Security Whitepaper

AskMyTrials

Clinical trial document intelligence for pharma sponsors and sites.

Version v1.0

Issued 2026-05-01

Pages 12

About this document

This whitepaper documents the security and compliance posture of AskMyTrials as of the issue date above. It is a companion to the public /trust page (askmytrials.com/trust) and is suitable for forwarding to pharma IT, security, and quality assurance teams during vendor assessment.

Honest posture

AskMyTrials is built for clinical trial document intelligence. We hold pharma sponsor protocols, lab manuals, pharmacy manuals, and the queries site coordinators ask against them. This page documents how we protect that data today, what we are still working on, and where we plan to be by Q4 2026. We do not claim certifications we have not earned.

For questions or vendor assessment requests, contact security@askmytrials.com.

Contents

Section content mirrors the public Trust & Compliance page at askmytrials.com/trust.

1. Posture statement

AskMyTrials is built for clinical trial document intelligence. We hold pharma sponsor protocols, lab manuals, pharmacy manuals, and the queries site coordinators ask against them. This page documents how we protect that data today, what we are still working on, and where we plan to be by Q4 2026. We do not claim certifications we have not earned.

Key claims

- SOC 2 Type I: In progress, target Q3 2026 [In progress]
- 21 CFR Part 11: Controls implemented, validation package in preparation [In progress]
- GDPR: DPA available on request, no EU data residency yet [In progress]
- Encryption in transit: TLS 1.3 [Implemented]
- Encryption at rest: AES-256 [Implemented]
- Data residency: US-East today, EU planned Q4 2026 [Planned]

2. 21 CFR Part 11 controls

The matrix below maps each Part 11 control to its current implementation. Status reflects what is live today, not the roadmap. Validation evidence is shared under NDA.

Reference	Control	Implementation	Status
11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Migration-versioned schema with checksum-validated SHA-256 on every uploaded document. Pre-deployment test suite covers RAG retrieval correctness, audit-log integrity, and rate-limit behavior. Validation Master Plan in preparation as part of the SOC 2 Type I package.	In progress
11.10(b)	Ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.	TMF ZIP Bundle Export produces an FDA-ready archive (cover PDF, per-query PDFs, audit-trail CSV, manifest.json with SHA-256 hash chain) for any trial and any window. PDFs use embedded standard fonts; CSVs are UTF-8.	In progress
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Postgres point-in-time recovery via Supabase, daily backups retained 30 days. Storage objects retained for the lifetime of the trial plus 25 years per ICH GCP, configurable per sponsor agreement.	Implemented
11.10(d)	Limiting system access to authorized individuals.	Role-based access control enforced at the Supabase row level (RLS) and API route level. Coordinators see only trials assigned to their site. Pharma admins see only trials owned by their organization. CRO admins inherit access scoped through parent_org_id.	Implemented
11.10(e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.	Immutable audit_log table with append-only RLS policy. Every create, update, delete, export, and access action logs actor, action, target, timestamp, IP, and metadata. Audit entries cannot be modified or deleted by application users; service-role writes only.	Implemented
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Document approval workflow gates RAG retrieval: only documents with current_version + IRB approval (where required by doc_type) are searchable. Sponsor verification on pinned answers requires medical_monitor or pharma_admin role.	Implemented
11.10(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Authority check at every API boundary via authenticatedClient(). Org-type checks (pharma, cro, site) gate sensitive endpoints (analytics, amendments, exports). Failed authority checks return 401 or 403 and are logged in access_anomalies for review.	Implemented
11.50(a)	Signed electronic records shall contain information associated with the signing that clearly indicates: the printed name of the signer, the date and time when the signature was executed, and the meaning associated with the signature.	TMF Bundle cover page captures Prepared by and Reviewed by signature blocks with name, title, date, and attestation paragraph. Pinned answer create / edit / delete actions log actor and timestamp. Full e-signature workflow (Part 11 Subpart C) is on the roadmap with the Validation Master Plan.	In progress
11.50(b)	The items identified in paragraph (a) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record.	Audit-log fields are exported alongside records in TMF Bundles and ROI PDFs. Signature metadata appears in human-readable form on cover pages.	Implemented
11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures	Signature metadata is stored in audit_log rows whose primary key references the target record. Records are content-hashed with SHA-256 on export; the hash is recorded with the signature event so a record cannot be silently swapped for another.	In progress

Reference	Control	Implementation	Status
	cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.		
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	User accounts are uniquely keyed by email + auth.uid(). Disabled accounts are soft-deleted, preserving the foreign key for historical signatures. New users with the same email as a disabled account receive a new auth.uid().	Implemented
11.100(b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Site coordinator identity is verified by the pharma sponsor through site-activation invite codes. Pharma admin identity is verified by AskMyTrials onboarding. MFA can be enforced per organization. SSO/SAML for enterprise tenants is on the roadmap.	In progress

3. GDPR posture

AskMyTrials acts as a Data Processor for sponsor-provided trial documents and as a Data Controller for our own platform user accounts. We sign DPAs with sponsors on request and pass-through DPAs to all listed sub-processors.

Data subject rights

- Access: site coordinators and pharma admins can export their own queries via Settings > Exports.
- Erasure: individual user accounts can be deleted on request. Trial-level data is retained per the sponsor's regulatory retention schedule.
- Rectification: sponsor admins can correct user metadata at any time.
- Portability: TMF Bundle Export and Audit-log CSV provide structured data export.

EU data residency (Frankfurt) is on the roadmap for Q4 2026 alongside SOC 2 Type II.

4. Data residency

Today: All production data resides in AWS US-East-1 via Supabase.

Planned: EU residency option (Frankfurt) targeted for Q4 2026. Sponsor-tier customers will be able to elect residency at organization creation.

5. Access controls and MFA

Access is enforced at two layers: Postgres row-level security policies on every table containing trial data, and authority checks at every API route boundary.

Role	Scope	MFA
Site coordinator	Read documents and ask questions for their site's assigned trials only.	Optional
Site investigator (PI)	Same as coordinator plus access to all coordinator activity within the site.	Optional
Pharma admin	Full read and write across all trials owned by their pharma organization. Manages access codes, pinned answers, exports.	Required
Pharma medical monitor	Read across all owned trials; accept and pin FAQ clusters; sign amendment briefs.	Required
CRO admin	Inherits pharma admin scope across child organizations linked via parent_org_id.	Required
AskMyTrials staff	No production data access by default. Service-role access is gated by named, time-bounded support escalations logged to audit_log.	Required

6. Audit trail immutability

Every business action writes to audit_log. Schema fields: actor_id, action, target_type, target_id, ip, user_agent, metadata jsonb, created_at.

Immutability

Append-only. RLS policy denies UPDATE and DELETE for application roles. Service-role writes are gated by lib/audit.ts and emit on every business action.

Retention

Lifetime of the trial plus 25 years (ICH GCP). Configurable per sponsor agreement.

Export

Sponsor admins can export audit-log CSV per trial or across the portfolio, scoped to a date range.

7. Encryption

In transit

TLS 1.3 enforced on all connections. HSTS preload with 2-year max-age + includeSubDomains.

At rest

AES-256 at the storage layer (Supabase Postgres + Storage, AWS S3 backend). Backups are also encrypted at rest.

Key management

Encryption keys are managed by the underlying providers (Supabase, AWS). AskMyTrials staff do not have direct access to raw key material.

8. Backups and disaster recovery

- Backup frequency: Daily automated Supabase backups
- Retention: 30 days rolling
- RPO: 24 hours
- RTO: 4 hours
- Quarterly DR restore drill against a non-production project. Last drill: 2026-04-15.

9. Sub-processors

Trial data passes through the third parties listed below. Each operates under a Data Processing Agreement.

Sub-processor	Purpose	Data type	Region
Supabase	Postgres database, authentication, file storage	All trial data, user accounts, uploaded documents, audit log	US-East-1 (AWS)
Vercel	Application hosting, serverless functions, CDN	Request metadata, no persistent storage of trial data	Global edge with US primary region
OpenAI	LLM chat completions for question answering	Question text and retrieved document excerpts (no PHI uploaded). API traffic excluded from training per OpenAI Data Processing Addendum.	United States
Voyage AI	Text embeddings for retrieval	Document chunk text. API traffic excluded from training.	United States
Cohere	Cross-encoder reranking of retrieval candidates	Question + candidate chunk pairs	North America
CloudConvert	DOCX and PPTX conversion to PDF for ingestion	Source document during conversion only; no persistent storage	Germany (EU)
Resend	Transactional email (invitations, alerts, security inquiries)	Recipient email, subject, body	United States

10. Vulnerability disclosure

Send findings to security@askmytrials.com with reproduction steps and any proof of concept.

PGP key available on request for sensitive reports. Reach out via the inquiry form below or email security@askmytrials.com to receive the current public key.

Scope

Production app (askmytrials.com), API endpoints, public marketing site. Out of scope: rate-limit testing, automated scanners against production, social engineering of staff, physical attacks.

Response times

Triage within 2 business days. Fix windows: 90 days for high and critical, 180 days for medium and low.

We will not pursue legal action against researchers who follow this policy in good faith and avoid privacy violations, destruction of data, and service degradation.

11. Contact

- Security: security@askmytrials.com
- Privacy: privacy@askmytrials.com
- General: hello@askmytrials.com
- 2 business days for security inquiries.