Aurora Data Processing Agreement Template

Template de trabajo para revision legal. No constituye asesoria juridica y debe adaptarse a la clinica, cadena de subencargados y jurisdiccion aplicable.

Data Processing Agreement Template

Working template for Aurora deployments that send patient data to an external AI router or model provider.

This document is a product-and-engineering template for counsel review. It is not legal advice and must be adapted for the specific clinic, vendor chain, and jurisdiction.

Scope

Use this template when Aurora relies on an external LLM processor, including:

- routing layers such as OpenRouter;
- downstream model providers selected through the router;
- any clinical AI workflow that may carry patient identifiers or health data.

Ecuador LOPDP minimum posture

Before using this template in production, confirm that the final customer-facing information flow covers the minimum Article 12 information duties and that the contract reflects the processor obligations required by Ecuador's LOPDP.

Aurora should treat the following as mandatory checklist items:

- controller identity and contact details
- processor identity and contact details
- data protection contact or delegate when applicable
- exact processing purposes
- categories of personal data
- explicit mention of sensitive data, including health data
- lawful basis used for each flow
- whether consent is required for the specific use case
- recipients and categories of recipients
- subprocessor list and routing model
- international transfers and destination countries
- retention periods or retention criteria
- security and confidentiality controls
- patient-rights channel and response workflow
- consequences of refusal where applicable
- existence of automated assistance and human clinical review
- incident notification and contract escalation path

Template

1. Parties and roles

Controller / Responsable

- Legal name:
- RUC / registration:
- Address:
- Contact email:
- Data protection contact:

Processor / Encargado

- Legal name:
- Registration / jurisdiction:
- Address:
- Contact email:
- Security contact:

Subprocessors / downstream model providers

- Allowed providers:
- Countries / regions:
- Routing restrictions:
- Data collection setting:
- Zero-retention setting:

2. Object

The processor will process personal data strictly on behalf of the controller for the operation of Aurora's AI-assisted clinical workflows, limited to the purposes described in this agreement and only under documented instructions from the controller.

3. Processing description

- Aurora module(s):
- Use case(s):
- diagnostic assistance
- SOAP drafting
- patient summary
- messaging or triage
- Data subjects:
- patients
- guardians
- staff users, if applicable
- Categories of data:
- identification data
- contact data

- clinical notes
- diagnoses
- medications
- images or files, if applicable
- other sensitive data:
- Processing operations:
- transmission
- inference
- temporary storage
- deletion
- audit logging

4. Lawful basis and consent posture

The parties acknowledge that health data is sensitive data. The controller is responsible for documenting the lawful basis for each workflow.

Complete this section explicitly:

- lawful basis for care delivery flow:
- lawful basis for analytics or product-improvement flow:
- whether patient consent is required for this AI use case:
- consent collection surface:
- consent evidence stored in Aurora:
- `pacientes.ai_consent_granted`
- additional evidence:

Important:

- `ai_consent_granted` is not a substitute for processor contracts or transfer controls.
- If the use case requires consent, the patient-facing copy must disclose external AI assistance and data routing.

5. Controller instructions

The processor may process data only on documented instructions from the controller and only for the approved Aurora workflows described above.

The processor must not:

- use the data for unrelated training or product development unless explicitly authorized in writing;
- route PHI-bearing requests to unapproved subprocessors;
- retain identifiable patient data beyond the agreed retention window;
- disable zero-retention or data-collection restrictions without written approval.

6. Security and confidentiality

The processor shall implement appropriate technical and organizational measures, including at minimum:

- encryption in transit
- access control and least privilege
- logging and auditability
- staff confidentiality obligations
- secret rotation
- vulnerability and patch management
- deletion workflow after retention period

Aurora-specific controls to require:

- provider allowlist for PHI-bearing requests
- `zdr = true` where the vendor supports it
- `data_collection = deny` where the vendor supports it
- prompt minimization and pseudonymization where clinically feasible

7. International transfers

This processing may involve international transfers.

The agreement must state:

- whether data leaves Ecuador
- the countries or regions involved
- the transfer mechanism relied upon
- the subprocessor chain participating in the transfer
- how the controller can suspend or restrict those transfers

8. Retention and deletion

- max retention for request content:
- max retention for logs:
- deletion SLA after request completion:
- deletion SLA after contract termination:
- evidence or certificate of deletion:

9. Subprocessors

The processor must disclose and keep updated the list of subprocessors relevant to Aurora's workflow.

The agreement should require:

- prior notice of material subprocessor changes
- controller right to object to new subprocessors

- ability to restrict routing to an approved allowlist
- contractual flow-down of confidentiality and security obligations

10. Data subject rights support

The processor must support the controller in responding to:

- access
- rectification
- deletion
- opposition
- portability where applicable
- review of automated or AI-assisted processing information

Aurora operational owner:

- rights inbox:
- response SLA:
- escalation path:

11. Incident notification

The agreement should define:

- processor notice channel
- notice deadline
- minimum content of the notice
- Aurora engineering escalation owner
- clinic escalation owner

Suggested minimum notice fields:

- date and time detected
- systems affected
- categories of data affected
- number of records affected
- containment action taken
- pending actions

12. Audit and evidence

The controller should retain the right to request evidence of:

- current subprocessor list
- active retention settings
- security certifications or equivalent controls

- incident logs relevant to the processing
- contract version in force

13. AI-specific clauses

Add these clauses explicitly:

- human clinician review remains mandatory for any clinical suggestion
- the processor may not present generated output as a medical diagnosis made by the vendor
- the controller may disable AI routing immediately for compliance or safety reasons
- the controller may require model or provider restriction by geography, retention policy, or specialty risk

Patient-facing information block

If consent is the lawful basis for the specific flow, the patient copy should disclose at minimum:

- that Aurora uses AI assistance to support the clinician
- whether data is sent to an external provider
- what categories of data are sent
- why the processing is performed
- whether the patient can refuse
- what happens if the patient refuses
- how to exercise data rights

Suggested short product copy:

> *Esta consulta puede usar asistencia de IA para apoyar al profesional de salud. Cuando aplique, cierta informacion clinica puede procesarse mediante proveedores tecnologicos autorizados bajo controles de seguridad y revision humana obligatoria.*

Signature block

- Controller representative:
- Processor representative:
- Date:
- Governing law:
- Annexes included:

Recommended annexes

- Annex A: processing inventory by Aurora feature
- Annex B: subprocessor allowlist
- Annex C: retention schedule
- Annex D: patient-facing consent and notice copy
- Annex E: security controls matrix