



INTUITIONLABS / RESEARCH & PRACTICAL GUIDANCE

# Salesforce in Claude for Pharma: CRM Read/Write Pilot Controls

Build practical AI for pharma and biotech with IntuitionLabs. We help life-science teams turn complex information and workflows into useful software, governed knowledge systems and AI tools.

Published by IntuitionLabs · 2026-10-30 · salesforce in claude for pharma · claude salesforce integration · salesforce plugin · claude · pharma crm · crm governance · human approval · mcp · audit trail

Original article: <https://intuitionlabs.ai/articles/salesforce-claude-pharma-crm-pilot-controls>



---

## In this article

1. Executive Summary
  2. Introduction and Background
  3. Key Changes: A Beta with Unevenly Documented Write Behavior
  4. Identity, Permissions, and Context Boundaries
  5. Implementation Considerations and Read/Write Workflows
  6. Pharma Data Governance and Process Exclusions
  7. Pilot Validation and Negative Tests
  8. Audit Evidence, Monitoring, and Rollback
  9. Data Analysis and Evidence
  10. Implications and Future Directions
  11. Conclusion
- 

## Executive Summary

**Salesforce in Claude for pharma should enter governance review as a permissioned integration capable of affecting customer relationship management (CRM) records.** Anthropic announced the beta on **September 15, 2026**, with **37 sales skills** and examples including opportunity updates, call logging, and follow-up tasks. ([claude.com](https://claude.com)) Its setup guide describes availability on paid Claude plans, subject to Salesforce beta approval, and use in chat and Claude Cowork on web and desktop. ([support.claude.com](https://support.claude.com))

The documentation retrieved for this **October 30, 2026** assessment contains material differences. Salesforce's overview describes beta skills as read-only or drafts requiring user action, ([help.salesforce.com](https://help.salesforce.com)) while its tool-restriction instructions describe Dispatch application programming interface (API) settings that permit confirmed writes, permit unconfirmed writes, or enforce read-only operation. ([help.salesforce.com](https://help.salesforce.com)) Eligibility also differs between the vendors' pages. ([help.salesforce.com](https://help.salesforce.com)) A controlled pilot must therefore establish its actual entitlement, installed tools, and effective restrictions before admitting writes.

Existing user permissions are necessary, but broader pilot controls are warranted. Anthropic documents **Allow once**, **Always allow**, and **Deny** choices; ([support.claude.com](https://support.claude.com)) general plugin documentation says the most permissive group setting applies. ([support.claude.com](https://support.claude.com)) The recommended starting position is named participants, a field allowlist, restricted tools, and review of every intended write. This follows the Open Worldwide Application Security Project (OWASP) recommendation to enforce authorization in downstream systems and obtain approval for high-impact actions. ([genai.owasp.org](https://genai.owasp.org))

Patient information and regulated workflows need separate admission decisions. Anthropic's business associate agreement (BAA) documentation excludes third-party connector data flows and skills from its coverage; ([privacy.claude.com](https://privacy.claude.com)) a general enterprise subscription does not establish this plugin's eligibility for protected health information. Nor does a chat approval establish compliance with electronic-record requirements. ([www.ecfr.gov](https://www.ecfr.gov)) Claude's documented audit export covers the previous **180 days** but excludes chat content, ([support.claude.com](https://support.claude.com)) while standard Salesforce field-history availability has different limits. ([trailhead.salesforce.com](https://trailhead.salesforce.com)) The practical go/no-go test is whether each admitted operation can be attributed,

checked against its approved proposal, reconciled in Salesforce, and corrected through a rehearsed procedure. The worksheet below measures approval, commitment, error, and review burden from the reader's own observations, without assuming productivity gains.

## Introduction and Background

The relevant question for commercial information technology (IT), CRM owners, sales operations, privacy, and medical-legal-regulatory teams is which data and operations can be admitted under an accountable operating model. Salesforce's integration guidance says Claude sees what the requesting user is authorized to see. That makes the permissions already attached to a sales role a starting point for assessment, rather than a sufficient pilot specification. ([help.salesforce.com](https://help.salesforce.com))

This report takes the perspective of **IntuitionLabs as an adjacent adviser**: the decision concerns third-party software and the organization's own controls. The analysis separates vendor-documented capabilities from recommended safeguards and unresolved questions. Recommendations below are a pilot design, not claims that every safeguard exists natively in the beta.

A commercial account summary and a record required by a regulated process can involve the same organization yet have different intended uses. The Food and Drug Administration (FDA) recommends determining whether particular electronic records fall under **21 CFR Part 11** by reference to the applicable predicate rules. ([www.fda.gov](https://www.fda.gov)) Its computer software assurance guidance has the narrower scope of medical-device production and quality-management software. ([www.fda.gov](https://www.fda.gov)) Neither document makes ordinary commercial CRM automatically subject to those requirements.

The review therefore uses distinct admissions for read access, generated drafts, and committed updates. It also treats Salesforce, Slack, email, Claude conversations, and retained evidence as separate data locations. The UK government's Data and AI Ethics Framework recommends mapping data flows before personal-data use; the Cybersecurity and Infrastructure Security Agency (CISA) recommends reviewing secure-deployment guidance when operating externally developed artificial intelligence (AI) systems. ([www.gov.uk](https://www.gov.uk)) ([www.cisa.gov](https://www.cisa.gov))

Public documentation is evidence of intended product behavior, not a completed qualification of a particular tenant. Where sources differ or do not establish a capability, the report identifies an acceptance test or an exclusion. This approach avoids turning a general integration announcement into an assertion of pharmaceutical suitability. The research did not establish Good Practice (GxP) validation, Part 11 compliance, or support for pharma-specific Salesforce clouds.

## Key Changes: A Beta with Unevenly Documented Write Behavior

### Eligibility and scope require a tenant-specific check

Anthropic's administrator guide requires the latest **Sales Cloud enterprise edition** and Salesforce approval of the beta request. ([support.claude.com](https://support.claude.com)) Salesforce's overview instead lists Enterprise, Performance, Unlimited, and Developer Editions and says Claude Enterprise is required. ([help.salesforce.com](https://help.salesforce.com)) These are not interchangeable eligibility statements. Obtain confirmation of the specific Salesforce organization, Claude plan, and supported surface before selecting participants.

The official AgentExchange listing could not be verified beyond limited rendered content during this session, including after the permitted fallback fetch. Its proposed listing date and detailed beta terms are consequently not treated as established facts here. Procurement should preserve the actual acceptance terms supplied to the organization.

## Separate skills, connectors, and operations

The official Skills Reference provides the following **37 skill identifiers**, grouped here for readability: account-context, research-prospect, account-plan, account-tiering, stakeholder-map, expansion-whitespace; deal-review, deal-advance-gap, deal-signals, deal-slip-scenario, close-plan, update-opportunity, handle-objection; pipeline-review, team-pipeline, forecast-narrative, sfdc-hygiene-check, weekly-wrap, win-loss-review; customer-health, renewal-radar, customer-voice; lead-triage, assign-target-to-sdr, draft-outreach; call-prep, call-follow-up, summarize-conversation-transcript, schedule-meeting, calendar-events, log-activity, query-activity-history; daily-briefing, inbox-sweep, rep-context, find-internal-answer, voice-profile.

([help.salesforce.com](https://help.salesforce.com))

Salesforce's separate [record-creation guide](#) documents creation and editing for standard and custom objects, including records using page layouts or Dynamic Forms. It identifies six skills supporting direct creation and updates: assign-target-to-sdr, account-plan, log-activity, schedule-meeting, summarize-conversation-transcript, and update-opportunity. This is documented general support; the pilot must still qualify its admitted objects, fields, approval behavior, and recovery procedures.

An inventory of names does not establish an object/action contract. For example, the reference describes log-activity as drafting an entry for review. ([help.salesforce.com](https://help.salesforce.com)) Anthropic's launch describes direct updates after approval. ([claude.com](https://claude.com)) Preserve both the installed skill definitions and the exposed connector tools; do not infer write capability from a skill named update-opportunity or infer read-only enforcement from a draft-oriented description.

## Approval defaults exist at different layers

Salesforce's **Dispatch API** guidance documents **Needs Approval**, **Always Allowed**, and **Deny**, and warns that tools are unrestricted by default. Anthropic separately describes user-facing approval choices. An administrator restriction and a user's conversational approval are different controls, and their combined behavior needs testing. Salesforce's [record-creation guide](#) says an administrator must set Dispatch API to **Always Allowed** to enable creation and updates. Its [tool-restriction guide](#) instead recommends **Needs Approval** and says users can create and update records under that setting after Claude asks for approval. Resolve this discrepancy with Salesforce and test the effective setting before admitting writes; the record-creation guide's general support does not establish that the pilot's approval policy is enforced.

([help.salesforce.com](https://help.salesforce.com)) ([support.claude.com](https://support.claude.com))

For the pilot, prefer a confirmed read-only restriction initially, followed by narrowly admitted writes with explicit confirmation. ([help.salesforce.com](https://help.salesforce.com)) Treat any unresolved interaction between defaults, saved permissions, and administrative restrictions as a reason to withhold write access. Australia's cyber security guidance recommends least privilege and human oversight for sensitive agentic actions, supporting this staged approach without establishing how this particular connector implements it. ([www.cyber.gov.au](https://www.cyber.gov.au))

## Identity, Permissions, and Context Boundaries

The documented identity path begins with organizational setup and ends with the individual Salesforce user. Claude administrators configure the connector using the External Client App credentials, and members subsequently sign in using their own Salesforce accounts. ([support.claude.com](https://support.claude.com)) The shared application configuration must not be mistaken for a shared sales identity.

The pilot record should describe this flow explicitly: **Claude organization and participant entitlement** → **installed plugin** → **Salesforce Model Context Protocol (MCP) connector** → **OAuth authorization** → **named Salesforce user** → **permitted records and fields**. MCP is the protocol connecting the assistant to external tools; OAuth is the authorization framework used to delegate access. General protocol security guidance forbids token passthrough, but that standard is not an implementation audit of this connector. ([modelcontextprotocol.io](https://modelcontextprotocol.io))

Document and test these controls:

- **Participant gate:** Maintain a named participant allowlist and establish that excluded identities cannot invoke the admitted tools. Require evidence of enforcement. ([www.cyber.gov.au](https://www.cyber.gov.au))
- **Application authorization:** Use the documented “Admin approved users are pre-authorized” configuration and verify that excluded users cannot self-authorize. ([help.salesforce.com](https://help.salesforce.com))
- **Token privilege:** Inventory the documented mcp\_api and refresh\_token/offline\_access scopes. These authorize services and continued access; they are not a field-level business allowlist. ([help.salesforce.com](https://help.salesforce.com))
- **Record access:** Check sharing and permission sets using an ordinary participant account and an excluded account. Salesforce says these controls continue to apply. ([trailhead.salesforce.com](https://trailhead.salesforce.com))
- **Token boundary:** Confirm requested resource and privilege boundaries against the Internet Engineering Task Force's OAuth guidance, which recommends minimum privileges and audience-restricted tokens. ([www.rfc-editor.org](https://www.rfc-editor.org))
- **Claude distribution:** Group-level plugin access is documented as an Enterprise feature. Assess actual group memberships, because the most permissive setting applies. ([support.claude.com](https://support.claude.com))
- **Context identity:** Require work identities for connected collaboration services. Slack documents identity-provider controls for this purpose, subject to its supported setup. ([slack.com](https://slack.com))

Slack and email require independent review. Slack's general MCP guidance includes reading channels, sending messages, and creating canvases. ([slack.com](https://slack.com)) An account-research permission therefore must not silently become permission to publish a summary to a channel. Give channel access and message publication separate acceptance tests.

Treat calendar and email as optional data sources requiring their own admission decision. Record the supplying connector, mailbox scopes, approved folders, retention settings, and permitted purpose. Disable a source until its boundaries are understood, rather than assuming authorization for account research permits unrestricted context gathering. ([cnil.fr](https://cnil.fr))

Least privilege also applies after data leaves Salesforce. Salesforce states that data handling at Anthropic is governed by the organization's Anthropic contract. ([help.salesforce.com](https://help.salesforce.com)) Review the destination, retention, and onward-processing conditions rather than assuming source-system permissions govern every subsequent copy.

## Implementation Considerations and Read/Write Workflows

A **read** retrieves approved information. A **draft** proposes a record or message without committing it. A **write** changes destination state. Use these operational definitions throughout testing and monitoring. OWASP recommends authorization in downstream systems, so a prompt telling Claude to avoid a field is supplementary guidance, not an access control. ([genai.owasp.org](https://genai.owasp.org))

*Table 1* maps candidate workflows to proposed pilot boundaries. Rows describe admission recommendations; a workflow label is not a guarantee of the connector's object schema or write support.

| Workflow                                  | Initial admission                                                    | Approval and evidence                                              | Reconciliation or correction requirement                                   |
|-------------------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------|
| Account research                          | Read approved account fields; exclude unrestricted narrative exports | Record source record identifiers and retrieval time                | Compare summary with current source records                                |
| Opportunity next steps, stage, close date | Draft first; admit individual writes only after tenant tests         | Show record, existing value, proposed value, and reviewer decision | Verify every changed field and check downstream effects                    |
| New contact or contact role               | Exclude automatic creation initially                                 | Require identity matching and explicit creation review             | Check duplicates and linkage before any corrective action                  |
| Follow-up task                            | Draft only until exact object and required fields are proven         | Preserve owner, due date, record linkage, and approved text        | Check for an existing task before retrying                                 |
| Forecast                                  | Read approved pipeline and draft a narrative                         | Separate narrative approval from any record update                 | No assumption of direct forecast-object write support                      |
| Call note or activity                     | Draft a minimized commercial summary                                 | Confirm record type and approved content before saving             | Verify linked account/contact and retained evidence                        |
| Slack summary or email                    | Draft; publication is a separate operation                           | Confirm destination and audience before sending                    | Record the sent message identifier; handle follow-up correction separately |

The matrix separates content review from execution approval. A polished draft can still refer to the wrong account, and an authorized operation can contain incorrect values. Check both stages against a versioned proposal, preserving the evidence and the reviewer's decision. ([oecd.ai](https://oecd.ai)) ([genai.owasp.org](https://genai.owasp.org))

A field allowlist should be **enforced through the strongest available system controls**, then exercised through negative tests. For an admitted opportunity update, the proposal should expose the record identifier, proposed fields, current values, new values, source evidence, and expected side effects. The reviewer must

be able to reject an individual operation without accepting a bundle. This is a recommended implementation of documented human-oversight principles. ([airc.nist.gov](https://airc.nist.gov))

Do not equate **Always allow** with a single reviewed change. ([support.claude.com](https://support.claude.com)) Its documented presence requires testing its actual persistence and scope, including a subsequent session and a different record. The public user guide does not establish those details. If administrators cannot demonstrate the required approval behavior, keep the affected operation outside the write pilot.

Maintain the destination's existing business controls. Salesforce says validation rules apply to new and updated records and recommends verifying each integration. ([help.salesforce.com](https://help.salesforce.com)) Test required fields, invalid stages, prohibited date combinations, and automation invoked by accepted updates using representative synthetic records. A displayed approval does not prove that the destination accepted the update or that downstream work completed. ([www.gov.uk](https://www.gov.uk))

## Pharma Data Governance and Process Exclusions

Data classification should follow the information and intended use, rather than the object name alone. A healthcare professional (HCP) contact can contain ordinary business details, sensitive narrative, or information collected for a distinct purpose. A healthcare organization (HCO) account can likewise mix commercial and operational material. The European Commission's guidance emphasizes a specific processing purpose and accurate, current personal data. ([commission.europa.eu](https://commission.europa.eu))

*Table 2* proposes an initial exclusion policy. These are conservative pilot decisions, not assertions that every listed category has the same legal status.

| Data or process                                         | Suggested pilot boundary                                           | Evidence needed to reconsider                                                                                   |
|---------------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Commercial HCP/HCO business information                 | Admit selected fields only after purpose and access review         | Documented purpose, participant role, field list, and permitted destinations                                    |
| Patient information or identifiable clinical narratives | Exclude from prompts, notes, attachments, Slack, and email context | Applicable contracts, feature-level coverage, lawful processing assessment, and separate qualification          |
| Consent or communication-preference records             | Read only if required; exclude changes initially                   | Authoritative source, approved change process, identity checks, and reconciled result                           |
| Medical-information requests and safety-related intake  | Keep outside the commercial write pilot                            | Separate process ownership, routing, completeness controls, and qualification                                   |
| Regulated source records and electronic signatures      | Exclude from ordinary commercial pilot                             | Applicable record requirements, validated intended use where required, and appropriate audit/signature controls |

The important boundary is often between a limited business fact and an unrestricted narrative field. The Information Commissioner's Office (ICO) advises using less personal data where the same outcome can be achieved. ([ico.org.uk](https://ico.org.uk)) Its AI guidance is under review, so use that principle alongside current jurisdiction-specific assessment. France's Commission nationale de l'informatique et des libertés (CNIL) similarly explains that purpose limitation constrains future reuse. ([cnil.fr](https://cnil.fr))

Apply these operational rules:

- **No opportunistic enrichment:** Do not add sensitive context merely because it is available in a connected thread. Limit collection to the defined task. ([ico.org.uk](https://ico.org.uk))
- **No assumed anonymity:** The European Data Protection Board (EDPB) calls for case-by-case assessment of model anonymity. Removing obvious names is not a complete anonymization assessment. ([www.edpb.europa.eu](https://www.edpb.europa.eu))
- **No assumed BAA coverage:** Evaluate both the organization and the feature/data flow. Anthropic excludes third-party connector flows and skills from its BAA coverage. ([privacy.claude.com](https://privacy.claude.com))
- **No universal HIPAA claim:** Where the Health Insurance Portability and Accountability Act (HIPAA) applies, the Department of Health and Human Services (HHS) requires appropriate BAA arrangements for cloud processing of electronic protected health information. ([www.hhs.gov](https://www.hhs.gov))
- **No unrestricted health-data access:** Apply the minimum necessary standard where applicable, taking account of its exceptions and the intended purpose. ([www.hhs.gov](https://www.hhs.gov))

Regional processing, storage, and connected services must be evaluated separately. Anthropic's United States-only inference documentation expressly says it does not change where third-party services operate and distinguishes inference from storage. ([support.claude.com](https://support.claude.com)) A regional inference setting therefore does not settle the residency of CRM, Slack, email, logs, or exports.

Training and retention also answer different questions. Anthropic excludes commercial-product inputs and outputs from training by default, with stated exceptions such as explicit feedback. ([privacy.claude.com](https://privacy.claude.com)) Its commercial retention page describes saved conversations and deletion from back-end storage within **30 days** after deletion, subject to the policy's qualifications. ([privacy.claude.com](https://privacy.claude.com)) Do not transplant an API retention rule onto saved chat.

For regulated uses, obtain a documented applicability assessment from the responsible quality and legal owners. Part 11 requires specific controls within its scope; ([www.ecfr.gov](https://www.ecfr.gov)) European Medicines Agency (EMA) guidance about attributable remote access to confidential health documents concerns clinical trials. ([www.ema.europa.eu](https://www.ema.europa.eu)) These sources help identify boundaries, not qualify this commercial beta for regulated processing.

## Pilot Validation and Negative Tests

A pilot should establish a documented intended use, repeatable tests, and retained results. The National Institute of Standards and Technology's (NIST) AI Risk Management Framework recommends testing before deployment and regularly in operation. ([airc.nist.gov](https://airc.nist.gov)) The UK government recommends anonymized or synthetic test data where possible. ([www.gov.uk](https://www.gov.uk)) Begin with synthetic accounts and realistic access differences before exposing live commercial records.

Freeze the test configuration: participant identities, Salesforce permission assignments, external application settings, Claude plan, plugin and skill versions where visible, tool restrictions, connected context sources, and model selection. Record unavailable version identifiers as a reproducibility limitation. Australia's guidance recommends a phased introduction with approved uses, classification, and validated controls. ([www.cyber.gov.au](https://www.cyber.gov.au))

Table 3 supplies proposed negative tests and acceptance evidence. A test passes only when the observed destination state and retained evidence support the expected result.

| Test                                                    | Expected boundary                                            | Evidence to retain                                               |
|---------------------------------------------------------|--------------------------------------------------------------|------------------------------------------------------------------|
| Excluded user installs or authorizes plugin             | Participant gate prevents effective access                   | User identity, group/permission assignments, attempt result      |
| User asks for an inaccessible account                   | Retrieval is denied or omits the restricted record           | Source-system access check and connector result                  |
| Approved record includes a prohibited field             | Field cannot be retrieved or changed under the admitted role | Effective field permissions and attempted request                |
| Reviewer selects Deny                                   | No related Salesforce write occurs                           | Decision, operation identifier, destination query                |
| "Always allow" selected, then session or record changes | Behavior matches the documented pilot policy                 | Subsequent prompts, tool restrictions, observed approvals        |
| Slack/email contains instructions to change CRM         | Retrieved content cannot bypass action authorization         | Input, proposed action, permission result                        |
| Write times out or partly completes                     | No blind retry; ambiguous state is reconciled first          | Each operation's observed destination state                      |
| Concurrent user edits the same record                   | Stale proposal is detected or workflow is withheld           | Proposal version, later record state, accepted or blocked result |

Permission tests should establish enforcement outside the model's generated explanation. OWASP advises downstream authorization and minimizing extension privileges. ([genai.owasp.org](https://genai.owasp.org)) Include an ordinary authorized user with a deliberately broader read scope than the admitted pilot workflow, so the team can see whether additional controls actually constrain access. ([www.cyber.gov.au](https://www.cyber.gov.au))

Separate prompt-injection tests from factual-accuracy tests. In the former, untrusted source content attempts to redirect an action; in the latter, the proposed values are wrong or unsupported. Both need a clear reviewer decision, but only system-level authorization can establish whether a disallowed operation was prevented. Human review remains a separate control. ([genai.owasp.org](https://genai.owasp.org))

A timeout is an **unknown outcome** until reconciled. The HTTP semantics standard advises against automatic retries of non-idempotent requests unless the client knows they are safe or knows the original was not applied. ([www.rfc-editor.org](https://www.rfc-editor.org)) This general principle does not prove that the Salesforce connector exposes idempotency keys or protects against duplicate creation.

Before live admission, require evidence for these exit criteria:

- **Identity:** The actor remains attributable throughout the request and destination change. ([oecd.ai](https://oecd.ai))
- **Authorization:** Excluded users, objects, and fields remain inaccessible through tested paths. ([www.rfc-editor.org](https://www.rfc-editor.org))
- **Review:** The proposed change and final decision can be reconstructed. ([airc.nist.gov](https://airc.nist.gov))

- **Correctness:** The committed values match the approved version, including required destination controls. ([airc.nist.gov](https://airc.nist.gov))
- **Recovery:** The team has demonstrated access revocation and correction on representative test records, retaining evidence of the actions. ([www.cyber.gov.au](https://www.cyber.gov.au))

## Audit Evidence, Monitoring, and Rollback

A usable audit trail must connect a proposal, the actor's decision, the tool operation, and the committed destination state. Australia's cyber security guidance recommends recording prompts, responses, tool invocations, approvals, actions, security events, and configuration changes. This is a useful evidence specification, not confirmation that the beta supplies all those fields. ([www.cyber.gov.au](https://www.cyber.gov.au))

Claude's Enterprise audit logs exclude chat and project titles and content. ([support.claude.com](https://support.claude.com)) The Compliance API separately provides programmatic access to activity events, chat data, and file content, enabled by the Primary Owner. ([support.claude.com](https://support.claude.com)) Neither description establishes complete Salesforce approval events, field-level before/after values, or destination transaction identifiers. Test export content before relying on it.

Build a reconciliation worksheet with the following columns:

- **Proposal identity:** Unique operation identifier, proposal version, reviewer, and decision timestamp.
- **Destination identity:** Salesforce organization, object, record, and requested fields.
- **Approved delta:** Previous values observed, proposed values, and evidence used.
- **Commit evidence:** Result, verified current values, observed time, and associated destination evidence.
- **Exception:** Rejected, failed, pending, ambiguous, mismatched, or corrected.
- **Recovery:** Corrective action, approving owner, completion evidence, and elapsed effort.

This worksheet operationalizes traceability rather than assuming the conversation is the authoritative transaction record. The Organisation for Economic Co-operation and Development's (OECD) AI accountability principle calls for traceability across datasets, processes, and decisions. ([oecd.ai](https://oecd.ai)) For records within Part 11 scope, changes must not obscure previously recorded information; ([www.ecfr.gov](https://www.ecfr.gov)) keeping only the latest chat answer would not establish that requirement.

Distributed tracing offers useful design language: OpenTelemetry describes correlating spans into a trace, ([opentelemetry.io](https://opentelemetry.io)) and W3C Trace Context standardizes request correlation across systems. ([www.w3.org](https://www.w3.org)) Use a common operation identifier where supported, or a controlled external ledger where it is not. These standards do not establish native beta instrumentation. Avoid placing sensitive record contents in identifiers.

Salesforce history requires field-specific assessment. Its developer guide excludes several field types from Field Audit Trail tracking, including long text. ([developer.salesforce.com](https://developer.salesforce.com)) A workflow centered on narrative call notes therefore needs a proven content-evidence route; the existence of field history alone does not establish reconstruction of the approved text.

Define **rollback as a controlled recovery procedure**, not a product promise. A corrective update can itself trigger business automation, and removing a record may affect linked records or retained evidence. Test the full effect of corrections instead of assuming an inverse field update restores the entire prior business state.

Preserve original evidence and obtain approval for the correction. ([www.ecfr.gov](http://www.ecfr.gov)) ([genai.owasp.org](http://genai.owasp.org))

The incident procedure should suspend affected workflows, preserve evidence, reconcile ambiguous operations, revoke access if necessary, and authorize recovery. Salesforce documents revocation of individual tokens, a user's application tokens, or all application tokens. ([help.salesforce.com](https://help.salesforce.com)) Rehearse those paths and verify loss of effective access; removing a visible plugin alone is insufficient evidence of revocation. ([www.cisa.gov](http://www.cisa.gov))

## Data Analysis and Evidence

The available product evidence describes scope and controls, not a quantified pharmaceutical productivity outcome. This research did not establish an independent pharma-specific benchmark for accuracy, reviewer burden, error rate, or recovery time. The **37 skills** are an inventory count, not measured performance. Use the tenant's own observations as the quantitative basis for expansion. ([help.salesforce.com](https://help.salesforce.com))

Retention figures show why evidence design needs separate clocks. Claude documents an Enterprise audit export spanning **180 days**. ([support.claude.com](https://support.claude.com)) Salesforce's training documentation describes standard tracking for **20 fields per object**, history retained for **18 months** in the user interface and available for up to **24 months** through the API. It describes Field Audit Trail as extending tracking to **up to 200 fields per object** with indefinite storage capability. ([trailhead.salesforce.com](https://trailhead.salesforce.com)) These are documented capabilities, not proof that a particular organization's configuration preserves every necessary field or narrative.

Before collecting metrics, define an **atomic intended operation**: one identified record and a versioned set of proposed changes. Count records or operations consistently, rather than mixing fields, conversations, and tool calls. Correlation concepts from OpenTelemetry and W3C support distinguishing one business operation from the requests used to perform it. ([opentelemetry.io](https://opentelemetry.io)) ([www.w3.org](http://www.w3.org))

The following worksheet is an analytical design, with all values supplied by the reader. Let **P** be proposed operations, **A** finally approved, **R** finally rejected, **C** distinct approved operations whose commitment was verified, **E** erroneous committed operations, **M** recorded reviewer minutes, and **T** recorded reversal minutes.

- **Approval rate:**  $A/P$ . **Rejection rate:**  $R/P$ . Report both numerator and denominator.
- **Unresolved proposal share:**  $(P - A - R)/P$ , provided final dispositions are mutually exclusive.
- **Confirmed commitment rate:**  $C/A$ . Separate pending, failed, and ambiguous outcomes.
- **Observed committed error rate:**  $E/C$  only when every committed operation was assessed. Otherwise use the assessed subset as denominator and disclose coverage.
- **Review minutes per disposition:**  $M/(A + R)$ , when  $M$  covers those decisions.  $M/P$  answers a different workload question.
- **Recorded review and reversal burden:**  $M + T$ . This is not net time saved without a measured baseline and the other work categories.
- **Reversal reporting:**  $T$  alone is total effort. A mean reversal time requires the completed reversal count or individual observations.

Multiply a rate by 100 to report a percentage. Treat a zero denominator as not applicable, not a measured zero rate. Version edited proposals and state whether P counts versions or original requests. Record any unapproved committed operation separately rather than including it inside C/A.

Evaluate these observations against thresholds agreed before the pilot. NIST recommends measurement and continuing assessment, while human-oversight processes should be defined and documented. A favorable approval rate cannot substitute for complete reconciliation, and a low observed error rate cannot establish that untested fields or workflows are safe. ([airc.nist.gov](https://airc.nist.gov))

## Implications and Future Directions

The immediate implication is to admit **bounded use cases**, not the plugin as an unrestricted category. A controlled read-only pilot can answer questions about identity, retrieval boundaries, contextual accuracy, and data movement. Draft generation can then assess review quality. Writes should follow only where authorization, approval, destination verification, and recovery have been demonstrated. This ordering follows phased-adoption and human-oversight guidance. ([www.cyber.gov.au](https://www.cyber.gov.au)) ([airc.nist.gov](https://airc.nist.gov))

For the publisher's advisory perspective, the useful deliverable is an evidence pack that commercial operations, security, privacy, and quality owners can all inspect. IntuitionLabs belongs in that discussion as an adjacent adviser, not a competing CRM product or a source certifying the beta's suitability.

Use these decisions:

- **Go for restricted reading:** Named participants, approved data, effective permission boundaries, and acceptable destination handling.
- **Go for a specific write:** Proven object/field behavior, stable approval policy, retained delta, verified destination result, and rehearsed recovery.
- **Hold the write workflow:** Conflicting documentation, ambiguous tools, persistent approval bypass, incomplete evidence, or unproven correction.
- **Exclude the process:** Patient, medical-information, consent-change, or regulated-record use that lacks a separate admission decision.

These are proposed decision rules. Their application should follow the organization's documented risk assessment, with record applicability assessed separately from commercial usefulness. FDA's Part 11 guidance supports justified, documented risk assessment within its applicable context; it does not confer validation status on the integration. ([www.fda.gov](https://www.fda.gov))

The roadmap should revisit unresolved requirements when documentation or installed behavior changes: exact object schemas, Slack/email scopes, approval persistence, beta terms, regional processing, evidence exports, and pharma-cloud compatibility. General MCP security guidance and OAuth standards are useful review criteria, but neither certifies a particular deployment. ([modelcontextprotocol.io](https://modelcontextprotocol.io)) ([www.rfc-editor.org](https://www.rfc-editor.org))

Finally, align retention and access reviews with data purpose. The European Commission describes storage limitation as keeping personal data no longer than necessary. ([commission.europa.eu](https://commission.europa.eu)) A retention schedule should reconcile that principle with applicable record obligations and actual evidence needs, rather than retaining every prompt indefinitely.

## Conclusion

**Salesforce in Claude can be evaluated for pharmaceutical commercial operations only through a defined data and action boundary.** The evidence reviewed supports a staged assessment, while leaving material implementation questions for tenant-level confirmation. In particular, conflicting descriptions of draft-only skills and approved write tools make demonstrated behavior essential before write admission.

The recommended pilot begins with named users, selected commercial fields, and effective read restrictions. It progresses to drafts and then to explicitly approved operations only when the record, proposed delta, reviewer decision, destination result, and correction route can be connected. Patient information and regulated processes require separate decisions and must not enter the pilot through unrestricted notes or collaboration context.

Success should be expressed in observed denominators: proposed, approved, rejected, committed, assessed, erroneous, and corrected operations, together with recorded review and recovery effort. Those measurements describe the admitted workflow; they do not justify claims about broader productivity or compliance.

The final go/no-go decision belongs to the accountable process owners reviewing the evidence pack. A workflow with incomplete permissions, approval, reconciliation, or recovery evidence should remain outside write scope. Expansion becomes defensible when the team can show what was allowed, what actually happened, and how the resulting state was checked and corrected.

## Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. <https://claude.com/blog/salesforce-in-claude>
2. <https://support.claude.com/en/articles/16952184-set-up-salesforce-in-claude-for-your-organization>
3. [https://help.salesforce.com/s/articleView?id=sales.what\\_is\\_salesforce\\_in\\_claude.htm&language=en\\_US&type=5](https://help.salesforce.com/s/articleView?id=sales.what_is_salesforce_in_claude.htm&language=en_US&type=5)
4. [https://help.salesforce.com/s/articleView?id=ai.set\\_tool\\_restrictions.htm&language=en\\_US&type=5](https://help.salesforce.com/s/articleView?id=ai.set_tool_restrictions.htm&language=en_US&type=5)
5. <https://support.claude.com/en/articles/16952186-use-salesforce-in-claude>
6. <https://support.claude.com/en/articles/13837433-manage-plugins-for-your-organization>
7. <https://genai.owasp.org/llmrisk/llm062025-excessive-agency>
8. <https://privacy.claude.com/en/articles/8114513-business-associate-agreements-baa-for-commercial-customers>
9. <https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B/section-11.10>
10. <https://support.claude.com/en/articles/9970975-access-audit-logs>
11. <https://trailhead.salesforce.com/content/learn/modules/field-audit-trail-basics/get-started-with-field-audit-trail>
12. [https://help.salesforce.com/s/articleView?id=ai.security\\_permissions\\_and\\_data\\_handling.htm&language=en\\_US&type=5](https://help.salesforce.com/s/articleView?id=ai.security_permissions_and_data_handling.htm&language=en_US&type=5)
13. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application>
14. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/computer-software-assurance-production-and-quality-management-system-software>
15. <https://www.gov.uk/government/publications/data-ethics-framework/data-and-ai-ethics-framework>

16. <https://www.cisa.gov/news-events/alerts/2024/04/15/joint-guidance-deploying-ai-systems-securely>
17. [https://help.salesforce.com/s/articleView?id=sales.skills\\_ref.htm&language=en\\_US&type=5](https://help.salesforce.com/s/articleView?id=sales.skills_ref.htm&language=en_US&type=5)
18. [https://help.salesforce.com/s/articleView?id=sales.salesforce\\_in\\_claude\\_record\\_crud.htm&language=en\\_US&type=5](https://help.salesforce.com/s/articleView?id=sales.salesforce_in_claude_record_crud.htm&language=en_US&type=5)
19. <https://www.cyber.gov.au/advisory/agentic-ai-harnesses>
20. [https://modelcontextprotocol.io/docs/2025-11-25/tutorials/security/security\\_best\\_practices](https://modelcontextprotocol.io/docs/2025-11-25/tutorials/security/security_best_practices)
21. [https://help.salesforce.com/s/articleView?id=ai.create\\_and\\_configure\\_the\\_eca.htm&language=en\\_US&type=5](https://help.salesforce.com/s/articleView?id=ai.create_and_configure_the_eca.htm&language=en_US&type=5)
22. <https://trailhead.salesforce.com/content/learn/modules/salesforce-in-claude-for-admins/get-to-know-salesforce-in-claude>
23. <https://www.rfc-editor.org/rfc/rfc9700.html>
24. <https://slack.com/help/articles/54548358406419-Manage-access-to-the-Slack-MCP-server-through-your-identity-provider>
25. <https://slack.com/intl/en-nz/help/articles/48855576908307-Guide-to-Model-Context-Protocol-in-Slack>
26. <https://cnil.fr/en/defining-purpose>
27. <https://oecd.ai/en/dashboards/ai-principles/P9>
28. <https://airc.nist.gov/airmf-resources/airmf/5-sec-core>
29. [https://help.salesforce.com/s/articleView?id=platform.fields\\_about\\_field\\_validation.htm&language=en\\_US&type=5](https://help.salesforce.com/s/articleView?id=platform.fields_about_field_validation.htm&language=en_US&type=5)
30. [https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/principles-gdpr\\_en](https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/principles-gdpr_en)
31. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai>
32. [https://www.edpb.europa.eu/news/edpb-opinion-on-ai-models-gdpr-principles-support-responsible-ai\\_en](https://www.edpb.europa.eu/news/edpb-opinion-on-ai-models-gdpr-principles-support-responsible-ai_en)
33. <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>
34. <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html>
35. <https://support.claude.com/en/articles/15422948-enable-us-only-inference-for-your-organization>
36. <https://privacy.claude.com/en/articles/7996868-is-my-data-used-for-model-training>
37. <https://privacy.claude.com/en/articles/7996866-how-long-do-you-store-my-organization-s-data>
38. <https://www.ema.europa.eu/en/human-regulatory-overview/research-development/compliance-research-development/good-clinical-practice/qa-good-clinical-practice-gcp>
39. <https://www.rfc-editor.org/rfc/rfc9110.html>
40. <https://support.claude.com/en/articles/13015708-access-the-compliance-api>
41. <https://opentelemetry.io/docs/concepts/signals/traces>
42. <https://www.w3.org/TR/trace-context>
43. <https://developer.salesforce.com/docs/platform/field-history-retention/guide/field-audit-trail.html>
44. [https://help.salesforce.com/s/articleView?id=sf.manage\\_external\\_client\\_app\\_usage.htm&language=en\\_US&type=5](https://help.salesforce.com/s/articleView?id=sf.manage_external_client_app_usage.htm&language=en_US&type=5)

## THE PUBLISHER

# About IntuitionLabs

IntuitionLabs is an AI consulting, custom software development and data engineering firm serving pharmaceutical, biotechnology, medical-device and other life-science organizations. We work with clinical, regulatory, medical-affairs, commercial, quality and IT teams to connect technology decisions with the work people need to accomplish.

## AI consulting and adoption

Our AI enablement services cover readiness assessments, use-case selection, governance and policies, team workshops, adoption measurement and ongoing advisory support. We help organizations structure the information layer behind AI: source material, context, permissions and maintained knowledge that make generated answers useful and reviewable. Private LLM inference and hosted AI options support teams evaluating how to operate AI with appropriate control over their data and infrastructure.

## Software, data and life-science workflows

IntuitionLabs develops custom software for pharma and biotech, integrates enterprise systems, and builds data engineering and business intelligence solutions. Areas of focus include AI agents, regulatory research, medical writing, medical affairs, CMC information, competitive intelligence and clinical-document workflows. Our eTMF intelligence work includes cross-system reconciliation and inspection-readiness support.

## Enterprise platforms and regulated delivery

We provide Veeva services, application support, managed services, integrations and custom applications, alongside enterprise content work involving platforms such as Egnyte. For regulated workflows, our services include GxP enablement, computer-system validation and software development addressing 21 CFR Part 11 requirements. The applicable controls, validation responsibilities and acceptance criteria are defined for each engagement.

## Work with IntuitionLabs

Explore [AI enablement](#), [pharma and biotech software development](#), [data engineering and BI](#), and [Veeva services](#). [Contact IntuitionLabs](#) to discuss your workflow, information sources and implementation needs.

IntuitionLabs publishes educational research to help life-science teams make informed technology decisions. Coverage of a product or organization does not imply a client relationship, endorsement or partnership.

**Website:** <https://intuitionlabs.ai>

---

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.