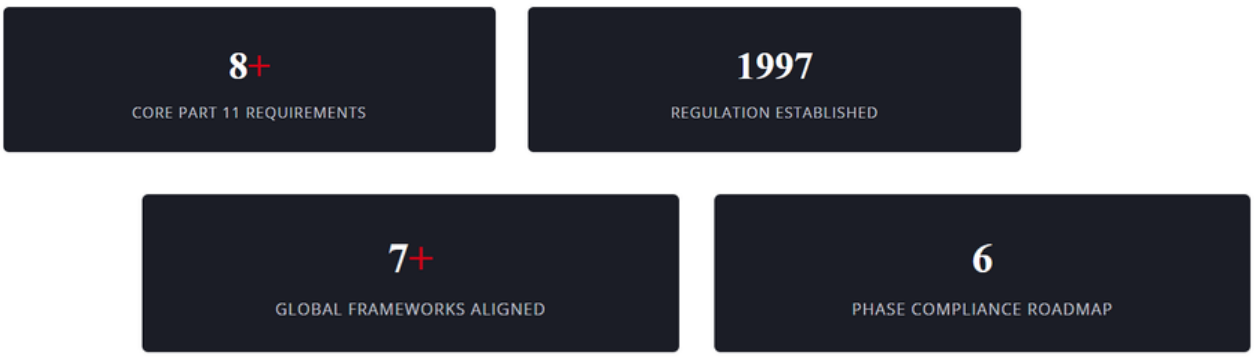
Digital transformation has fundamentally reshaped the medical device industry. Quality management, manufacturing execution, CRM, ERP, and post-market surveillance are increasingly managed through cloud platforms and among the most important regulations governing those systems is FDA 21 CFR Part 11.

Part 11 establishes the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records. For medical device manufacturers, compliance is not optional: every electronic record used to demonstrate regulatory compliance must be able to withstand inspection scrutiny. Failure to do so can result in warning letters, Form 483 observations, product delays, import alerts, or consent decrees.

Can Salesforce support Part 11 compliance?

Yes but with an important qualification. Salesforce provides a secure, configurable platform with strong access control, audit logging, and automation. But compliance is not achieved simply by deploying it. Compliance depends on how the platform is configured, validated, governed, and integrated into the organization's quality management system. The FDA evaluates the manufacturer not the software vendor.

This white paper explores what Part 11 requires, how Salesforce supports compliance, where additional controls are necessary, best practices for validation, common implementation mistakes, and strategies for building an inspection-ready digital system — whether you manufacture diagnostic equipment, implantable devices, surgical instruments, or connected medical technologies.



02 - Digital Transformation & Regulatory Risk

Medical device companies today generate enormous volumes of electronic data design history files, device master and history records, complaint investigations, CAPA documentation, supplier records, training records, production approvals, validation evidence, electronic batch records, and calibration logs.

Historically, most of this documentation lived on paper. Cloud platforms have replaced filing cabinets with digital workflows that enable faster collaboration, global accessibility, and real-time decision-making but digital efficiency introduces new risk. Regulators now routinely ask:

- Who created the record, and who modified it?
- When was it changed, and was anything deleted?
- Can the original version be reconstructed?
- Was the record electronically signed, and was that signature authentic?
- Were unauthorized users prevented from making changes?

These questions sit at the heart of FDA 21 CFR Part 11. Rather than regulating software products themselves, Part 11 regulates the trustworthiness of the electronic records used to demonstrate compliance with FDA regulations.

Why Part 11 Matters More Than Ever

Medical device manufacturers increasingly operate globally, satisfying FDA regulations alongside ISO 13485, EU MDR, UK MDR, Health Canada, TGA Australia, MDSAP, and PMDA Japan simultaneously. Each framework has unique requirements, but all emphasize one principle: data integrity. Cloud platforms like Salesforce can significantly strengthen an organization's ability to demonstrate complete, accurate, consistent, secure, and traceable records provided they sit inside a compliant governance framework.

03 - Understanding FDA 21 CFR Part 11

DA 21 CFR Part 11 was introduced in 1997 to establish the legal framework for electronic records and electronic signatures used in FDA-regulated industries. Its objective is straightforward: **electronic records should be as trustworthy, reliable, and authentic as traditional paper records.** The regulation applies whenever companies choose to maintain records electronically instead of on paper, and it establishes requirements covering system validation, audit trails, electronic signatures, user authentication, record retention, security controls, operational and authority checks, documentation, and training.

Who Must Comply

A common misconception is that Part 11 applies only to pharmaceutical companies. In reality it reaches medical device manufacturers, in vitro diagnostic companies, biotechnology firms, pharmaceutical manufacturers, combination product manufacturers, contract manufacturing organizations, clinical research organizations, blood banks, and tissue establishments.

For device manufacturers specifically, Part 11 frequently intersects with 21 CFR Part 820 (the Quality Management System Regulation, aligning with ISO 13485), design controls, complaint handling, CAPA, production controls, supplier quality, post-market surveillance, labeling, and servicing records. If any of these records are maintained electronically, Part 11 requirements generally apply.

> "A medical device cannot be demonstrated as safe or effective if the supporting records cannot be trusted."

For this reason, inspectors evaluate not only the records themselves but the systems that generate them which is why data integrity sits at the foundation of everything Part 11 requires.

04 - The ALCOA+ Data Integrity Framework

High-quality data should satisfy principles commonly summarized as ALCOA+ the framework regulators worldwide use to assess whether electronic records can be trusted.

PRINCIPLE	WHAT IT MEANS	HOW SALESFORCE SUPPORTS IT
Attributable	Every action is traceable to a specific individual, timestamp, and change.	User authentication, record ownership, Created By / Last Modified By fields, login history.
Legible	Records stay readable throughout their required retention period.	Standardized data formats; long-term accessibility depends on org retention policy.
Contemporaneous	Information is recorded as activities occur, not recreated later.	Workflow automation, mobile capture, and real-time data entry.
Original	The original record — or a certified copy — is preserved.	Audit trails and version control demonstrate originality.
Accurate	Data reflects the activity performed without omission or manipulation.	Validation rules, required fields, standardized picklists.
Complete	All relevant information is retained, including evidence and approvals.	Related-record architecture keeps evidence and approvals linked.
Consistent	Dates, approvals, and workflow progression follow a logical sequence.	Approval Processes and Flow enforce sequencing.
Enduring / Available	Records remain durable and retrievable throughout their retention period.	Cloud infrastructure resilience; retention strategy remains the company's responsibility.

These principles form the backbone against which FDA inspectors and international counterparts evaluate whether a company's electronic records can be trusted.

05 - The Eight Core Requirements of Part 11

Most inspection findings ultimately trace back to a handful of foundational controls. Understanding each one and where Salesforce's native capability ends is essential to a defensible implementation.

1. System Validation

The FDA does not certify software as "Part 11 compliant." Companies must validate that their specific implementation performs as intended that workflows operate as designed, permissions work, signatures are enforced, and audit trails are accurate. Two companies on identical Salesforce environments can have very different inspection outcomes depending on the strength of their validation evidence.

2. Secure, Computer-Generated Audit Trails

An audit trail provides a chronological history of activity, allowing organizations and regulators to reconstruct events who created or modified a record, what changed, when, and why. Salesforce supports this through Field History Tracking, Setup Audit Trail, Event Monitoring, Login History, API activity logging, and report execution history. Limitations to plan around: only selected fields are tracked, retention varies by configuration and licensing, and not every system event is captured automatically which is why many regulated organizations supplement native tracking with validated audit frameworks.

3. Electronic Signatures

An electronic signature carries the same legal weight as a handwritten one when it is unique to an individual, attributable, difficult to falsify, and permanently linked to its record. Signatures typically capture a printed name, date/time, and meaning (approval, review, verification). Salesforce authentication unique usernames, MFA, SSO, role-based permissions is a strong foundation, but organizations generally pair it with validated approval workflows or dedicated e-signature applications to fully satisfy Part 11.

4. Access Controls

Part 11 expects employees to be able to perform only the activities appropriate to their role quality engineers create CAPAs, production supervisors approve manufacturing activity, administrators maintain configuration but hold no authority to approve quality records. Salesforce's Profiles, Permission Sets, Role Hierarchies, Sharing Rules, and Field-Level Security map well to this model, provided permissions are reviewed regularly. Excessive administrative access is one of the most common findings in internal audits.

5. Record Retention

Records must remain accessible, readable, retrievable, and secure often for years or decades. Salesforce's cloud infrastructure supports high availability, but archival procedures, backup frequency, disaster recovery, and restoration testing remain the regulated company's responsibility.

6. Operational Checks

Workflow automation ensures activities occur in the correct sequence a CAPA cannot close before investigation; a device cannot release without quality authorization. Salesforce Flow, Approval Processes, and validation rules support these controls when properly designed and validated.

7. Authority Checks

Authority checks verify that only the right individuals can perform regulated activities only Quality Managers approve CAPAs, only Regulatory Affairs approve submissions complementing access permissions with organizational governance.

8. Device Checks

Where laboratory equipment, barcode scanners, or IoT-enabled devices feed regulated records, Salesforce integrations should be validated alongside the connected systems, ensuring correct device identification and accurate, unauthorized-input-free data transfer.

06 - Computer System Validation (CSV)

Most inspection findings ultimately trace back to a handful of foundational controls. Understanding each one and where Salesforce's native capability ends is essential to a defensible implementation.

VALIDATION SHOULD ANSWER

Does the platform support regulated processes as designed? Are access controls and audit trails functioning correctly? Are electronic signatures properly linked to records? Can data be recovered after a failure, and do integrations preserve data integrity?

Risk-Based Validation

Rather than testing every feature equally, the FDA aligned with ISPE's GAMP® framework encourages manufacturers to prioritize validation effort by business and patient impact.

RISK TIER	REPRESENTATIVE FUNCTIONS
High Risk	Electronic signatures, CAPA approval workflows, complaint handling, device release processes, audit trail generation, production approvals.
Medium Risk	Dashboards, reporting, notifications, workflow automation.
Lower Risk	Cosmetic page layouts, branding elements, non-regulated reports.

Typical Validation Documentation

- Validation Plan & Strategy
- User & Functional Requirements Specifications
- Risk Assessment & Mitigation Plan
- IQ / OQ / PQ Test Scripts & Results
- Traceability Matrix & Validation Summary Report
- Training Records & SOP Updates

The FDA evaluates functionality, not development methodology a low code Salesforce Flow supporting a regulated process requires the same validation rigor as custom Apex code.

07 - Change Control in a Validated Environment

Medical device companies rarely operate static software environments. Salesforce delivers major platform releases three times each year, alongside security updates and feature enhancements and organizations continuously introduce new workflows, objects, integrations, and process improvements. Each change carries the potential to affect validated functionality.

Medical device companies rarely operate static software environments. Salesforce delivers major platform releases three times each year, alongside security updates and feature enhancements and organizations continuously introduce new workflows, objects, integrations, and process improvements. Each change carries the potential to affect validated functionality.

1. **Change Request**
   Document the proposed modification.

2. **Impact Assessment**
   Determine whether regulated functionality is affected.

3. **Risk Evaluation**
   Assess potential impact on compliance and patient safety.

4. **Testing Strategy**
   Define regression and functional testing requirements.

5. **Approval & Implementation**
   Authorize, then deploy changes in a controlled manner.

6. **Verification & Documentation**
   Confirm production behavior; update validation records, SOPs, and training.

Without structured change control, organizations risk invalidating processes that were previously tested and approved.

08 - Salesforce Inside the Quality Management System

Increasingly, manufacturers use Salesforce as more than a CRM as the operational backbone connecting quality, manufacturing, service, and customer operations.

QMS PROCESS	WHAT SALESFORCE COORDINATES
CAPA	Issue identification, investigation, root cause, corrective/preventive action, effectiveness verification, management approval, closure.
Complaint Management	Intake, product identification, risk classification, investigation, escalation, regulatory reporting, trend analysis, closure.
Nonconformance (NCR)	Detection, containment, investigation, disposition, corrective action, verification.
Supplier Quality	Qualification, audits, performance metrics, approved-supplier status, corrective actions, risk assessments.
Training Management	Required training, completion, competency assessment, electronic acknowledgment, history.
Device History Record	Manufacturing dates, lot/serial numbers, inspection results, production approvals, release documentation.
Device Master Record	Bills of materials, production procedures, packaging specs, labeling, QA procedures — with change control ensuring only current versions remain active.
Design History File	Design reviews, approval workflows, action items, and cross-functional traceability across development activities.

Without structured change control, organizations risk invalidating processes that were previously tested and approved.

09 - Preparing for an FDA Inspection

Inspectors are not evaluating software for its own sake they are assessing whether the organization can consistently demonstrate control over its regulated activities. An inspection rarely focuses on a single requirement in isolation; regulators trace records through every connected process, from complaint intake through investigation, corrective action, management approval, and closure.

Questions FDA Inspectors Frequently Ask

System Validation

- How was Salesforce validated, and where is the documentation?
- How do you determine which functions require testing?

Electronic Signatures & Audit Trails

- How are signatures authenticated, and can they be reassigned?
- Can you demonstrate who modified a record, and for how long are logs retained?

Access Management

- Who can modify regulated records, and how are permissions reviewed?
- How are terminated employees removed?

Change Control

- How are Salesforce upgrades and new workflows validated?
- Who approves configuration changes?

Organizations that answer these questions confidently typically have mature governance processes not simply well-configured software.

10 - Shield, Security & Advanced Controls

For organizations in highly regulated environments, Salesforce Shield extends the platform with enhanced security and monitoring.

Platform Encryption
Encrypts sensitive information patient identifiers, complaint data, clinical data, supplier records while keeping it available for authorized business processes.

Field Audit Trail
Extends retention of historical field changes beyond standard field history tracking, supporting long-term retention requirements.

Event Monitoring
Visibility into login behavior, report exports, API usage, data downloads, and security events strengthening governance alongside, not in place of, Part 11 audit trails.

Cybersecurity Baseline
MFA, password policies, SSO, IP restrictions, session timeouts, encryption at rest and in transit, vulnerability assessments, and disaster recovery testing.

> "A secure system is better positioned to preserve data integrity throughout the record lifecycle."

11 - Common Mistakes & Best Practices

COMMON MISTAKES

- Assuming the software is automatically compliant
- Treating validation as a one-time project
- Poor or undocumented change control
- Excessive user permissions left unreviewed
- Weak supporting documentation
- Ignoring data integrity gaps
- Delaying user training

BEST PRACTICES

- Build compliance into the design, not after
- Define clear cross-functional ownership
- Adopt risk-based validation
- Standardize documentation templates
- Automate — and validate — where appropriate
- Conduct periodic access and SOP reviews
- Maintain a culture of continuous improvement

12 - A Practical Compliance Roadmap

For organizations planning or expanding Salesforce within regulated operations, a phased approach establishes a strong compliance foundation.

1. **Assessment**
   Identify regulated business processes, map applicable regulatory requirements, and conduct a gap analysis.

2. **Design**
   Define user requirements, design security roles, establish governance procedures, and plan validation activities.

3. **Implementation**
   Configure Salesforce, develop required automations, integrate supporting systems, and create validation documentation.

4. **Validation**
   Execute IQ/OQ/PQ as appropriate, test workflows, verify signatures and audit trails, and document results.

5. **Deployment**
   Train users, release the controlled production environment, monitor adoption, and establish support procedures.

6. **Continuous Compliance**
   Review changes, validate updates, perform periodic access reviews, update SOPs, and prepare for regulatory inspection.

13 - Frequently Asked Questions

Q. Is Salesforce FDA 21 CFR Part 11 certified?
No. The FDA does not certify software platforms. Salesforce provides capabilities that support compliance, but each organization is responsible for validating and governing its own implementation.

Q. Can Salesforce support electronic signatures?
Yes, when properly configured and validated — often alongside specialized electronic signature solutions where appropriate.

Q. Does Salesforce provide audit trails?
Yes. Native audit and history-tracking capabilities are available, and features such as Field Audit Trail and Event Monitoring can enhance traceability depending on licensing and implementation.

Q. Is validation required for every Salesforce update?
Not necessarily. Organizations should perform impact assessments and apply a risk-based approach to determine the extent of revalidation needed.

Q. Can Salesforce replace a Quality Management System?
Salesforce is flexible enough to support many QMS processes. Whether it fully replaces an existing QMS depends on organizational requirements, regulatory needs, and implementation scope.

Q.How often should user permissions be reviewed?
Most organizations conduct formal access reviews at least annually, with additional reviews following organizational or system changes.

Q.What is the biggest compliance mistake organizations make?
Assuming that deploying compliant technology automatically results in regulatory compliance. Compliance depends on governance, validation, documentation, and disciplined operational practices.

Build a Validated, Inspection-Ready Salesforce Environment

Axolt helps medical device and life sciences manufacturers configure, validate, and govern Salesforce as a compliant system of record from CAPA and complaint handling to device history and supplier quality.

See Axolt in Action