

DATA PROCESSING AGREEMENT

ClinicalRIS Platform — Radiology Information System, PACS, Reporting and Patient Portal

Version 1.0 · Effective 16 October 2026

Parties

Processor:

Legal name: Claridad Health Solutions
Registered address: P.O. Box CT 4835, Cantonments, Accra, Ghana
Company registration no.: BN099561220
Contact for this Agreement: privacy@clinicalris.com

Controller:

Legal name: [PLACEHOLDER: customer legal name]
Registered address: [PLACEHOLDER: customer address]
Registration no.: [PLACEHOLDER: registration number]
Authorized representative: [PLACEHOLDER: name and title]
Contact for data protection matters: [PLACEHOLDER: email]

The Processor and the Controller are each a "Party" and together the "Parties". This Data Processing Agreement ("DPA") forms part of the master agreement or Terms of Service between the Parties governing use of the ClinicalRIS platform (the "Services") and applies wherever the Processor processes Personal Data on behalf of the Controller.

Recitals

(A) The Controller operates a healthcare or diagnostic imaging organization and has entered into an agreement with the Processor for the provision of the ClinicalRIS platform, including radiology information system functions, DICOM image storage and viewing, diagnostic reporting, patient engagement features, and optional AI-assisted analysis tools.

(B) In providing the Services, the Processor will process Personal Data, including patient health information, on behalf of and under the documented instructions of the Controller.

(C) The Parties wish to record in this DPA the terms governing that processing, including the roles of the Parties, the applicable safeguards, and the obligations of each Party under applicable data protection laws, which include (as applicable to each Party) the EU General Data Protection Regulation 2016/679 ("GDPR") and the UK GDPR, the Ghana Data Protection Act, 2012 (Act 843), the Nigeria Data Protection Act 2023 ("NDPA"), and the US Health Insurance Portability and Accountability Act ("HIPAA") where the Controller is a Covered Entity.

(D) Where a country-specific Annex C to F applies to the Controller, that Annex supplements and, where expressly stated, prevails over the core terms of this DPA.

1. Definitions and Interpretation

- 1.1** "Applicable Data Protection Law" means the data protection and health-information laws that apply to a Party's processing under this DPA, including those listed in Recital (C) and any equivalent national law of the Controller's jurisdiction.
- 1.2** "Personal Data", "Controller", "Processor", "Processing", "Data Subject", "Personal Data Breach" and "Special Category Data" have the meanings given by Applicable Data Protection Law. Patient health information, imaging, and identifiers are treated as Special Category Data (or their equivalent, e.g. Protected Health Information under HIPAA) regardless of the formal framework applied.
- 1.3** "Patient Data" means Personal Data contained in or arising from use of the Services, including DICOM studies and embedded metadata, patient demographics, clinical orders and reports, appointment and billing records, and contact details used for patient engagement.
- 1.4** "Sub-processor" means any third party engaged by the Processor to process Patient Data in connection with the Services.
- 1.5** "Documented Instructions" means the Controller's instructions as set out in this DPA, the master agreement, the configuration of the Services by the Controller and its administrators, and any written instructions given through support or account channels.
- 1.6** References to writing include email. Headings are for convenience only. The word "including" is without limitation.

2. Roles, Scope and Details of Processing

- 2.1** Roles. The Controller determines the purposes and means of the processing of Patient Data. The Processor processes Patient Data solely as a processor (or Business Associate, where Annex F applies) acting on the Controller's Documented Instructions. The Controller confirms it is entitled to transfer Patient Data to the Processor and to give the instructions it gives.

- 2.2** Details of processing. The subject matter, duration, nature and purpose of the processing, the categories of data and data subjects are set out in the table below.

Subject matter	Provision and operation of the ClinicalRIS platform for the Controller's diagnostic imaging operations.
Duration	For the term of the master agreement, plus the deletion period in clause 10.
Nature and purpose	Storage, retrieval, viewing, reporting, workflow management, billing support, patient engagement (portal, share links, WhatsApp/SMS/email delivery where enabled by the Controller), and optional AI-assisted analysis initiated by the Controller's authorized users.
Categories of data subjects	Patients of the Controller; the Controller's staff and contracted professionals (radiologists, technologists, administrators, referring physicians); payers where online payments are enabled.
Categories of Patient Data	Identifiers (name, patient ID/MRN, date of birth, sex, contact details); DICOM imaging studies including pixel data and embedded metadata; clinical history, orders and radiologist reports and addenda; appointment and preparation data; billing records; staff account and authentication data; audit and technical logs.
Sensitive categories	Health data (diagnostic imaging and reports) is processed throughout; other special-category data only where included by the Controller in free-text fields.

- 2.3** Restrictions. The Processor shall not process Patient Data for its own purposes, shall not sell or monetize Patient Data, and shall not use Patient Data to develop, train, or improve any machine-learning model, except for de-identified copies created at the Controller's request with the on-demand de-identification tool.

3. Processor Obligations

- 3.1** Instructions. The Processor shall process Patient Data only on Documented Instructions, including with regard to international transfers, unless required by law to process otherwise, in which case the Processor shall inform the Controller before doing so (unless prohibited by law).
- 3.1a** Hospital-system linkage (HL7). Where the Controller links ClinicalRIS to its own hospital information system (such as its ClinicalHIS instance) through an HL7 interface, Documented Instructions include the retention of full patient metadata on arriving studies so clinical records match across the linked systems; such processing remains for the same Controller and subject to this DPA.

- 3.2 Confidentiality. The Processor shall ensure that persons authorized to process Patient Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that access is limited to the minimum necessary for their role.
- 3.3 Security. The Processor shall implement and maintain the technical and organizational measures set out in Annex A.
- 3.4 Sub-processors. The Processor may engage Sub-processors only in accordance with clause 5 and Annex B.
- 3.5 Assistance. The Processor shall provide reasonable assistance to the Controller, taking into account the nature of the processing, in responding to Data Subject requests (clause 8), in ensuring compliance with security and breach-notification obligations (clauses 6 and 7), and in data protection impact assessments relating to the Services.
- 3.6 Records and demonstration. The Processor shall maintain records of processing activities and make available the information reasonably necessary to demonstrate compliance with this DPA, including supporting audits under clause 9.
- 3.7 Deletion or return. The Processor shall delete or return Patient Data at the end of the provision of the Services in accordance with clause 10.

4. Controller Obligations

- 4.1 The Controller shall ensure that its processing instructions, and its use of the Services, comply with Applicable Data Protection Law, including having a lawful basis for the processing and for any transfer of Patient Data to the Processor.
- 4.2 The Controller is responsible for the accuracy and quality of Patient Data it enters or causes to be entered into the Services, and for configuring patient engagement features (portal, messaging channels, retention settings) in a manner consistent with its obligations to its patients.
- 4.3 The Controller acknowledges that patient messages delivered through WhatsApp, SMS, or email contain the patient's name and appointment or study details and a secure link, and is responsible for ensuring an appropriate legal basis and patient notice for those communications.
- 4.4 The Controller shall promptly inform the Processor if it becomes aware that an instruction infringes Applicable Data Protection Law; the Parties shall then cooperate in good faith to modify the instruction.

5. Sub-processors

- 5.1 Current Sub-processors are listed in Annex B and in the Processor's public sub-processor register at clinicalris.com/legal/subprocessors.
- 5.2 The Processor shall give the Controller at least thirty (30) days' prior written notice before authorizing a new Sub-processor to process Patient Data (target; urgent security-driven replacements shall be notified as soon as reasonably practicable).
- 5.3 The Controller may object to a new Sub-processor on reasonable, data-protection-related grounds by written notice within the notice period. The Parties shall discuss the objection in good faith. If the objection cannot be resolved, the Controller may terminate the affected Services (or the master agreement, if the affected Services cannot be severed) without penalty, receiving a pro-rata refund of prepaid fees for the terminated Services.
- 5.4 The Processor shall impose data protection obligations on each Sub-processor that are no less protective than those in this DPA, and remains liable to the Controller for the performance of each Sub-processor's obligations to the extent the Sub-processor fails to meet them.

6. International Transfers and Data Residency

- 6.1 Residency disclosure. The Controller acknowledges that, as of the Effective Date, the primary production environment processing Patient Data is located in the United States of America, with infrastructure available in the European Union; the current arrangement for the Controller is stated at onboarding and in the platform's data-residency disclosure.
- 6.2 Where the Controller is established outside the United States, transfers of Patient Data to the Processor and its Sub-processors constitute international transfers. The Processor shall support such transfers with a valid transfer mechanism, which the Parties incorporate by reference where applicable:
 - for controllers subject to the GDPR or UK GDPR, the EU Standard Contractual Clauses (module two: controller to processor) and the UK International Data Transfer Addendum, each as incorporated by Annex E; and
 - for other jurisdictions, contractual terms at least equivalent, including the local annexes (C or D) where applicable.
- 6.3 Where the Controller requires Patient Data to remain within a specific territory, the Parties shall agree a hosting arrangement (including the local-PACS mode in which imaging studies are stored on the Controller's own in-country server) before processing begins; the agreed arrangement prevails over clause 6.1 for that Controller.

7. Security Incident Management and Notification

- 7.1** The Processor shall maintain appropriate incident response procedures and shall notify the Controller without undue delay, and in any event with a target of forty-eight (48) hours, after becoming aware of a Personal Data Breach affecting Patient Data, unless the breach is unlikely to result in a risk to Data Subjects (in which case the Processor shall keep a record and inform the Controller on request).
- 7.2** The notification shall, to the extent known: describe the nature of the breach, the categories and approximate number of records and Data Subjects concerned, the likely consequences, and the measures taken or proposed; and identify a contact point. Information may be provided in phases as it becomes available.
- 7.3** The Processor shall take reasonable steps to contain, investigate, and mitigate the effects of the breach and shall provide reasonable cooperation to enable the Controller to meet its own regulatory notification obligations (including any 72-hour or 60-day windows applicable to the Controller).
- 7.4** The Controller is responsible for determining whether and how to notify regulators, patients, or other affected parties for processing carried out on its instructions, and for the content of any such notification.

8. Data Subject Rights

- 8.1** The Processor shall provide reasonable assistance to the Controller in fulfilling Data Subject requests to access, rectify, erase, restrict, or port Patient Data, including by exporting the relevant records (reports in PDF/structured formats and DICOM studies in standard format) within a reasonable period.
- 8.2** If a Data Subject complaint or request is received directly by the Processor, the Processor shall forward it to the Controller without undue delay and shall not respond substantively without the Controller's authorization (except to direct the Data Subject to the Controller).
- 8.3** The Parties acknowledge that statutory medical record retention obligations may lawfully override a request to erase clinical records; where deletion is not permitted, the Processor shall restrict processing instead where feasible.

9. Audits and Inspections

- 9.1** The Processor shall make available to the Controller, on reasonable notice and no more than once per year (unless following a Personal Data Breach or where required by a regulator), the information reasonably necessary to demonstrate compliance with this DPA.

- 9.2** Where Applicable Data Protection Law requires an audit or on-site inspection, the Parties shall agree in advance its scope, timing, duration, and security and confidentiality controls. The Controller may appoint a bound-to-confidentiality independent auditor. The Controller shall bear the costs of its audit unless it reveals material non-compliance with this DPA.

10. Retention, Return and Deletion

- 10.1** During the term, the Processor retains Patient Data as configured by the Controller and instructed by law; the Controller manages retention settings for its records.
- 10.2** Upon termination or expiry of the Services, the Controller may request export of its complete Patient Data, including DICOM studies and structured reports, in standard formats. The Processor shall provide the export within thirty (30) days of the request and reasonable migration assistance.
- 10.3** After the export window closes (or, if no export is requested, thirty (30) days after the end of the Services), the Processor shall securely delete the Controller's Patient Data, including from backups, within ninety (90) days, and shall confirm deletion in writing upon request.
- 10.4** The only Patient Data the Processor may retain after deletion is that which it must keep to comply with a legal obligation, held under restricted processing and only for so long as required; and de-identified statistical data that can no longer be linked to any Data Subject.

11. AI-Assisted Analysis Terms

- 11.1** Where the Controller enables AI-assisted analysis, the Processor submits the relevant study to its contracted GPU-inference Sub-processor (Annex B) via a secure, single-study, expiring download token.
- 11.2** The Processor requires of the inference Sub-processor, and attests to the Controller, a zero-retention arrangement: submitted studies are processed in ephemeral worker environments, are not persisted after the completion of the job, and are not used to train, fine-tune, or evaluate any model.
- 11.3** AI outputs are decision-support only. The Processor does not practice medicine; the Controller's licensed practitioners remain solely responsible for interpretation and diagnosis (as further stated in the master agreement).

12. Liability and Indemnity

- 12.1** Each Party's liability arising under or in connection with this DPA is subject to the limitations and exclusions of liability in the master agreement, except that liability arising

from a Party's breach of its data protection obligations under this DPA shall not be subject to the exclusion of indirect or consequential loss to the extent such loss flows directly from that breach. [LIABILITY CAP — TO BE CONFIRMED WITH COUNSEL]

12.2 Nothing in this DPA limits either Party's liability that cannot lawfully be limited.

13. Term and Termination

13.1 This DPA takes effect on the Effective Date and continues for as long as the Processor processes Patient Data on behalf of the Controller.

13.2 This DPA terminates automatically when the Processor has deleted or returned all Patient Data in accordance with clause 10. The Processor may suspend processing if the Controller's instructions would require the Processor to breach Applicable Data Protection Law, after notifying the Controller and allowing a reasonable cure period.

14. Governing Law and Disputes

This DPA and any dispute arising out of or in connection with it are governed by the laws of the Republic of Ghana. The Parties submit to the jurisdiction of the competent courts of Ghana, sitting at the High Court of Justice, Accra. The Parties will attempt to resolve any dispute amicably before commencing proceedings. A country Annex may specify mandatory local provisions for data protection matters which prevail for that Controller.

15. General Provisions

15.1 Order of precedence. Where there is a conflict between this DPA and the master agreement regarding the processing of Personal Data, this DPA prevails. Where an applicable Annex conflicts with the core terms, the Annex prevails for Controllers in that jurisdiction.

15.2 Amendments. The Processor may update this DPA to reflect changes in the Services or Applicable Data Protection Law by giving the Controller at least thirty (30) days' notice; material changes to the Controller's obligations require the Controller's agreement. Version changes are re-presented for acceptance in the platform.

15.3 Notices. Notices under this DPA shall be in writing to the contacts in the Parties section or as updated in writing. The Processor's privacy contact is privacy@clinicalris.com; security contact is security@clinicalris.com.

15.4 Severability; entire agreement; counterparts. If any provision of this DPA is invalid or unenforceable, the remainder continues in force, and the Parties shall replace it with a valid provision reflecting its intent. This DPA, its Annexes, and the master agreement form the

entire agreement of the Parties on the processing of Personal Data. This DPA may be executed in counterparts, including electronically.

Execution

The Parties have executed this Data Processing Agreement by their authorized representatives as of the Effective Date.

For the Controller

Name: [PLACEHOLDER]

Title: [PLACEHOLDER]

Signature: _____

Date: [____/____/____]

For the Processor

Name: [PLACEHOLDER]

Title: [PLACEHOLDER]

Signature: _____

Date: [____/____/____]

Annex A — Technical and Organizational Measures

The measures below are implemented in the Services as deployed. They are maintained on an ongoing basis and reviewed as the platform evolves.

- Transport security: All access over TLS with automatic certificate management; cleartext HTTP redirected. Machine-to-machine study transfers use HMAC-signed tokens scoped to a single study and expiring within one hour.
- Infrastructure isolation: Dedicated, single-tenant servers administered by the Processor; each platform component (application, database, imaging archive, viewer, translation, transcription, antivirus) runs in an isolated container on a private network, with a reverse proxy as the only public entry point.
- Tenant scoping: Every request is scoped to the requester's organization at the API layer; cross-organization access is enforced in code and covered by regression tests.
- Access control: Role-based permissions with per-resource granularity; least-privilege administration; every administrative action audit-logged.
- Authentication: Two-factor authentication (TOTP authenticator apps, WebAuthn passkeys, backup codes), mandatory for administrators with a configurable per-organization policy; automatic account lockout after repeated failures; step-up confirmation for sensitive actions.
- Audit logging: Study views, exports, edits, anonymizations, report signings, and message sends are logged with user identity, timestamp, and source address, and exported off-site as a tamper-evident, hash-chained archive.
- Abuse controls: Rate limiting on patient portal and share links and on authentication endpoints.
- Upload screening: Patient-uploaded files are virus-scanned (ClamAV) before storage.
- De-identification tool: On-demand creation of de-identified study copies for research or teaching, with tag-level scrubbing of identifiers; every use audit-logged.
- Vulnerability management: Automated daily scanning of software dependencies against published vulnerability databases; tracked remediation.
- Data minimization in messaging: Patient notifications carry name, appointment details, and a secure link — never report contents.
- Local-PACS mode: Optional deployment in which imaging studies are stored on the Controller's own in-country server.

Annex B — Sub-processors

Current as of the Effective Date. The live register is maintained at clinicalris.com/legal/subprocessors. Per-deployment providers (SMS, email) are confirmed to the Controller at onboarding.

Contabo	Physical hosting of the Processor's dedicated servers. Location: United States (primary); European Union available.
RunPod	GPU inference for AI-assisted analysis, when enabled. Receives the study being analyzed via expiring secure link; zero-retention after processing (clause 11). Location: United States.
WhatsApp (Meta)	Delivery of patient/physician messages when the Controller enables WhatsApp. Receives phone number and message content. Location: United States (global routing).
SMS gateway (as configured)	SMS delivery. Receives phone number and message content. Location: varies by provider.
Email provider (as configured)	Transactional email. Receives recipient address and message content. Location: varies by provider.
Payment processors (Stripe, PayPal, Flutterwave, Pystack)	Online payments and payouts, where enabled. Receive payer/recipient name, email, amount, and reference; no clinical data. Location: United States / Nigeria / Ghana.
GitHub	Off-site integrity archive of the audit trail with identifiers redacted; private repository. Location: United States.

Annex C — Ghana (Data Protection Act, 2012 — Act 843)

This Annex applies where the Controller is established in Ghana or the processing is otherwise subject to Act 843. It supplements the core terms.

- C.1** The Parties acknowledge that the Controller is responsible for registering with the Data Protection Commission as required for its activities, and the Processor shall reasonably assist with information the Controller needs for its registration or notifications concerning the Services.
- C.2** Act 843 follows a controller/processor model consistent with this DPA. The Processor shall process Personal Data only for the specified purpose, on Documented Instructions, and shall not transfer Personal Data outside Ghana except as permitted by Act 843 and this DPA, including with the safeguards in clause 6.
- C.3** The security, breach-response, data-subject-rights, and retention provisions of this DPA are intended to satisfy the Processor's obligations under Act 843 for the processing carried out under this Agreement.
- C.4** [PLACEHOLDER: any additional registration, licensing, or local representation requirements confirmed with Ghanaian counsel at onboarding.]

Annex D — Nigeria (Nigeria Data Protection Act 2023)

This Annex applies where the Controller is established in Nigeria or the processing is otherwise subject to the NDPA. It supplements the core terms.

- D.1** The Parties acknowledge their respective roles as data controller and data processor under the NDPA. Where required by the NDPA or the Nigeria Data Protection Commission for the scale or nature of the processing, the Controller is responsible for filing the applicable registrations or notices, and the Processor shall reasonably assist with the information required.
- D.2** The Processor shall implement the security safeguards, breach notification, data-subject support, and accountability provisions of this DPA in a manner consistent with the NDPA, including support for the Controller's own breach reporting duties to the Commission where applicable.
- D.3** [PLACEHOLDER: any additional local requirements confirmed with Nigerian counsel at onboarding.]

Annex E — EU / UK (GDPR and UK GDPR)

This Annex applies where the Controller is established in the EU/EEA or the UK, or the processing is otherwise subject to the GDPR or UK GDPR. The core terms of this DPA are intended to satisfy Article 28(3) GDPR.

- E.1** Standard Contractual Clauses. In respect of transfers of Personal Data from the EU to the Processor, the EU Commission Standard Contractual Clauses for controller-to-processor transfers (Decision 2021/914, Module Two) are incorporated by reference and shall apply as if executed by the Parties, with: (a) Clause 17 governed by the law identified in clause 14; (b) Clause 18(b) disputes resolved in that forum; (c) Annex I populated by the details of processing in clause 2.2 and the Party information above; (d) Annex II populated by Annex A of this DPA; and (e) Annex III populated by Annex B of this DPA. Where the UK GDPR applies, the UK International Data Transfer Addendum is incorporated by reference with the tables completed by reference to this DPA.
- E.2** Where the GDPR applies, the Processor shall assist the Controller with data protection impact assessments and prior consultations with supervisory authorities to the extent reasonable.
- E.3** On termination, Clauses 8.5 and 16 of the incorporated Standard Contractual Clauses apply as modified by clause 10 of this DPA.

Annex F — United States (HIPAA Business Associate Terms)

This Annex applies only where the Controller is a HIPAA Covered Entity (or a Business Associate acting for one) and Patient Data includes Protected Health Information. In that case the following Business Associate terms apply in place of (or, if the Parties so agree, alongside) the GDPR-style provisions.

- F.1** The Processor (as Business Associate) shall use PHI only to provide the Services and as permitted by this DPA and HIPAA (45 CFR Parts 160 and 164); shall not use or disclose PHI other than as permitted; and shall not sell PHI or use it for marketing.
- F.2** The Processor shall implement the administrative, physical, and technical safeguards of the HIPAA Security Rule with respect to electronic PHI, including Annex A as the Processor's safeguard documentation, and shall report Security Incidents and breaches to the Controller without unreasonable delay and no later than the timelines in clause 7 (which the Parties intend to satisfy the Controller's own obligations, including any 60-day outer window).
- F.3** The Processor shall ensure Sub-processors (subcontractors) that create, receive, maintain, or transmit PHI agree in writing to the same restrictions, per clause 5; shall make PHI available for access, amendment, and accounting of disclosures requests per clause 8; and shall return or destroy PHI at termination per clause 10, retaining PHI only where infeasible to return or destroy and for no other purpose.
- F.4** The Controller shall not instruct the Processor to use or disclose PHI in a manner that would violate HIPAA if done by the Controller.
- F.5** [NOTE: This Annex is a framework. Where a US Covered Entity executes this DPA, the Parties should have healthcare counsel review or supplement it with the Covered Entity's own BAA form if required.]