

STANDARD OPERATING PROCEDURE (SOP)

Privacy Policy and Management of Patient Information and Sensitive Data

Document Code:	SOP-PRIV-001 / HR-ECU
Responsible Entity:	HR Services SA (Data Controller)
Regulatory Framework:	Organic Law on the Protection of Personal Data (LOPD) of Ecuador
Official Channel:	info@hrservicesec.com (Response within 15 calendar days)
Scope of Application:	Patient Programs (Co-payments), Clinical Research, Clients, Collaborators and Suppliers

Document Index

This standard operating procedure contains the following personal data control structure:

Table of Contents Update Note:

The table of contents above will be automatically updated when you open or print this document in Microsoft Word or Google Docs.

1. Purpose, Scope and Regulatory Framework

HR Services SA establishes this Standard Operating Procedure (SOP) with the objective of regulating the activities of collection, storage, validation, processing, custody, preservation and elimination of personal data and sensitive health data under its responsibility.

1.1. Operational Purpose

This document comprehensively describes the procedures implemented to ensure data quality, information validation, discrepancy management, and rigorous confidentiality protection across all medical programs and administrative services. This Standard Operating Procedure (SOP) must be followed by all personnel until updates are made based on client requirements or contractual modifications.

1.2. Scope of the Document

The provisions of this SOP apply to all activities carried out in the following areas:

- **Patient Programs:** Patients enrolled in support and adherence programs such as the COPAGO program.
- **Medical Research:** Clinical research, epidemiological studies, and pharmacoeconomic analyses.

- **Patient Environment:** Family members, legal representatives and emergency contacts designated by the holder.
- **Personnel and Human Talent:** Job candidates, active employees and collaborators under various modalities.
- **Third Parties and Providers:** Providers of medical services, independent professionals, auditors and technology providers.
- **Digital Users:** Users of websites, interactive portals and mobile applications of health projects.

1.3. Legal Regulatory Framework

The processing of personal data carried out by HR Services is strictly based on the Organic Law on the Protection of Personal Data (LOPD) of the Republic of Ecuador, respecting the health sector regulations on the confidentiality of medical records and medical confidentiality.

2. Roles and Responsibilities in the Treatment

To ensure proper information governance, HR Services defines the following institutional responsibilities:

- **Data Controller:** HR Services is the Data Controller of the personal data collected in projects with patients undergoing treatment. It assumes the legal obligation regarding the security, legitimacy, and custody of this data in physical and digital files, whether active or inactive.
- **Internal Staff and Collaborators:** HR Services' operational, medical, administrative, and audit staff must strictly comply with the confidentiality and access segregation protocols stipulated in this SOP.
- **Data Processors (Third Parties):** Any natural or legal person who provides services to HR Services (physical custody, computer platforms, legal services, health professionals) and requires processing data on behalf of HR Services will act under the strict condition of Data Processor.

3. Categories of Personal Data Processed

Depending on the health and clinical research projects, HR Services processes different categories of personal data obtained directly from the data subject, their legal representative, or their emergency contact.

Data Category	Examples of Data Collected	Origin / Source	Sensitivity Level
Identifying Data	Full names, ID/passport number, home address, email address, contact phone number and signatures.	Data subject, legal representative or emergency contact.	Standard / Confidential
Health Data (Sensitive)	Medical history, medical diagnoses, treatment follow-up, medical prescriptions, and medication administration invoices.	The attending physician, the health center, or the patient himself.	High / Sensitive Data
Social Circumstances	Personal characteristics, family environment or socioeconomic conditions relevant to the program.	Admission forms completed by the	Sensitive / Reserved

		patient or family member.	
Supplier and Candidate Data	Resumes, professional background, billing bank details and employment references.	Candidate for the position or contracted supplier.	Standard / Commercial

4. Purposes of the Processing and Legal Bases

HR Services guarantees the principle of purpose by collecting only the data necessary for explicit and legitimate purposes.

Operational Purpose	Detailed description of activities	Legal Basis (LODPD)	Storage Period
Co-payment programs	Diagnosis, treatment monitoring, medication invoice management, prescription control, and satisfaction surveys.	Data subject consent / Contractual performance	Duration of the subscribed COPAY program.
Clinical Research and Pharmacoeconomics	Epidemiological studies, medical research, and cost-effectiveness analysis of treatments.	Express and unequivocal authorization of the patient	Study duration set in the consent.
Handling of Requests and Complaints	Management of requests, suggestions, incidents and requests for ARCO+ rights.	Legal obligation / Legitimate interest	Until the resolution of the request or requirement.
Legal and Health Compliance	Response to requests from competent health or judicial authorities.	Compliance with legal obligation imposed by regulation	Mandatory legal deadline according to health/tax law.
Contract Execution	Administration of contracts with employees, independent contractors and suppliers.	Execution of prior contractual relationship	Contract validity plus limitation periods.

5. Preservation, Custody and Destruction of Documents

Personal and health data will be kept only for the time strictly necessary to fulfill the authorized purposes or comply with legal mandates.

5.1. Retention Rules by Category

- **Patient Health Data:** Will be kept in strict compliance with the time limits established in the current national health regulations for medical records.
- **Data in Research and COPAYMENTS:** These will be kept for the duration of the project and according to the specific authorization signed by the patient.

- **Contractual Relationship and Notifications:** These will be kept throughout the contractual relationship or until the holder revokes their consent through the enabled mechanisms.

5.2. Certified Destruction Procedure

Once the legal retention period has expired or the project has ended, HR Services will proceed with the destruction of physical and digital files in accordance with its Document Destruction and Elimination Policy. This process guarantees the impossibility of recovery through secure physical shredding and certified logical deletion.

6. Data Processors and Transfer to Third Parties

To ensure operability and the highest quality of services, HR Services collaborates with specialized providers who act as Personal Data Processors.

6.1. Contractual Requirements for Third Parties

Any third party with access to data on behalf of HR Services must first sign a Data Processing Agreement that imposes:

- **Limitation of Use:** Process the data solely and exclusively under the written instructions of HR Services.
- **Security Measures:** Implement technical and organizational security measures equivalent to or better than those of HR Services.
- **Absolute Confidentiality:** Maintain strict professional secrecy regarding medical and personal information to which you have access.
- **Prohibition of Transfer:** Prohibition of delivering data to third parties except as mandated by law or express court order.

6.2. Examples of Third-Party Processors

Contracted providers include independent healthcare professionals, physical storage and archiving providers, confidential document destruction companies, external legal advisors, and IT infrastructure and software providers.

7. Operational Protocol for the Exercise of ARCO+ Rights

In accordance with Ecuador's Organic Law on the Protection of Personal Data, data subjects or their legal representatives may exercise their guaranteed fundamental rights.

7.1. Rights Guaranteed under the LOPDP

- **Right to Information:** To know the details of the processing, purposes and responsible parties.
- **Right of Access:** To obtain confirmation and a copy of your personal data in custody.
- **Right of Rectification:** Request the correction of inaccurate, outdated or incomplete data.
- **Right to Erasure:** To request the deletion of data when the purpose or term has ceased.
- **Right to Object:** To object to the processing of data for specific purposes.
- **Right to Portability:** To receive your personal data in a structured and commonly used format.

- **Right of Suspension:** Request the temporary cessation of treatment under legal grounds.
- **Right to No Automated Decision:** Avoiding decisions based solely on automated assessments.
- **Rights to Consultation and Education:** Access to educational mechanisms and direct consultations on data protection.

7.2. Step-by-Step Procedure for Handling Requests

The standardized procedure for processing any request to exercise rights is detailed in the following operational matrix:

Operational Step	Specific Activity	Responsible	Term / Condition
1. Sending the Request	Send an email to info@hrservicesec.com or a written communication indicating the right to exercise and the specific data.	Owner or Representative	Any time
2. Identity Validation	Please include a clear copy of the holder's national identity card or legal representation document.	Data Officer / LOPDP	Immediately upon receipt
3. Legal Assessment	Verification of legal origin, contractual validity and any applicable regulatory exceptions.	Legal / Operational Area	Days 1 to 10
4. Official Response	Issuance of a response informing of the exercise of the right or the reasoned refusal with legal basis.	HR Services SA	Maximum 15 calendar days

8. Technical and Administrative Security Measures

HR Services applies advanced safeguards to mitigate risks of unauthorized access, loss, alteration, or improper disclosure of personal and sensitive data.

8.1. Administrative and Organizational Measures

- **Continuing Education:** Mandatory periodic training for staff on data protection, confidentiality and good practices according to the LOPDP.
- **Confidentiality Agreements:** Individual confidentiality agreements signed by each employee and collaborator at the start of their duties.
- **Access Control:** Restrictive access policies based on the need-to-know principle according to the professional role.

8.2. Technical and Digital Measurements

- **Encryption and Web Portals:** Maintenance of security controls in web portals and COPAGOS program applications, including encryption of data in transit and at rest.
- **Backups and Incidents:** Periodic backup systems and standardized protocols for managing incidents or data discrepancies.

9. Glossary of Operational Terms

To facilitate the interpretation of this procedure, the following formal definitions are established in accordance with the legal and institutional framework:

Formal Term	Standard Operational Definition
Personal Data	Any information relating to an identified or identifiable natural person, directly or indirectly (e.g., names, ID number, address, telephone, signature).
Health-Related Data (Sensitive)	Personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveals information about their health status (e.g., medical history, diagnoses, treatments).
Confidential Information	Information protected under secrecy and confidentiality that can only be provided to its owner or to formally authorized third parties through legal or contractual support.

Dissemination and Validity Control:

This instrument will be permanently included in the HR Services SA operations manuals and will be mandatory in all programs that process patient information.