DATA PROCESSING AGREEMENT

ClinicalHIS — Data Processing Agreement (DPA)

Document version: 1.0 · Effective date: 17 October 2026

This Data Processing Agreement ("**DPA**") forms part of the agreement ("**Agreement**") between:

- **Claridad Health Solutions**, P.O. Box CT 4835, Cantonments, Accra, Ghana (Company Reg. No. BN099561220) ("**Processor**", "we", "us"), the operator of the ClinicalHIS hospital management platform; and
- the hospital or clinic that has contracted for ClinicalHIS ("**Controller**", "you", "Customer"),

each a "Party", together "the Parties".

The Controller acts as the data controller (or, where applicable under US law, as the HIPAA Covered Entity) for personal data processed through ClinicalHIS. Claridad Health Solutions acts as the data processor (or HIPAA Business Associate) and processes personal data only on the Controller's documented instructions.

1. Definitions

- "**Personal Data**", "**Processing**", "**Data Subject**", "**Breach**": as defined in the data-protection law applicable to the relevant Personal Data, including the Ghana Data Protection Act, 2012 (Act 843), the Nigeria Data Protection Act, 2023 (where applicable), the EU/UK General Data Protection Regulation (where applicable), and HIPAA (where applicable).
- "**ClinicalHIS**": the hospital management platform and its modules (admissions, outpatient and inpatient care, EMR, laboratory, pharmacy, billing, HR and the patient portal), operated by the Processor.
- "**Sub-processor**": any third party engaged by the Processor to Process Personal Data.
- "**clinicalris transfer**": the intra-group transfer described in Section 7.3 and Annex B relating to our radiology platform clinicalris.com.

2. Processing on documented instructions

2.1 The Processor Processes Personal Data only to provide, operate, secure and support ClinicalHIS in accordance with the Agreement and this DPA, and on the Controller's documented instructions (including configuration choices made by Controller administrators in the product), unless required to do otherwise by applicable law.

2.2 The Processor immediately informs the Controller if an instruction appears to infringe applicable data-protection law.

2.3 The Processor does not sell Personal Data and does not Process it for its own marketing or advertising purposes. Aggregated, de-identified statistics that do not identify any patient, staff member or Controller may be used to operate and improve the platform.

3. Confidentiality

The Processor ensures that all personnel authorised to Process Personal Data are bound by written confidentiality obligations and receive data-protection training appropriate to their role. Personnel access Personal Data only on a need-to-know basis to perform their duties.

4. Security measures

The Processor implements and maintains the technical and organisational measures described in **Annex A**. The measures in Annex A are the minimum; the Processor may update them, provided no update reduces the overall level of protection.

5. Sub-processors

5.1 The Controller authorises the Sub-processors listed in **Annex B**.

5.2 The Processor will give the Controller at least **30 days' prior notice** (by email to the Controller's administration contact, by a notice in the product, and by updating the public register at https://www.clinicalhis.com/legal/subprocessors) before adding or replacing a Sub-processor in a way that changes what Personal Data is disclosed or where it is processed. The Controller may object in writing within that period on reasonable data-protection grounds. If the Parties cannot resolve the objection, the Controller may terminate the affected services with pro-rata refund of prepaid unused fees as its exclusive remedy.

5.3 The Processor imposes data-protection obligations on each Sub-processor equivalent to this DPA and remains fully liable for their performance.

6. Data subjects' rights

Taking into account the nature of the Processing, the Processor assists the Controller — by appropriate technical and organisational measures, insofar as this is possible — in fulfilling the Controller's obligation to respond to Data Subject requests (access, rectification, erasure, restriction, portability, objection). Where ClinicalHIS provides self-service tools (for example patient portal records or export functions), the Controller may respond to requests directly through those tools. The Controller remains the point of contact for Data Subjects; the Processor routes any Data Subject request received directly to the Controller.

7. International transfers

7.1 Primary hosting. ClinicalHIS runs on the Processor's European Union infrastructure (servers in Germany/France operated by Contabo GmbH). Tenant-local deployments (the Controller's own servers) keep all ClinicalHIS data on hardware under the Controller's physical control.

7.2 Transfer mechanism. Where Personal Data is transferred outside the country of the Controller, the Processor makes such transfer only under this DPA and the safeguards of the applicable annex: Annex C (Ghana Act 843), Annex D (Nigeria NDPA 2023), Annex E (EU/UK GDPR, with Standard Contractual Clauses / the UK IDTA incorporated by reference where required), or Annex F (US Business Associate Agreement, when executed).

7.3 Intra-group radiology transfer (clinicalris.com). The Processor's affiliate operates the radiology platform clinicalris.com, hosted in the United States. Where the Controller uses radiology services connected to clinicalris.com:

- ClinicalHIS transmits radiology orders to clinicalris.com. The order message carries the patient identifier used by the hospital (medical record number), the patient's first and last name, date of birth and sex, together with the imaging order details (order number, procedure code and name).
- Reports and diagnostic images produced through clinicalris.com are returned to ClinicalHIS for the Controller's clinical use; image and report exchange is enabled per tenant and only for studies associated with such orders.
- clinicalris.com Processes this data solely to perform the radiology services (scheduling, image acquisition support, reading, reporting) and under safeguards equivalent to this DPA. clinicalris.com is listed in Annex B as an intra-group processor. Where the EU/UK annexes apply, the transfer is subject to Standard Contractual Clauses / IDTA incorporated by reference in Annex E.

7.4 Other transfers disclosed in Annex B (messaging, payments, hosting) are limited to the data described there and are protected by the safeguards of this Section 7.

8. Personal data breach

8.1 The Processor notifies the Controller of a Personal Data Breach affecting ClinicalHIS **without undue delay and no later than 48 hours** after becoming aware of it, by email to the Controller's designated security contact.

8.2 The notification includes, to the extent known at the time and supplemented as the investigation progresses: the nature of the Breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed. This 48-hour Processor-to-Controller target is designed to let the Controller meet its own regulatory notification deadlines (which are the Controller's responsibility), including any 72-hour supervisory-authority deadline.

9. Return and deletion; exit

9.1 On the Controller's written request, or on termination of the Agreement, the Processor makes all Controller records available for export in a structured, commonly used format covering the Controller's full records (patients, clinical records, billing and administrative data) for a period of **30 days** following termination or request ("Exit Export Window").

9.2 After the Exit Export Window, the Processor deletes or anonymises the Controller's Personal Data from production systems within **90 days**, except where retention is required by applicable law (in which case the Processor informs the Controller of the requirement and protects the retained data under this DPA). Backups are overwritten according to the backup rotation cycle and the Processor does not restore Personal Data from backups into production after deletion except at the Controller's instruction.

9.3 Upon request, the Processor certifies in writing that deletion has been completed.

10. Audit and evidence

The Processor maintains records of Processing sufficient to demonstrate compliance with this DPA, makes the public registers at /legal/dpa and /legal/subprocessors available, and upon reasonable prior written notice (no more than once per year, except following a Breach) provides the Controller with written summaries of audit evidence (such as configuration standards, access-control descriptions and penetration-test summaries actually performed) sufficient to demonstrate compliance.

11. Liability and indemnity

Each Party's liability under this DPA is subject to the limitations of liability in the Agreement, except that this Section does not limit liability for breaches of data-protection law where such limitation is not permitted.

12. Term

This DPA takes effect with the Agreement and remains in force for as long as the Processor Processes Personal Data for the Controller. The Processor may update this DPA; material changes are notified in advance and the change-notice and objection rights in Section 5.2 apply mutatis mutandis, including re-acceptance through the product's acceptance gate where a new version materially changes Controller obligations.

13. Governing law

This DPA is governed by the laws of the Republic of Ghana, without prejudice to mandatory data-protection provisions of the country annexes. The Parties submit to the jurisdiction of the competent courts of Ghana sitting at the High Court of Justice, Accra, save that a signed Service Order may vary jurisdiction for that Customer, and the mandatory provisions of any annexed country law continue to apply to the Processing they govern.

ANNEX A — TECHNICAL AND ORGANISATIONAL MEASURES

The following measures are implemented in the ClinicalHIS platform and infrastructure as deployed by the Processor. This Annex describes only measures that verifiably exist in the deployed platform.

A1. Transport security. All browser and API traffic is served over HTTPS with TLS 1.2/1.3, forward-secret cipher suites and HTTP Strict Transport Security (HSTS, preload). Plain HTTP requests are redirected to HTTPS. Internal service traffic runs on an isolated Docker network.

A2. Access control. Role-based access control (RBAC) with permission sets per role; per-tenant data scoping enforced in the API (every clinical query is scoped to the authenticated user's tenant); configurable permission restrictions per tenant; least-privilege database access by the application.

A3. Authentication. Password authentication with hashing (bcrypt); optional and (for sensitive roles) enforceable multi-factor authentication: TOTP authenticator apps, WebAuthn passkeys, and single-use backup codes; TOTP secrets and integration credentials are encrypted at the field level with AES-256-GCM; short-lived access tokens with server-side revocation (token versioning and refresh-token rotation); step-up re-authentication for sensitive account operations; account lockout and login rate limiting with exponential backoff.

A4. Session security. Idle session timeout (configurable, default 15 minutes); HttpOnly, scoped refresh-token cookies; CSRF protection on state-changing browser endpoints.

A5. Audit logging. Append-only audit logs (database triggers reject UPDATE/DELETE) with per-row SHA-256 checksums and integrity-verification functions; login history and PHI-access logging; audit-log archival functions with restricted access.

A6. Platform hygiene. Centralised security headers (X-Content-Type-Options, X-Frame-Options DENY, XSS protection); API rate limiting; input validation; parameterised database queries; secrets held outside the codebase (environment/encrypted store); automated dependency updates where feasible.

A7. Data separation. Logical multi-tenancy: shared application and database infrastructure with tenant identifier scoping in every query, per-tenant branding/configuration, and per-tenant module enablement. Tenant-local deployment mode, where contracted, keeps the full stack on the Controller's own hardware.

A8. Backups. The Processor takes local database backups on the hosting server. Backups are currently retained locally and are **not** replicated off-site; there is currently no full disk/volume encryption of the hosting servers. The Processor discloses this openly and maintains it as a known improvement item; the Controller should weigh this in its own risk assessment and may choose tenant-local hosting as the strictest alternative.

A9. Personnel. Named individuals with production access; confidentiality undertakings; access revocation on role change.

ANNEX B — SUB-PROCESSORS

Current list; maintained publicly at https://www.clinicalhis.com/legal/subprocessors. "Location" is where the processing entity is established / processes data.

#	Sub-processor	Purpose	Personal data disclosed	Location
B1	Contabo GmbH (EU hosting)	Hosting of the ClinicalHIS application, database, storage and backups	All ClinicalHIS data (server hosting)	Germany / France (EU)
B2	Claridad Health Solutions — clinicalris.com (intra-group)	Radiology services (RIS/PACS): order routing, reading and reporting support	Patient MRN, first/last name, date of birth, sex, imaging order details; reports and images for studies routed via clinicalris.com	United States
B3	WhatsApp / Meta Platforms (via self-hosted WAHA gateway or Meta Cloud API)	Patient/staff messaging: appointment reminders, notifications, one-time codes, announcements (tenant-configured)	Recipient phone number; message content (may include the patient's name where the tenant's templates include it)	Ireland / US
B4	Textbee (SMS gateway)	SMS notifications and one-time codes (tenant-configured)	Recipient phone number; message text	Provider's infrastructure (US)
B5	Twilio	SMS / WhatsApp messaging (tenant-configured)	Recipient phone number; message text	US
B6	Paystack	Payment collection	Transaction amount/currency; payer email	Nigeria / Ghana

#	Sub-processor	Purpose	Personal data disclosed	Location
B7	Stripe	Payment collection	Transaction amount/currency; payer email	US
B8	Flutterwave	Payment collection	Transaction amount/currency; payer email and name	Nigeria
B9	Email (SMTP) provider configured by the Processor or tenant	System and clinical email (portal credentials, critical-result alerts, notifications)	Recipient email address; message content (clinical emails may contain patient identifiers where clinically necessary)	Per configuration
B10	Chat support widget provider (brandedclaws.com)	Public-website support chat	Visitor IP, user agent, pages visited on public pages	Provider's infrastructure
B11	Google Fonts (only where a tenant configures brand typography)	Font delivery for tenant branding	Visitor IP (standard web request)	Google infrastructure (global)
B12	Jitsi meeting server (tenant-configured endpoint)	Telemedicine video consultations	Call metadata; participant identifiers for consultations routed to the configured server	Per tenant configuration

Services that process no personal data (disclosed for completeness): exchange-rate feed (open.er-api.com). Inactive/discontinued: goqr.me QR service (eliminated — QR codes are now generated locally).

ANNEX C — GHANA (Data Protection Act, 2012, Act 843)

Where the Controller is established in Ghana or the Processing is otherwise subject to Act 843:

1. The Processor Processes Personal Data on behalf of the Controller in accordance with Act 843 and the Controller's instructions and does not Process for its own purposes.

2. The Processor assists the Controller in meeting its obligations under Act 843, including provisions on data security (Section 30), data subject rights and notification.

3. The Processor implements the security measures in Annex A, having regard to harm that would be likely to result from unauthorised access, loss or destruction of health data.

4. Transfers of data outside Ghana under Section 60 of Act 843 are made subject to adequate safeguards, as set out in this DPA (including Annex A, the sub-processor register and, for clinicalris.com, equivalent intra-group obligations).

5. Breach notification to the Controller follows Section 8 of this DPA (≤ 48 hours), enabling the Controller to meet its duties under Act 843 and any Data Protection Commission directives.

ANNEX D — NIGERIA (Nigeria Data Protection Act, 2023)

Where the Processing is subject to the NDPA 2023:

1. The Processor provides the Controller with the information necessary to demonstrate compliance with NDPA obligations and assists with data subject requests.

2. The Processor maintains the security measures in Annex A appropriate to the risk of health-data processing.

3. Cross-border transfers under Section 41 NDPA are made pursuant to this DPA's safeguards and any additional measures required by the Nigeria Data Protection Commission.

4. Breach assistance: the Processor notifies the Controller within the timescale in Section 8 so the Controller can meet NDPA notification duties.

ANNEX E — EU / UK (GDPR; UK GDPR & Data Protection Act 2018)

Where the Processing is subject to the EU GDPR or the UK GDPR:

1. Roles: the Controller determines the purposes and means; the Processor acts only on instructions (Art. 28 EU GDPR / Art. 28 UK GDPR).

2. The **Standard Contractual Clauses** (Commission Implementing Decision (EU) 2021/914, Module Two: Controller-to-Processor) and, for the UK, the **International Data Transfer Agreement (IDTA)** or the UK Addendum, are incorporated into this DPA by reference for transfers outside the EEA/UK, with the following elections: Clause 7 (docking) applies; Clause 9(a) Option 2 (30 days' notice of sub-processor changes); Clause 11(a) independent dispute resolution is not used; the governing law of the Clauses is the law of Ghana; the chosen forum is Accra, Ghana, without prejudice to Data Subjects' rights to lodge complaints with their supervisory authority.

3. The Processor conducts transfer impact assessments as required and implements supplementary measures where needed.

4. Technical and organisational measures: Annex A. Sub-processors: Annex B (including the clinicalris.com intra-group transfer, protected by the Clauses).

ANNEX F — UNITED STATES (Business Associate Agreement — reserved)

Where the Controller is a HIPAA Covered Entity in the United States, the Processor makes a Business Associate Agreement (BAA) available on request (contact privacy@clinicalhis.com). Upon execution, the BAA forms Annex F and, for PHI within the meaning of HIPAA, prevails over this DPA to the extent of any conflict. Indicative commitments aligned with the platform's current controls: permitted uses limited to Treatment, Payment and Health Care Operations and as required by law; security safeguards per Annex A; breach reporting to the Covered Entity (≤ 48 hours target); individual-rights assistance; return/deletion on termination per Section 9; flow-down obligations to Sub-processors (Business Associate subcontractors) per Annex B.

Claridad Health Solutions · P.O. Box CT 4835, Cantonments, Accra, Ghana · Reg. No. BN099561220 · privacy@clinicalhis.com · security@clinicalhis.com

This document is provided for informational purposes and does not constitute legal advice. Version 1.0 — 17 October 2026.