CoreSR Inc.
c/o LaBarge Weinstein LLP, 800-515 Legget Drive, Kanata, ON K2K 3G4, Canada
help@coresr.ai · coresr.ai

PUB-009 · Version 1.4
Effective: 2026-11-17
Public Procurement & Governance

Institutional Vendor Information Pack

Public Security & Trust Centre: https://coresr.ai/security
Direct PDF Download: https://coresr.ai/api/public/vendor-pack

This Institutional Vendor Information Pack provides hospital, university, health technology assessment (HTA), and clinical guideline procurement offices with a complete, self-contained due-diligence summary for **CoreSR** (https://coresr.ai). Every commitment in this document corresponds to an active technical control or signed governance policy in production.

1. Corporate & Vendor Identification

Field	Detail
Legal Entity Name	**CoreSR Inc.** *(formerly operating under product brand Synthero)*
Jurisdiction of Incorporation	Canada (Federal / Province of Ontario)
Registered Corporate Address	c/o LaBarge Weinstein LLP, 800-515 Legget Drive, Kanata, ON K2K 3G4, Canada
Primary Platform	**CoreSR** (https://coresr.ai) — End-to-end systematic review, Risk-of-Bias, meta-analysis, and GRADE evidence synthesis platform
Founder & Chief Executive Officer	**Tyler Pitre, MD PhD FRCPC** (tyler.pitre@coresr.ai)
Security & Vulnerability Disclosure	security@coresr.ai (https://coresr.ai/.well-known/security.txt)
Privacy & Data Protection Officer	security@coresr.ai
Legal & Institutional Contracting	legal@coresr.ai · General Support: help@coresr.ai

2. Certification Status & Independent Assurance Roadmap

- **Current Certification Status:** CoreSR holds **no external third-party ISO 27001 or SOC 2 certificate today**.
- **Internal Security Programme:** CoreSR operates a formal internal Information Security Management System (ISMS) **modelled on ISO/IEC 27001:2022**, comprising signed security and continuity policies, a full ISO/IEC 27001:2022 Statement of Applicability continuously reconciled against live infrastructure (zero control drift), a formal Risk Register, quarterly

privileged-access reviews, and continuous automated production posture verification (**Grade A** across all 7 security control domains).

- **SOC 2 Type II Path:** CoreSR is pursuing **SOC 2 Type II** directly (rather than a single-day Type I snapshot), with the **Type II observation window scheduled to open in Q1 2027** (target attestation report **Q4 2027**).
- **Vulnerability Scanning & Penetration Testing:** Blocking CI static analysis (SAST), software composition analysis (SCA), automated secret detection, and weekly dynamic application security testing (DAST) run continuously today. An independent accredited third-party penetration test is commissioned upon institutional purchase requirement or at SOC 2 Type II kickoff (Q1 2027), whichever occurs first.

3. Data Classification & Strict No-PHI Boundary

- **Data Processed by CoreSR:** Published scientific literature (bibliographic citations, abstracts, DOIs/PMIDs, full-text study PDFs) and methodological review work product (protocols, PICO definitions, screening decisions, extracted study statistics, Risk-of-Bias judgements, GRADE evidence profiles, meta-analysis datasets, and manuscript drafts), alongside minimal account records (email, display name, salted adaptive password hash, AES-256-GCM encrypted TOTP seed, session/audit metadata, and Stripe billing reference).
- **Strict Exclusion of Patient Health Records (No PHI):** CoreSR never connects to hospital electronic medical records (EMRs), clinical registries, or patient portals, and **strictly prohibits uploading Protected Health Information (PHI)** or identifiable patient records regulated under Ontario PHIPA, US HIPAA, or GDPR Article 9 (Terms of Service §6.1; DPA §2.3).
- **Payment Card Data:** Processed 100% by **Stripe, Inc.** (PCI-DSS Level 1); raw card numbers never touch CoreSR infrastructure.

4. Hosting, Data Residency & Regional Deployment Options

Infrastructure Layer	Location & Operator	Residency & Legal Transfer Basis
Primary Production Compute, Database & Encrypted Storage	**Helsinki, Finland (EU / EEA)** — Hetzner Online GmbH (ISO/IEC 27001 certified data centres)	EEA primary residency; AES-256 volume encryption at rest
Dedicated GPU Inference & Primary Off-Site Backup Infrastructure	**Ontario, Canada** — CoreSR-operated private hardware connected over an authenticated point-to-point encrypted tunnel	Canadian PIPEDA jurisdiction (EU Commission Adequacy Decision 2002/2/EC, reaffirmed Jan 2024)
Immutable Disaster-Recovery Cloud Archive	**Backblaze, Inc.** (Compliance-mode WORM Object Lock) & **Google Cloud / Workspace**	Pre-encrypted backup ciphertext only — zero cloud provider access to decryption keys
US-Region Deployment Option (Team & Institution)	**United States** dedicated regional deployment available under a Team or Institution Order Form	Scopes database, object storage, and ephemeral GPU execution to US regions where institutional governance mandates US-only residency (legal@coresr.ai)

5. Summary of the Four Core Technical Control Domains

(Full verbatim specification published in the Security Controls Statement at https://coresr.ai/api/public/controls-statement.)

1. **Encryption:** TLS 1.3 + HSTS preload + mutual TLS (mTLS) origin authentication in transit; authenticated point-to-point encrypted east–west tunnel; AES-256 encrypted production storage volumes with hardware-isolated keys; salted adaptive password hashing; AES-256-GCM encrypted TOTP seeds; SHA-256 hashed session tokens; asymmetrically pre-encrypted off-site backup archives.

2. **Network Security:** Global Anycast WAF/DDoS protection; default-deny host ingress restricted to mTLS-authenticated edge origins; non-public internal isolation of database and application workers; public-key-only infrastructure administration with 100% MFA enforcement; SSRF network-range blocking; strict CSP and HTTP security headers.
3. **Vulnerability Management:** Blocking CI/CD SAST, SCA, and secret-detection gates; automated daily OS security patching with anomaly alerting; weekly production DAST scans; RFC 9116 safe-harbor disclosure (`/.well-known/security.txt`); binding remediation SLAs (**Critical ≤ 7d, High ≤ 30d, Medium ≤ 90d**).
4. **Data Loss Prevention:** Contractual & architectural No-PHI boundary; server-enforced block on third-party commercial LLM egress (one stated exception, Kaplan–Meier figure reading) and zero model training for Team/Institution workspaces; automated cross-tenant RBAC isolation tests; workspace-enforced TOTP 2FA, configurable session lifetimes, and instant session revocation; append-only security audit trail with real-time anomaly alerts; One-Click Full Account ZIP Export; revocable account deletion followed by automated live purge.

6. AI Governance & Customer Data Protection (Controls 4.1–4.6)

(Full specification in AI Governance & Provenance at https://coresr.ai/api/public/ai-governance and Model Version Changelog at https://coresr.ai/api/public/model-changelog.)

- **4.1 Training Provenance: TITAN-SR** (`v6-2026-10-15` , 3,097,955 public scholarly bibliographic records across 19,926 reviews), **GLASS v3** (6 task specialists, 65,536-token context, built on Apache-2.0 open weights + open-access biomedical literature and curated appraisal rubrics), and **ROB BERT v6.1** (4,237 deduplicated RoB 2 worksheets).
- **4.2 Customer Content & Model Training: Team and Institution workspace content is NEVER used to train, fine-tune, or evaluate CoreSR models**, unless governed by a separate, bilaterally signed written research/co-development agreement. Individual/Free accounts have one-click opt-out in Account Settings.
- **4.3 Zero Prompt Logging:** Operational usage telemetry records token counts, model identifiers, and latency only — **zero prompts, zero responses, zero study text**. Stateless GPU workers retain zero bytes post-response.
- **4.4 Model Version Pinning:** Every AI output pins its exact model release tag and cryptographic manifest digest in project records and CSV/ZIP exports.
- **4.5 Human-in-the-Loop Control:** AI proposals and human reviewer decisions are stored non-destructively in separate fields; extractions require locatable verbatim PDF quotes prior to human verification; quantitative GRADE domains (Risk of Bias, Imprecision, Publication Bias) are computed **100% deterministically in code**.
- **4.6 Commercial LLM Egress:** Blocked in server code for all Team and Institution workspaces — **no data is transmitted to OpenAI, Anthropic, or DeepSeek, and none to Google Gemini apart from one stated exception** effective November 17, 2026: when a reviewer runs KM Cor on a Kaplan–Meier figure, the cropped image of that figure, its caption, and the review's subgroup names are sent to Google's Gemini vision model through a commercial model API.

7. Authorized Subprocessors & 30-Day Advance Notice

Subprocessor	Role	Region	Attestations & DPA
Hetzner Online GmbH	Primary compute, relational database & AES-256 encrypted storage	Helsinki, Finland (EEA)	ISO/IEC 27001 · GDPR Art. 28 DPA
Cloudflare, Inc.	DNS, CDN, WAF/DDoS, TLS 1.3 & mTLS origin authentication	Global Edge	SOC 2 Type II · ISO 27001 / 27701

Subprocessor	Role	Region	Attestations & DPA
RunPod, Inc.	Standby only: stateless, zero-retention GPUs running CoreSR's own GLASS weights, used only as a standby when CoreSR's private servers are down or unavailable	US / EU	SOC 2 Type II
Backblaze, Inc.	Compliance-mode WORM Object Lock storage of pre-encrypted backups	US / CA / EU	SOC 2 Type II · DPA + SCCs
Google LLC	Secondary pre-encrypted backup archive, transactional email & optional OAuth	Global	SOC 2 Type II · ISO 27001 / 27701
Stripe, Inc.	Subscription billing & PCI-DSS Level 1 card processing	US & Ireland	PCI-DSS Level 1 · SOC 1 & 2 Type II

*CoreSR provides **at least 30 calendar days' advance written notice** prior to adding or materially changing any Subprocessor, with a 14-day objection and pro-rata refund termination right (https://coresr.ai/api/public/subprocessors).*

8. Business Continuity, Incident Response & Accessibility

- **3-2-1-1 Immutable Backups & Recovery Objectives:** Daily asymmetrically encrypted off-site backups replicated across independent jurisdictions and Compliance-mode WORM Object Lock storage (write-only credentials), verified continuously via automated restore checks and quarterly clean-room recovery drills (**RPO ≤ 24 hours · RTO ≤ 24 hours**).
- **Executive Continuity & Institutional Escrow:** Unattended patching, certificate renewal, health monitoring, and anomaly alerting operate autonomously, backed by a formally designated executive Continuity Custodian with escrowed emergency recovery procedures and an optional **Source-Code & Container Escrow Rider** for Institution agreements.
- **72-Hour Breach Notification SLA:** Confirmed Personal Data Breaches are notified **without undue delay and within 72 hours** (targeting **24 hours** for Institution customers) per GDPR Art. 33 and PIPEDA s. 10.1.
- **Accessibility (WCAG 2.1 Level A & AA):** Zero automated accessibility violations across 20 audited public and core views; full ITI **VPAT® 2.5 ACR (PDF)** published at https://coresr.ai/api/public/vpat.

9. Executive Attestation

CoreSR Inc. attests that the technical controls, data-residency boundaries, AI governance commitments, and recovery objectives summarized in this Vendor Information Pack accurately describe the live production CoreSR platform as of the effective date above. Detailed internal ISMS policies, Statement of Applicability schedules, and Privileged Access Register records are available to institutional reviewers under mutual NDA via security@coresr.ai.

Tyler Pitre, MD PhD FRCPC
Founder and Chief Executive Officer, CoreSR Inc.
tyler.pitre@coresr.ai