

PAIA Manual

Prepared for a private body in terms of section 51 of the Promotion of Access to Information Act 2 of 2000, as amended

Document details: PAIA Manual

Private body	PonyaData (Pty) Ltd
Registration number	2026/556145/07
Registered / principal address	7 Acacia Road, Duxberry, Morningside, Sandton 2191
Head of private body / Information Officer	Matthew Trusler
Deputy Information Officer	Dr Jessica Trusler
Email / telephone	info@ponyadata.com / 082 399 8678
Public PAIA-manual URL	ponyadata.com/paia-manual
Effective / last updated	17 September 2026

1. Introduction and purpose

Purpose. This manual assists a person to identify records held by PonyaData and the procedure for requesting access under PAIA. It also describes categories of personal information and processing for purposes of POPIA transparency.

Business. PonyaData develops and supports health-technology and practice-management services, including beta deployments with healthcare practices. PonyaData may hold its own corporate, workforce, user, support and service records and may process patient information as operator for practices. A PAIA request to PonyaData cannot automatically compel disclosure of a practice's record where PonyaData is not the responsible record holder or disclosure is otherwise prohibited.

Availability. This manual is available for inspection on request from info@ponyadata.co.za, subject to lawful reproduction arrangements. It is available in English. Reasonable accessibility assistance may be requested.

2. Information Regulator guide

PAIA Guide. The Information Regulator has published a guide on how to use PAIA, including assistance and remedies. Current guides, forms and contact details are available at <https://inforegulator.org.za/paia/> and from the Information Regulator.

Information Regulator contact	
Website	https://inforegulator.org.za/
Telephone	010 023 5200
Email	enquiries@inforegulator.org.za
Physical address	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg
Postal address	P.O. Box 31533, Braamfontein, Johannesburg, 2017

3. Records automatically available

Without a PAIA request. The following records may be obtained without Form 2 where publicly available or provided through the stated channel. Availability does not waive copyright, confidentiality, security or lawful-use restrictions.

Category	Examples	Access route
Public corporate information	Registration details, public policies and contact information.	Website / CIPC as applicable
Public product and legal information	Public service descriptions, privacy notices, PAIA manual and published terms.	Website
Requester's own service information	Certain portal/account information, subject to verified identity and applicable POPIA/PAIA process.	Account / request process
Other category	NONE	

4. Records held and applicable legislation

Record category	Examples
Corporate and governance	Incorporation, shareholders, board, policies, risk, compliance and insurance.
Finance and tax	Accounting, banking, invoices, budgets, tax, audit and procurement.
People and contractors	Recruitment, employment, performance, payroll, training, access and contracts.
Customers, practices and users	Contracts, onboarding, configuration, users, support, billing and service records.
Product, technology and security	Design, source/configuration, testing, releases, logs, incidents, vendors and continuity.
Privacy and information governance	ROPA, PIIAs, notices, requests, incidents, operators, retention and evidence.
Marketing and website	Website, communications, enquiries, events and lawful marketing preferences.
Intellectual property and legal	Trade marks, copyright, licences, disputes and legal advice.

Legislation. Records may be maintained under laws applicable to the business, including PAIA, POPIA, Companies Act, Income Tax Act, VAT Act, Tax Administration Act, Basic Conditions of Employment Act,

03. PAIA manual

Labour Relations Act, Employment Equity Act, Occupational Health and Safety Act, Electronic Communications and Transactions Act, Consumer Protection Act, Copyright Act, Trade Marks Act and other health, professional, contractual or sector laws applicable to actual activities. This list must be reviewed and localised; it does not imply every statute applies to every record.

5. Request procedure

- Use the current prescribed Form 2 — Request for Access to Record — available from <https://info regulator.org.za/paia/>.
- Submit it to Matthew Trusler, info@ponyadata.co.za. Describe the record sufficiently, preferred access form and contact details.
- For a private body, identify the right to be exercised or protected and explain why the requested record is required for that right.
- Provide satisfactory proof of identity and authority. Agents must provide authority and proof for both agent and requester.
- Pay the prescribed request fee, if applicable, after notice. Search/preparation and access fees may also apply; a deposit may be required where permitted.
- PonyaData ordinarily decides within 30 days, subject to a lawful extension. Form 3 is used for the outcome and fees payable.
- Access may be granted, partially granted, transferred/referred where appropriate, or refused on PAIA grounds. Reasons and remedies will be given.

Grounds and remedies

Refusal or severance. PAIA contains mandatory and discretionary grounds protecting privacy, commercial/confidential information, safety, law-enforcement interests, legally privileged material, research and other protected interests. PonyaData must consider severability and disclose any reasonably separable portion not protected.

Complaint / court. A requester may complain to the Information Regulator using current Form 5, generally within the prescribed period, or seek court relief as permitted. A private body has no compulsory internal appeal unless it voluntarily provides a review that does not displace statutory remedies.

6. Personal information processing

Category	Data subjects / information	Purposes	Recipients
Customers / practices	Contacts, contracts, billing, configuration and communications	Contract, service, support, compliance	Personnel and providers
Practice users	Identity, role, professional identifiers, logs, support and security	Accounts, access, service, audit and security	Practice, PonyaData and providers
Patients (often as operator)	Identity, health, communications, billing and clinical records as configured	Practice-directed care workflow and administration	Practice/care team/integrations
Workforce / applicants	Identity, employment, payroll, performance, access and training	Employment / contracting, security and law	HR / payroll / advisers / authorities
Suppliers / contacts	Identity, contract, payment and communications	Procurement, payment and relationship	Personnel / banks / advisers
Website / enquiries	Contact, device/cookie, enquiry and preference data	Website, response, security and lawful communications	Hosting / analytics / communications

Cross-border flows. The intended PonyaData architecture is South Africa based. The Company does not intend routine processing of identifiable Health Information outside South Africa. However, cross-border transfer or access may occur if a Patient directs sharing with an overseas provider, if an authorised international care team is involved, if an overseas support or vendor access path is used, if global disaster-recovery or security tools are used, or if approved research or AI validation involves an overseas collaborator.

Health Information must not be transferred to, accessed from, hosted in, backed up in, supported from, or otherwise processed in another country unless the Responsible Party allocated to the affected data flow has approved and documented the transfer and POPIA section 72, POPIA section 57 where triggered, and any applicable health-information regulations are satisfied. Safeguards may include an adequacy assessment, binding corporate rules, binding agreements with substantially similar protection, data subject consent, contract necessity, benefit to the data subject, genuine de-identification, encryption,

03. PAIA manual

role-based access, transfer-impact assessment, and Data Transfer or Data Sharing Agreements where required.

Before a material cross-border transfer of identifiable Health Information for which the Company is Responsible Party, the Company will give appropriate notice of the transfer, the country or categories of countries involved, the recipient or recipient category, the purpose, the level of protection or safeguards, and the Patient choices where required. Where the proposed Company-controlled transfer involves special personal information or children's Personal Information to a third party in a foreign country that does not provide an adequate level of protection as contemplated in POPIA section 72, the Company must obtain prior authorisation from the Information Regulator under POPIA section 57 read with section 58 before the transfer, or restructure the activity so that it is genuinely de-identified, patient-directed, routed to an adequate-protection recipient, or otherwise lawfully authorised and documented. Where the Company is Operator, it must not initiate or authorise a cross-border transfer of Practice-controlled clinical records unless the relevant Responsible Party has issued documented instructions or Applicable Laws require the transfer, and it must alert the Responsible Party to any section 57 trigger it identifies.

Where prior authorisation under section 57 is required and the Information Regulator has not published a procedural framework or has not responded to an application within 90 days, the Company shall document the application, the delay, and the safeguards in place, and may proceed on the basis of binding agreements providing substantially similar protection as contemplated in section 72(1)(a), pending the Regulator's response, provided the Company has taken reasonable steps to mitigate risk.

For clarity, a Patient's own decision to disclose or share their record with an international recipient through the Global Health Record is treated as patient-directed sharing, provided the Patient chooses the recipient and scope and receives a clear warning about foreign protections. The Company remains responsible for platform security, consent logging, access controls and any POPIA duties that apply to its facilitation role, but must not treat patient-directed sharing as consent for Company-controlled overseas hosting, support access, vendor processing, research, AI validation, analytics or product improvement. Cross-border transfers for research, AI training, AI validation or commercialisation require additional safeguards under Schedule 6, including ethics approval or waiver where required, specific consent where required, de-identification where feasible, and DTA, DSA or MTA controls.

Security. PonyaData applies reasonable organisational and technical safeguards proportionate to risk, including governance, access control, authentication, logging, encryption where appropriate, supplier controls, testing, incident response, continuity and workforce confidentiality. Details that would prejudice security are not published.

Retention. Records are retained for legal, professional, contractual, operational and evidential periods, then securely destroyed, deleted or de-identified when no longer authorised to retain.

7. Approval and publication record

Approved by	Matthew Trusler
Signature / date	 17/09/2027
Public URL	ponyadata.com/paia-manual
Physical-copy location	Available from info@ponyadata.co.za
Languages / accessibility	English
Submitted/uploaded to Regulator if applicable	Reference / date - still to be submitted once the regulator has provided the necessary instructions as to the procedure
Next review	December 2026

Official forms: Use current versions from <https://infoeregulator.org.za/paia/>: Form 2 (request), Form 3 (outcome/fees) and Form 5 (complaint). Do not embed stale fee amounts or forms without verifying the current regulations.