Sub-processors

VERSION 1.1 · IN EFFECT FROM 6 OCTOBER 2026

True copy as at 6 October 2026. This is a copy of a living document provided for your records. The current version at cogent.clinic/trust/sub-processors governs.

Cogent Clinic Ltd, a company registered in Scotland, company number SC887432. Data protection registration ICO ZC132394. Questions about this document: privacy@cogent.clinic.

This register names the third-party processors engaged by Cogent Clinic Ltd to deliver the service, together with the processing location and the safeguards in place. Copies of each executed data processing addendum, and the specific legal-entity details and processing regions behind the summaries below, are available on request at privacy@cogent.clinic. Material changes to this list are communicated to customers in advance.

Active sub-processor categories

Primary cloud infrastructure

Entity: Amazon Web Services (AWS), UK region (London, eu-west-2). **Purpose:** Compute, database, object storage, secrets management, scheduled jobs, and backups. Hosts the Cogent Clinic application and all customer account data and audit logs. **Location of processing:** United Kingdom. **Data categories:** Stream A (clinician account data, audit logs, subscription metadata). Stream B (de-identified, tokenised clinical content at rest; the placeholder mapping and session transcripts stored encrypted at rest under a Cogent-held key in AWS Key Management Service (KMS), with access least-privilege and logged). **Safeguards:** Data Processing Addendum in place. ISO 27001, SOC 2 Type II, and Cyber Essentials Plus certifications held by the provider. Provider does not access customer content except to provide the service. Audit-plane logging enabled. IAM principle of least privilege enforced. **Onward transfers:** None for clinical content. Account metadata may transit to provider support channels in limited support cases, governed by the provider's DPA.

AI inference (Anthropic via Amazon Bedrock)

Entity: Anthropic (large-language-model provider), accessed through Amazon Bedrock in the AWS UK region (eu-west-2). Anthropic is not given direct access to a Cogent account; it is reached only as the model served through Bedrock. **Purpose:** Provides the large-language-model inference used to generate draft clinical documentation, folder-scoped reflective-thinking chat replies, formulation sections drawn from the clinician's own content, documentation-completeness checks, and text extraction from clinician-uploaded handwritten notes. **Location of processing:** United Kingdom. **Data categories:** For drafting, chat, formulation and completeness checks: tokenised clinical content, with patient-identifying details replaced by placeholders on the clinician's device before transmission, so no direct patient identifiers reach the inference path. For handwritten-note extraction the position differs and is stated plainly: the uploaded image or PDF is sent as-is for transcription and may contain identifying information, and the protection

applies to the extracted text, which is returned to the clinician for tokenisation review before it can enter a draft. See clause 4.2 of the Data Processing Agreement. **Safeguards:** Inference-only contractual posture: customer content is not used to train or fine-tune any model. Model provider holds ISO 27001:2022 and ISO 42001 certifications; SOC 2 Type I and II. Provider's Data Processing Addendum is in force, incorporating UK IDTA v B.1.0 for UK GDPR transfers and EU SCCs Modules 2/3 for EU transfers; 48-hour breach notification from provider to customer; 15-day objection period for new sub-processors; annual audit rights; 30-day data deletion on termination. The cloud inference service's data processing addendum is the operative instrument for this processing, because the inference runs within that service and the Provider's contractual relationship for it is with the cloud provider. **Onward transfers:** None.

Live session speech-to-text

Entity: AssemblyAI, European Union region. **Purpose:** Converts a clinical session's audio to text in real time, so the clinician can capture a transcript without leaving the browser. Diarisation (speaker separation) is enabled on every session. **Location of processing:** European Union. **Data categories:** Audio stream containing speech from the clinician and (with client consent) the client. Audio is streamed directly from the clinician's browser to the service over a WebSocket, using a short-lived streaming token minted per session from Cogent Clinic's server-side API key. Audio does not transit Cogent Clinic's infrastructure. **Safeguards:** Provider's Data Processing Addendum executed (click-through acceptance incorporated into their Terms of Service at signup). UK GDPR transfers are covered by the UK Addendum to the EU Standard Contractual Clauses, being the ICO template laid before Parliament on 2 February 2022, as completed by Exhibit D of the provider's DPA. Cogent Clinic Ltd's contractual opt-out from using customer audio or transcripts for model training, benchmarking, fine-tuning, or de-identified model development was processed and confirmed in writing by the provider on 2026-04-23 under the relevant section of their Terms of Service. With the opt-out in force, the provider's zero-data-retention controls apply to streaming: audio and transcripts are not retained beyond the WebSocket session; only certain metadata is kept for logging and billing. Short-lived streaming tokens are minted per session: tokens expire in 10 minutes (the provider's maximum), and a single WebSocket session is bounded to 30 minutes by the `max_session_duration_seconds` parameter on mint. The returned text transcript is held in the clinician's browser and, at the clinician's choice, saved under the client folder; saved transcripts are stored by Cogent Clinic in the UK encrypted at rest under a Cogent-held key in AWS Key Management Service (KMS), with access least-privilege and logged. SOC 2 Type II and ISO 27001 attestations held; reports available via the provider's Trust Center under NDA. **Onward transfers:** None material to customer data. US support-access paths, where they occur, are covered by the same DPA framework (Exhibit D UK Addendum to the EU SCCs) and confirmed in writing by the provider.

Payment processing and subscription billing

Entity: Stripe Payments UK, Ltd. **Purpose:** Processes subscription payments, stores payment instruments, generates invoices, manages subscription lifecycle events. **Location of processing:** United Kingdom and European Economic Area primarily; limited US transfers for operational support, governed by UK IDTA and EU SCCs as applicable. **Data categories:** Clinician name, email address, Stripe customer and subscription identifiers, payment card tokens (Stripe-held, Cogent Clinic does not see card data), invoice metadata, VAT information. No clinical content. **Safeguards:** Stripe Data Processing Agreement in place. PCI DSS Level 1 service provider. UK IDTA for transfers outside the UK. **Onward transfers:** Stripe uses its own sub-processor chain for payment networks (Visa, Mastercard, banks). Customer-facing chain published by Stripe.

Authentication

Approach: Self-hosted. Cogent Clinic's authentication layer runs inside the application and writes to the primary UK-resident database. There is no third-party authentication-as-a-service sub-processor. **Purpose:** Authenticates clinician accounts, offers time-based one-time-password (TOTP) two-factor authentication (optional for clinicians, required for administrators), manages session tokens. **Location of processing:** United Kingdom. Same location as the primary database. **Data categories:** Email, hashed credentials, TOTP secrets, session metadata. No clinical content. **Safeguards:** Strong password hashing; TOTP available to all clinicians and required for administrators; short sessions (8h absolute, 30min idle) with rotation; per-user rate limits on login, signup, password reset, and TOTP verification.

Transactional email

Entity: Zoho, EU region. **Purpose:** Sends account verification, password reset, two-factor codes, billing notifications, and other operational email. **Location of processing:** European Union. **Data categories:** Recipient email address, email content relating to account operation. No clinical content in email. **Safeguards:** Provider's standard Data Processing Addendum. TLS in transit. Content retained only for operational delivery, per the provider's retention policy. **Onward transfers:** None material to customer data.

Error tracking

Entity: Sentry, EU region. **Purpose:** Records application errors to support debugging and reliability. **Location of processing:** European Union. **Data categories:** Error metadata only (stack traces, timestamps, user ID, browser context). Scrubbing rules strip request or response bodies before transmission. **Safeguards:** Provider's Data Processing Agreement. Scrubbing rules reviewed before each release where error handling changes. **Onward transfers:** None material to customer data.

Product analytics (metadata only)

Entity: PostHog, EU region. **Purpose:** Aggregate product-usage metrics to support product decisions. Used on the authenticated application for feature-level usage patterns only; not for marketing analytics. **Location of processing:** European Union. **Data categories:** Non-content event metadata (feature use, doc type selected, timestamps, account id). No draft bodies, no chat messages, no transcript content, no patient-identifying content. **Safeguards:** Provider's Data Processing Agreement. EU-region instance (content kept in-region). Runs server-side only: the PostHog browser SDK is never loaded, so no analytics cookie or client-side storage is set in the clinician's browser. We never send content payloads. **Onward transfers:** None material to customer data.

DNS and marketing-site CDN

Entity: Cloudflare. **Purpose:** DNS resolution for cogent.clinic and static hosting for the marketing site. Not deployed on the authenticated application domain. **Location of processing:** Global edge, EU-biased routing. **Data categories:** Public-site request metadata only (IP, User-Agent, request path). No clinical content. **Safeguards:** Provider's Customer Data Processing Addendum. Standard-contractual-clause transfer safeguards where applicable. **Onward transfers:** Inherent to global CDN operation; the provider publishes its own sub-processor chain.

Named sub-processors at a glance

Category	Named entity	Processing location
Primary cloud infrastructure	Amazon Web Services (AWS)	UK (London, eu-west-2)
AI inference	Anthropic, via Amazon Bedrock	UK (eu-west-2)
Live session speech-to-text	AssemblyAI	European Union
Payment and subscription billing	Stripe Payments UK, Ltd	UK / EEA, with limited US support transfers
Transactional email	Zoho	EU
Error tracking	Sentry	EU
Product analytics (server-side, cookieless)	PostHog	EU
DNS and marketing-site CDN	Cloudflare	Global edge, EU-biased routing

Authentication is self-hosted by Cogent Clinic and is not a third-party sub-processor.

Copies of each executed data processing addendum, and the specific legal-entity details and processing regions behind the summaries above, are available to customers and to prospective customers doing procurement diligence on request at privacy@cogent.clinic (we'll respond within two working days).

Change policy

Before any new sub-processor is engaged, and before any removal, substitution or change of processing region, we update this register, the Data Protection Impact Assessment and our Article 30 record, and give customers at least 30 days' notice by in-application message and email. Customers who object may terminate the contract under the standard DPA terms.