IntuitionLabs

INTUITIONLABS / RESEARCH & PRACTICAL GUIDANCE

Claude Enterprise Pharma Data Security: EFS Analysis

> 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 · 2026-09-19 · claude enterprise pharma data security · enterprise frontier safeguards · claude efs · pharma ai governance · zero data retention · hipaa readiness · customer-managed encryption keys · pharma data custody · anthropic enterprise

Original article: https://intuitionlabs.ai/articles/claude-enterprise-pharma-data-safeguards

In this article

Executive Summary

Enterprise Frontier Safeguards (EFS) changes one important part of the Claude Enterprise pharma data security decision: it gives eligible customers a proposed way to use covered frontier models while keeping monitoring activity in customer-controlled cloud storage. Anthropic announced EFS on **September 1, 2026**, with phased access beginning later in fall 2026 (anthropic.com). The access form describes broad availability as a goal, not a committed date, and says a request does not guarantee access (claude.com). As of **September 19, 2026**, a pharma buyer should therefore treat EFS as a gated, phased capability to qualify, not a generally available control already present in every Claude contract.

The design separates custody, detection, and disposition. Activity data can be held in the customer's Amazon S3, Azure Blob Storage, or Google Cloud Storage environment under customer keys, policies, and audit logging. Automated systems analyze a rolling traffic window, then route signals to customer personnel; human review is by default performed by the customer rather than Anthropic (anthropic.com) (anthropic.com). This is material for drug-safety reports, confidential research and development, and other content whose review may need to remain with cleared customer staff. It does not eliminate the need to establish what fields are stored, how long they persist, where detection executes, what a signal contains, or whether any exceptional access path exists.

EFS is also not interchangeable with **zero data retention (ZDR)**, **Health Insurance Portability and Accountability Act (HIPAA) readiness**, a **Business Associate Agreement (BAA)**, good practice validation, electronic-record controls, or model-output review. Covered Model prompts and outputs normally require **30-day** retention for safety work (support.claude.com). A standard Claude Enterprise plan does not automatically include BAA coverage (support.claude.com). FDA guidance separately ties validation scope to intended use and documented risk assessment (fda.gov).

The decision is consequently conditional. Request access now when covered models are strategically necessary and customer-owned review resolves a named custody blocker. Pilot only with low-risk or de-identified content until the contract, data map, retention schedule, key model, alert interface, cloud geography, and evidence package are explicit. Wait when the workload requires guaranteed availability, a published EFS technical specification, validated regulated-record handling, or BAA scope that has not been confirmed.

Anthropic charges no separate EFS fee, but the customer pays cloud storage, read, write, and egress charges (anthropic.com). The sound economic test is therefore cost per monitored request or workload, not a guessed universal monthly price.

Introduction and Background

Pharma adoption of frontier models exposes a genuine architectural tension. Safety monitoring becomes more useful when activity can be correlated across requests and accounts, but a drug manufacturer may be unable to let an external reviewer inspect a pharmacovigilance narrative, unpublished molecule data, protocol material, or patient-linked clinical text. Anthropic explicitly includes **drug-safety reports** among information customers may reserve for their own cleared reviewers (anthropic.com). EFS addresses that custody conflict. It does not settle the wider question of whether the surrounding use case is lawful, validated, record-complete, or operationally safe.

This distinction matters because “pharma data” is not one regulatory class. Confidential research intellectual property may be commercially critical without being protected health information (PHI). An individual case safety report can include personal data, and ICH defines it as an observation concerning an individual patient at a particular time (database.ich.org). EMA likewise says EudraVigilance safety reports contain patient and primary-source personal data (ema.europa.eu). A generated quality record may become a regulated record because of its intended use. The HIPAA Security Rule, meanwhile, applies to electronic PHI maintained or transmitted electronically, not automatically to every secret held by a pharmaceutical company (hhs.gov).

This report evaluates EFS as a **division-of-responsibility architecture** for chief information security officers, privacy and AI-governance leaders, enterprise architects, legal and compliance teams, and platform owners. The perspective is implementation-focused. IntuitionLabs describes its role as connecting AI to authoritative sources with identity, permissions, retrieval, citations, evaluation, and accountable operation (intuitionlabs.ai). That adjacent advisory posture is relevant to qualification and integration, but IntuitionLabs is not an alternative to Claude and is therefore not placed in the product matrices.

Key Changes

Customer-controlled custody replaces a forced monitoring tradeoff

The central change is not merely another encryption option. EFS combines misuse detection with a custody pattern intended to preserve ZDR-like privacy. Anthropic says customers store their data on their own cloud infrastructure rather than its systems (anthropic.com). Under the announced pattern:

- **Inference:** The user or application sends a request to a supported Claude surface.
- **Activity capture:** Monitoring activity is retained in a customer cloud account.
- **Automated correlation:** Detection analyzes a rolling traffic window, rather than only an isolated prompt.
- **Signal delivery:** A suspected pattern produces a signal sent directly to the customer.
- **Human triage:** Customer-designated staff review and decide how to respond.

- **Disposition:** The customer applies its retention, evidence, escalation, and deletion rules, subject to the eventual EFS contract and implementation specification.

The architecture is attractive precisely because custody is not the same as visibility. Customer-owned storage can apply the customer's encryption keys, access policies, and logging controls (anthropic.com). Yet the public announcement does not specify whether detection reads plaintext outside the account, which service identity performs reads, or what content appears in a flag. These are qualification questions, not details to infer from the phrase “customer controlled.”

Three opt-in controls, not one indivisible package

Anthropic describes **customer-owned storage**, **customer-managed encryption keys (CMEK)**, and **fully automated review** as separately opt-in controls (anthropic.com). This creates configuration flexibility, but it also creates combinations that procurement teams must enumerate. The buyer should obtain a written state table showing where data resides, who may access it, who reviews flags, and what retention rule applies for every selected combination.

Do not assume that generic Claude Enterprise CMEK and EFS CMEK have identical scope. Current Claude documentation says Anthropic retains no copy of a customer's key, while the customer controls rotation, audit, and revocation (platform.claude.com). The same page also says Activity Feed, audit-log, and telemetry data remain under Anthropic-managed encryption (platform.claude.com). Until EFS documentation maps each dataset to each key boundary, buyers should not project the generic CMEK coverage table onto EFS activity data.

Phased access and temporary ZDR

EFS was announced for Claude Code, Claude Enterprise, Claude Platform, Amazon Bedrock, Claude Platform on AWS, Google Agent Platform, and Microsoft Foundry. Support on a slide or announcement is not the same as operational availability. Anthropic's Covered Models page calls the pre-EFS ZDR route time-limited and transitional (support.claude.com). AWS is more specific for Bedrock, documenting temporary ZDR for eligible EFS customers through **December 31, 2026** (docs.aws.amazon.com).

The transition needs its own change plan. A platform owner should record the current ZDR authorization, its end date, the workspace or account scope, the model list, and the precise event that moves the workload to EFS. Anthropic states that a ZDR organization can enable **30-day retention** only for a specific workspace while other workspaces keep ZDR (platform.claude.com). That can support segmentation, but it is not a substitute for confirming EFS eligibility.

EFS Reference Architecture and Control Boundaries

Data flow and accountable owners

Table 1 summarizes the announced flow and the evidence a regulated buyer should demand. “Customer controlled” is treated as a control objective that must be demonstrated in the selected cloud, not as a blanket compliance conclusion.

Stage or data element	Expected location and actor	Customer control and evidence	Open qualification question
Inference prompt and output	Depends on direct Claude or cloud-partner surface. Bedrock keeps retained review data inside AWS, while Microsoft says Anthropic acts as an independent processor for Claude prompts and outputs in Foundry (docs.aws.amazon.com) (learn.microsoft.com).	Approved endpoint, network boundary, data-processing agreement, regional route, input classification.	Which legal entity and subprocessor touches each copy, and in which geography?
EFS activity record	Announced for the customer's S3, Blob Storage, or Cloud Storage account.	Bucket or container policy, CMEK policy, object-access logs, lifecycle rule, immutable evidence path.	What fields and content are written, in what format, and at what sampling rate?
Automated detection	Anthropic-operated logic analyzes a rolling traffic window.	Service identity, least privilege, network path, read log, version and performance change record.	Where does execution occur, and does plaintext leave the account?
Signal	Routed to customer staff for triage.	Authenticated delivery, severity taxonomy, case identifier, timestamps, evidence pointer, service-level target.	What is the payload, latency, false-positive measure, and delivery guarantee?
Human review	Customer reviewer by default, with no Anthropic review required.	Role-based access, clearance rules, dual control for sensitive cases, training, audit trail.	Are exceptional vendor access, legal process, or support-access paths possible?
Disposition record	Customer case-management or security operations system.	Decision, reason, linked evidence, containment, notification analysis, retention and deletion.	Which record is authoritative when EFS, security, privacy, and quality cases overlap?

The table shows why EFS is best understood as an interface between two control systems. Anthropic supplies detection and a signal. The customer supplies the storage security, reviewer, triage process, evidence record, and downstream response. NIST recommends defining ownership and rehearsing incident-response functions for third-party generative AI systems (nvlpubs.nist.gov). The practical consequence is that an EFS alert should enter an established security and privacy workflow, not an unowned mailbox.

Surface and cloud-provider availability

Table 2 separates announced EFS support from the standard controls providers currently document. It should be refreshed during contracting because public EFS operational material remains incomplete.

Surface	EFS announcement status	Current documented custody or monitoring baseline	Decision note as of September 19, 2026
Claude Enterprise and Claude Code	Announced as supported.	Enterprise custom retention is indefinite by default unless configured, with a **30-day minimum** for custom periods (support.claude.com).	Confirm whether the particular interface, organization, and covered model are enabled. Claude Teams and Enterprise interfaces are not generally ZDR-eligible apart from documented Claude Code arrangements (platform.claude.com).
Direct Claude Platform	Announced as supported.	ZDR means prompts and responses are not stored at rest after the API response (platform.claude.com). Covered Models require retention unless expressly authorized.	Obtain the organization-level entitlement and a feature-by-feature eligibility schedule.
Claude Platform on AWS	Announced as supported.	Anthropic-operated; Anthropic's HIPAA-ready program is not available on this surface (platform.claude.com).	Do not confuse an AWS hosting location with AWS being the inference-data processor. Confirm ZDR terms separately.
Amazon Bedrock	Announced as supported.	none mode writes no request or response to durable AWS storage; models requiring review use up to **30 days** inside AWS (docs.aws.amazon.com) (docs.aws.amazon.com).	AWS describes bring-your-own-bucket and CMEK as planned EFS capabilities, so require the operational release evidence.
Google Agent Platform	Announced as supported.	Standard Advanced AI monitoring retains prompts and responses up to **30 days** in the selected region or multi-region (docs.cloud.google.com). Standard monitoring logs are not covered by CMEK (docs.cloud.google.com).	Require written confirmation of what EFS changes, because generic monitoring is not the announced EFS design.
Microsoft Foundry	Announced as supported.	Hosted-on-Azure prompts and outputs run on Azure; Anthropic-hosted deployments may process outside Azure and the selected region (learn.microsoft.com) (learn.microsoft.com).	Select the hosting option first, then qualify EFS. Generic Foundry CMK and diagnostics are not proof of EFS behavior.

The matrix exposes a frequent procurement error: cloud brand does not determine the full custody chain. Surface, hosting option, model, retention mode, organization entitlement, geography, and feature set all matter. Google warns that global endpoints provide no data-residency guarantee (docs.cloud.google.com); AWS says retained cross-region inputs and outputs are stored in the destination region (docs.aws.amazon.com). Architecture review must therefore use actual request routes, not just contract logos.

Pharma Data Classification and Compliance Boundaries

Route data by intended use, not by a single “sensitive” label

Table 3 provides a routing matrix. It is a starting point for a company-specific data inventory, not legal advice or a universal classification.

Data class	Primary concern	EFS pilot posture	Additional controls before production
Non-public R&D intellectual property	Confidentiality, trade-secret handling, export and collaboration restrictions.	Pilot with synthetic or compartmentalized material.	Named project access, retrieval filtering, output leak testing, contractual use restrictions, regional route.
Drug-safety report	Personal data, pharmacovigilance workflow, source fidelity, reporting deadlines.	De-identify where possible; customer pharmacovigilance staff triage EFS flags.	Preserve source record and lineage. ICH says an expedited report may be due within **15 calendar days** after day zero (database.ich.org).
Clinical-trial data	Participant protection, protocol context, metadata, sponsor oversight, system validation.	Use a segregated workspace and approved data subset.	ICH expects data and metadata to remain protected from unauthorized access and alteration throughout retention (database.ich.org).
PHI or electronic PHI	HIPAA role, minimum necessary, BAA scope, security controls.	Do not process until the exact organization, feature, model, and interface are BAA-covered.	HHS requires systems containing electronic PHI to record and examine activity (hhs.gov). Apply role-based access to only the minimum PHI needed for the purpose (hhs.gov).
GxP or Part 11 record	Intended use, predicate rule, attributable and complete record, audit trail, validation.	Keep model output non-authoritative until validated within the end-to-end process.	Part 11 applies when required records are kept electronically instead of paper (fda.gov). Preserve required metadata and approvals.
Public or approved content	Accuracy, provenance, copyright, medical and promotional review where applicable.	Suitable for early technical testing.	Retrieval citations, output evaluation, approved-source controls, human approval before regulated use.

The classification step determines whether EFS resolves the binding issue. For R&D intellectual property, customer-controlled review may directly reduce a custody objection. For PHI, it cannot replace a BAA or HIPAA security analysis. HHS says a BAA limits the service provider's permitted uses and disclosures of PHI (hhs.gov). Anthropic says its BAA covers only the organization that accepted it and that not all API features are covered (support.claude.com) (support.claude.com).

For regulated records, EFS is a security-monitoring control, not a record system. FDA defines an audit trail as a secure, computer-generated, time-stamped record that permits event reconstruction (fda.gov). The EFS public description does not claim electronic signatures, record versioning, contemporaneous attribution, or predicate-rule retention. ICH E6(R3) likewise places ultimate responsibility for delegated trial activities with the sponsor (database.ich.org). Moving review to customer staff changes who sees the monitoring data, not who owns trial governance.

GDPR analysis also remains separate. Personal data must be limited to what is necessary and retained in identifiable form no longer than needed for the purpose (eur-lex.europa.eu) (eur-lex.europa.eu). A controller must use processors that provide sufficient guarantees for appropriate technical and organizational measures (eur-lex.europa.eu). Customer-owned storage helps with technical control, but it does not by itself determine legal roles, subprocessors, transfers, or deletion duties.

EFS, ZDR, standard retention, HIPAA readiness, and compliance telemetry

These labels answer different questions:

- **Standard API retention:** Anthropic normally deletes API inputs and outputs from backend systems within **30 days** (privacy.claude.com). Saved enterprise product content follows product and organization settings.
- **Covered Model retention:** Prompts and outputs are retained for **30 days** for safety work, with model policies following the model across surfaces (support.claude.com).
- **ZDR:** For eligible API behavior, prompts and responses are not stored at rest after the response. Stateful features can remain ineligible, and Covered Models require express authorization.
- **EFS:** Monitoring continuity is preserved while activity storage and human review move toward customer control. It is intended to address safety monitoring for covered frontier models, not every product-retention category.
- **HIPAA readiness and BAA:** These are organization, product, feature, and contract-specific. HIPAA readiness adds broader privacy and security safeguards than ZDR (platform.claude.com).
- **Compliance API and Activity Feed:** The feed records who did what and when but not prompt text or model responses (platform.claude.com). It retains events for **six years**, with new events queryable within **one minute** (platform.claude.com).
- **Access Transparency:** This records covered human vendor access, not automated processing, and events may take up to **two business days** to appear (platform.claude.com) (platform.claude.com).

The result is a layered evidence model. EFS activity data may support safety triage. The Activity Feed supports administrative accountability. Cloud audit logs show object, key, and service access. Application telemetry shows user and workload context. A validated system of record preserves regulated content and approvals. None is a complete substitute for the others.

Implementation Considerations and Process Changes

Contract and architecture questions before a pilot

A qualification package should answer the following in writing:

- **Eligibility:** Which legal entity, organization, workspace, account, subscription, project, model, region, and interface are approved?

- **Timeline:** What phase is contracted, when does access start, and what happens to temporary ZDR if EFS is delayed?
- **Stored fields:** Are full prompts and outputs stored, or a subset, sample, hash, embedding, classifier feature, or metadata record?
- **Retention:** What is the default and configurable period, deletion lag, backup behavior, preservation rule, and legal-hold process?
- **Keys:** Which customer key protects which object, which principal can decrypt, and how are rotation, revocation, caching, and recovery tested?
- **Detection:** Where does analysis execute, what network path reads activity, which model or classifier version applies, and how are material changes communicated?
- **Signals:** What fields, severity levels, confidence values, evidence pointers, delivery method, latency target, retry behavior, and service commitment apply?
- **Human access:** Which customer roles can review? Can any Anthropic or cloud-provider human access content under support, exception, or legal-process conditions?
- **Residency and transfers:** Where do inference, storage, detection, backup, support, and telemetry occur, including cross-region failover?
- **Subprocessors:** Which parties handle each data category, and how are changes notified and assessed?
- **Assurance:** Which independent reports, penetration-test summaries, architecture diagrams, control mappings, and business-continuity evidence cover the EFS components?
- **Exit:** How are activity data, keys, signals, cases, and derived artifacts exported or destroyed at termination?

Contract review must be as specific as the architecture review. Anthropic's current commercial terms put responsibility on the customer to decide whether outputs are appropriate, including whether human review is needed (anthropic.com). Its Data Processing Addendum identifies the customer as controller and Anthropic as processor for customer personal data (anthropic.com). The same addendum provides **15 days** after notice to object to a new subprocessor on reasonable privacy or security grounds and says external auditors assess Anthropic annually against established standards (anthropic.com) (anthropic.com). Buyers should reconcile those baseline terms with any EFS-specific schedule, cloud-provider terms, and BAA.

Assurance evidence should also be scoped, not name-checked. Anthropic lists **ISO 27001:2022** for information-security management, **ISO/IEC 42001:2023** for AI management systems, and SOC 2 Type I and Type II (support.claude.com) (support.claude.com) (support.claude.com). The qualification question is whether the EFS components, locations, and operational processes are within the relevant report or certificate boundary.

This list should be turned into acceptance tests. For example, revoke a non-production key and observe access loss, rotate it and confirm recovery, issue a synthetic signal and verify routing, test duplicate and delayed deliveries, and show that an unauthorized reviewer cannot open the underlying object. Anthropic documents that ordinary CMEK revocation may take up to **one hour** because of key caching (platform.claude.com). EFS-specific timing should be measured independently rather than assumed to match.

Responsibility model and incident playbook

The operating model should assign one accountable owner per decision:

- **Platform owner:** configures the surface, entitlement, storage destination, regional routing, and service integration.
- **Cloud security:** owns bucket or container policy, CMEK, service identities, private connectivity, audit logs, and lifecycle controls.
- **Security operations:** receives the signal, enriches it, preserves evidence, contains credentials or sessions, and coordinates response.
- **Privacy:** determines personal-data scope, minimization, processor terms, transfer basis, data-subject implications, and deletion requirements.
- **Quality or validation:** decides whether the workflow affects a regulated record, defines intended use, risk assessment, testing, change control, and periodic review.
- **Pharmacovigilance or clinical owner:** interprets domain context, protects reporting timelines, and decides whether source or safety records are affected.
- **Legal and procurement:** owns contractual scope, BAA or data-processing terms, subprocessor review, preservation, support access, and exit rights.
- **Model-risk owner:** evaluates output quality, prohibited uses, red-team coverage, drift, and human-oversight design.

An alert runbook should capture the signal identifier, detection time, relevant account and model, storage object reference, access-log snapshot, classifier version if available, reviewer identity, triage result, containment action, privacy and quality assessments, notification decision, and closure evidence. NIST says all six Cybersecurity Framework functions have roles in incident response (nvlpubs.nist.gov). CISA identifies centralized logging as an enabler of better incident response (cisa.gov). Together, these support a process spanning governance, identification, protection, detection, response, and recovery, rather than treating flag review as a single analyst task.

Request now, pilot, or wait

Request access now when covered-model capability is required, the present blocker is external human review or vendor-side custody, and the organization can supply cloud engineering plus trained reviewers. The request should still be conditional on a written architecture and data-handling schedule.

Pilot when EFS appears directionally suitable but field schemas, signal quality, or operating costs remain uncertain. Start with public, synthetic, or de-identified inputs; cap users and models; isolate the workspace; define success measures; and keep generated outputs outside authoritative GxP or safety systems. IntuitionLabs' stated implementation approach is to select one department, govern a small workflow portfolio, and scale from observed evidence (intuitionlabs.ai). That is a proportionate pattern for EFS evaluation.

Wait when the use case requires a generally available feature, a published implementation guide, a fixed residency statement, proven alert integration, or BAA and validation scope that the available documents do not establish. Waiting is also appropriate when the enterprise cannot staff customer review. EFS intentionally transfers that work; it does not make the need disappear.

Data Analysis and Evidence

What is quantified, and what is not

The public record provides several decision-relevant quantities: **September 1, 2026** announcement; phased access later in fall; more than **100** design participants; ordinary Covered Model retention of **30 days**; Bedrock temporary ZDR through **December 31, 2026**; Compliance API Activity Feed retention of **six years**; new Activity Feed events within **one minute**; and Access Transparency delivery within **two business days**.

These figures describe availability, retention, and telemetry. They do not establish EFS detection accuracy, false-positive rate, alert latency, event size, reviewer workload, or outcomes. Collaboration with more than **100 customers** is design-input evidence, not adoption or effectiveness evidence (anthropic.com). A pilot should therefore measure:

- **Coverage:** monitored requests divided by eligible requests.
- **Signal rate:** signals per 1,000 monitored requests, segmented by model, workflow, and data class.
- **Triage precision:** confirmed actionable signals divided by reviewed signals.
- **Time to review:** median and 95th-percentile time from signal creation to a documented decision.
- **Evidence completeness:** cases containing every required field divided by closed cases.
- **Custody exceptions:** vendor or provider human accesses, cross-region writes, or objects outside the approved key policy.
- **Unit cost:** EFS-related cloud cost per 1,000 monitored requests and per reviewed signal.

NIST recommends regular reassessment of both metric suitability and control effectiveness (airc.nist.gov). The program should consequently set thresholds before the pilot, then review whether the measures still represent the actual risk.

Reader-input cloud log-cost worksheet

Anthropic says EFS has no separate vendor fee, while cloud storage, reads, writes, and egress remain customer charges. A portable monthly estimate is:

```
Monthly bytes = event volume per day × average record bytes × retention days

Storage GB-month = monthly bytes ÷ 1,000,000,000

Storage cost = Storage GB-month × applicable storage rate

Write cost = write requests ÷ provider billing unit × write-request rate

Read cost = read requests ÷ provider billing unit × read-request rate

Egress cost = egress GB × applicable destination and regional rate

Key cost = active-key charge + cryptographic operations × operation rate

Observability cost = ingested log GB + retained log GB-month + query or scan charges

Total EFS cloud cost = storage + writes + reads + egress + keys + observability +
replication
```

Each input must come from the expected EFS schema, pilot telemetry, selected region, storage class, redundancy option, retention policy, and contract rate card. AWS separates S3 storage, request and retrieval, and transfer components; CloudWatch likewise separates ingestion, archive storage, and data scanned by queries (aws.amazon.com) (aws.amazon.com). Google prices Cloud KMS according to active key versions, protection level, and operation volume (cloud.google.com). Azure Monitor Log Analytics pricing is based on ingested volume and retention, while Key Vault counts each successfully authenticated REST API call as one operation (learn.microsoft.com) (azure.microsoft.com). FinOps guidance supports unit measures such as cost per service request, workload, or seat used (finops.org).

No responsible estimate can be produced without event count and average record size, because those two variables drive storage, ingestion, and often request volume. Retention is the next leverage point, but shortening it can conflict with investigation, validation, privacy, or regulated-record needs. NIST log guidance says policy should define how long each log type is preserved and how unneeded logs are disposed of (nvlpubs.nist.gov). Cost optimization must follow the approved evidence schedule, not silently rewrite it.

Implications and Future Directions

EFS is significant because it converts one binary choice, retain with external review or forgo the frontier model, into a more granular shared-responsibility design. For some confidential R&D and safety workflows, that may resolve the decisive blocker. It also moves obligations toward the customer: storage hardening, key operations, cleared staffing, triage quality, evidence preservation, and downstream response become part of the deployment's minimum operating capability.

The largest near-term risk is **documentation lag**. Public sources do not yet provide the activity schema, exact retention window, deletion semantics, detection execution boundary, service principal, signal contract, performance commitment, or full exception-access model. Provider documentation shows why those details matter. Bedrock invocation logging is disabled by default but can collect full request, response, and metadata when enabled (docs.aws.amazon.com). Google Data Access logs cover reads and writes of customer-provided data (docs.cloud.google.com). Microsoft diagnostics can export audit plus request and response logs (learn.microsoft.com). None of these generic facilities proves how EFS itself is configured.

Buyers should watch for four publication milestones:

- **Operational specification:** schema, topology, identities, interfaces, error handling, and version policy.
- **Availability matrix:** exact models, products, clouds, regions, organization types, eligibility rules, and phase dates.
- **Contract schedule:** processors, subprocessors, residency, retention, support access, preservation, deletion, and exit.
- **Assurance evidence:** independent control coverage, tested key and access paths, service commitments, and change notification.

As these arrive, governance teams should maintain a dated decision record. The September announcement is valid evidence of product direction, but not proof that a particular tenant has the capability. A production authorization should reference the entitlement and configuration actually observed in that tenant.

Frequently Asked Questions (FAQs)

Does EFS make Claude Enterprise HIPAA compliant for pharma?

No. EFS is a custody and monitoring design. HIPAA applicability depends on whether the workflow handles PHI, the parties' roles, the exact product and features, security controls, and an applicable BAA. Anthropic states that standard Enterprise plans do not automatically include BAA coverage, while HHS requires a written arrangement before a business associate handles electronic PHI (hhs.gov).

Is EFS the same as zero data retention?

No. ZDR describes whether eligible prompts and responses are stored at rest by the service. EFS preserves a monitoring history in customer-controlled storage so automated systems can correlate patterns while customer staff perform human review. It aims for ZDR-like privacy, but introduces a deliberately retained customer-side activity dataset.

Does EFS validate a GxP workflow or satisfy 21 CFR Part 11?

No. FDA guidance calls for risk-based validation tied to intended use, and Part 11 does not replace predicate-rule record requirements (fda.gov). Qualification must cover the complete workflow, including source data, prompts, retrieval, output review, approvals, audit trail, changes, and the authoritative record system.

Can EFS monitor drug-safety reports without Anthropic staff reading them?

That is the announced design: automated review operates over activity and signals go to customer reviewers, with no Anthropic employee review required. Before production, the buyer should confirm the exact content stored, analysis location, exceptional-access terms, reviewer roles, and pharmacovigilance evidence path in its own contract and tenant.

What should an enterprise request first?

Request an entitlement statement, architecture diagram, data dictionary, retention and deletion schedule, key and service-principal design, signal schema, regional-flow map, subprocessor list, BAA or data-processing scope where relevant, assurance evidence, and a non-production test plan. If those artifacts are unavailable, restrict the pilot to synthetic or de-identified data.

Conclusion

Claude Enterprise EFS can remove a specific pharma deployment blocker, but only conditionally. Its customer-owned storage, customer-managed keys, automated correlation, customer-routed signals, and customer human review create a credible division of responsibility for sensitive activity. This is particularly relevant where external access to confidential R&D, clinical material, or drug-safety narratives is unacceptable.

The control should be evaluated for what it is. EFS does not itself provide a BAA, determine HIPAA scope, validate a GxP process, create a Part 11 record system, set a defensible retention period, satisfy GDPR processor obligations, or assure model-output quality. Those controls remain attached to the workload, contract, selected Claude surface, cloud route, organization configuration, and end-to-end operating process.

As of **September 19, 2026**, the sound decision is to request phased access when customer custody addresses a documented barrier, then run a bounded, measurable pilot. Production approval should wait for tenant-level evidence covering schema, retention, keys, access, geography, signals, reviewer operations, contracts, and exit. Organizations that cannot obtain those artifacts, or cannot staff accountable review, should retain current ZDR-compatible models or wait for broader availability and complete operational documentation. EFS changes the architecture of oversight. It does not outsource the customer's responsibility for trustworthy pharmaceutical use.

Source links

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

1. https://www.anthropic.com/claude-fable-and-mythos-5-1?frmapp=yes
2. https://claude.com/form/enterprise-frontier-safeguards
3. https://www.anthropic.com/news/enterprise-frontier-safeguards
4. https://support.claude.com/en/articles/15425996-data-retention-practices-for-covered-models
5. https://support.claude.com/en/articles/8114513-business-associate-agreements-baa-for-commercial-customers
6. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application
7. https://database.ich.org/sites/default/files/ICH_E2D%28R1%29_Step4_FinalGuideline_2025_0819.pdf
8. https://www.ema.europa.eu/system/files/documents/regulatory-procedural-guideline/gvp-module-vi-addendum-ii-masking-personal-data-icsrs-eudravigilance-en.pdf
9. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
10. https://intuitionlabs.ai/articles/responsible-enterprise-ai-privacy-governance
11. https://intuitionlabs.ai/

12. https://platform.claude.com/docs/en/manage-claude/cmek
13. https://support.claude.com/en/articles/15425695-covered-models
14. https://docs.aws.amazon.com/bedrock/latest/userguide/abuse-detection.html?trk=article-ssr-frontend-pulse_little-text-block
15. https://platform.claude.com/docs/en/manage-claude/api-and-data-retention
16. https://docs.aws.amazon.com/bedrock/latest/userguide/data-retention.html
17. https://learn.microsoft.com/en-us/azure/foundry/responsible-ai/claude-models/data-privacy?view=foundry
18. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
19. https://support.claude.com/en/articles/10440198-configure-custom-data-retention-controls-for-enterprise-plans
20. https://platform.claude.com/docs/en/build-with-claude/claude-platform-on-aws
21. https://docs.cloud.google.com/gemini-enterprise-agent-platform/models/abuse-monitoring?authuser=0
22. https://docs.cloud.google.com/gemini-enterprise-agent-platform/resources/data-residency
23. https://database.ich.org/sites/default/files/ICH_E6%28R3%29_Step4_FinalGuideline_2025_0106.pdf
24. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
25. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
26. https://www.fda.gov/media/119267/download
27. https://eur-lex.europa.eu/legal-content/EN-FR-DE/TXT/?uri=CELEX%3A32016R0679
28. https://privacy.claude.com/en/articles/7996866-how-long-do-you-store-my-organization-s-data
29. https://intuitionlabs.ai/articles/is-claude-hipaa-compliant
30. https://platform.claude.com/docs/en/manage-claude/compliance-faq
31. https://platform.claude.com/docs/en/manage-claude/access-transparency
32. https://www.anthropic.com/legal/commercial-terms
33. https://www.anthropic.com/legal/data-processing-addendum
34. https://support.claude.com/en/articles/10015870-what-certifications-has-anthropic-obtained
35. https://intuitionlabs.ai/articles/pharma-llm-security-red-teaming-prompt-injection
36. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf
37. https://www.cisa.gov/sites/default/files/2023-02/cloud_security_technical_reference_architecture_2.pdf
38. https://airc.nist.gov/airmf-resources/airmf/5-sec-core/
39. https://aws.amazon.com/s3/pricing/
40. https://aws.amazon.com/cloudwatch/pricing/
41. https://cloud.google.com/kms/pricing
42. https://learn.microsoft.com/en-us/azure/azure-monitor/logs/cost-logs
43. https://azure.microsoft.com/en-us/pricing/details/key-vault/?msockid=1815163abdd26f59354100a9bc886e03
44. https://www.finops.org/framework/capabilities/unit-economics/
45. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
46. https://docs.aws.amazon.com/bedrock/latest/userguide/model-invocation-logging.html
47. https://docs.cloud.google.com/gemini-enterprise-agent-platform/models/enable-audit-logs?hl=en
48. https://learn.microsoft.com/en-us/azure/foundry/how-to/diagnostic-logging

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