

TERMS AND CONDITIONS

PonyaData Electronic Doctor and Patient Health Management Programme

South Africa

PonyaData means 'to heal with data'. This document reflects the intended point-of-care, practice, clinic, hospital, ward, outpatient, telehealth and patient-held health-record use cases described by the Company.

Item	Publication detail
Programme / platform	PonyaData.com
Legal entity	PonyaData (Pty) Ltd
Trading name	PonyaData
Company registration number	2026/556145/07
Registered office	7 Acacia Road, Duxberry, Morningside Sandton 2191
Principal place of business	7 Acacia Road, Duxberry, Morningside Sandton 2191
Website / app	ponyadata.com / app-ponyadata.com
Information Officer under POPIA section 56	Matthew Trusler, info@ponyadata.co.za ; 7 Acacia Road, Duxberry Morningside; 0823998678
Deputy Information Officer, if appointed	
Clinical Governance Lead	Jessica Trusler, MB ChB (UCT), DCH (SA), DTM&H (Wits), FC(Path)CLIN (SA), MMed Clinical Pathology (Wits) Mobile: 0829024929 Email: jessica@ponyadata.co.za
AI Safety / Medical Device Lead	Jessica Trusler jessica@ponyadata.co.za
SAHPRA status	classification assessment pending
Version	1
Prepared date	16 September 2026
Effective date	16 September 2026

- PonyaData is primarily a point-of-care and health-information management platform for doctors, healthcare practitioners, practices, clinics, wards, hospitals and outpatient units. Telehealth and teleconferencing are supported features but are not the sole or main use case.
- The platform supports scheduling, consultations, clinical notes, referral letters, discharge letters, sick notes, patient information letters, medical-aid and funder motivations, scripting workflows, laboratory and imaging requests, billing support, triage, medication safety alerts, adverse-event reduction, patient education and a patient-held/global health record.
- AI Functions are used as assistive workflow, documentation, summarisation, safety and decision-support tools. PonyaData is designed on a human-in-the-loop model. AI must support and not replace clinical judgement.
- The intended data architecture is South Africa based, with no routine processing of identifiable Health Information outside South Africa. Any cross-border access, support, hosting, patient-directed sharing, research collaboration or vendor processing must meet POPIA section 72 safeguards.

Document structure

Part	Purpose
Main Terms	Binding terms for patients, practices, practitioners, administrators, caregivers and authorised users.
Schedule 1	POPIA privacy notice, binding Responsible Party / Operator role allocation, layered lawful-basis table, children/representative access controls and retention notice.
Schedule 2	Digital health and telehealth informed consent language.
Schedule 3	AI-assisted healthcare notice, AI Function Register and model-card controls.
Schedule 4	Practice and healthcare practitioner addendum.
Schedule 5	Narrowed Break Glass emergency-access terms.
Schedule 6	Research, analytics, data sharing and model development controls.
Schedule 7	Cybersecurity and incident response schedule, including POPIA section 22 notice from awareness/reasonable belief.
Schedule 8	Retention and deletion schedule aligned to POPIA section 14, health-record minimums, patient-held retention, occupational-health 20-40 year regulation-specific rules and de-identification.
Schedule 9	Legal and ethical source alignment matrix, including PAIA, MHCA, direct marketing, occupational-health and medical-scheme complaint routes.

Main Terms

1. Introduction, acceptance and legal effect

These Terms and Conditions apply to the use of PonyaData, including the website, mobile application, patient portal, practitioner portal, practice administration portal, electronic health record, scheduling, communication, point-of-care workflow, telehealth, remote monitoring, billing support, analytics and AI-enabled functions made available by the Company from time to time.

By registering for an account, logging in, booking or attending a consultation, uploading information, accepting a consent screen, using a digital health record, communicating with a Practitioner, using a Practice account, or otherwise using PonyaData, you agree to these Terms. If you act for a Practice, Patient, child, dependent, incapacitated person, juristic person or health establishment, you warrant that you have authority to do so.

Electronic acceptance, click-wrap acceptance, data messages, electronic signatures, audit logs and electronic records may be used to evidence agreement, consent, instructions and notices to the extent permitted by the Electronic Communications and Transactions Act 25 of 2002 and other Applicable Laws.

These Terms operate with any privacy notice, informed consent, clinical consent, telehealth consent, AI notice, practitioner agreement, practice agreement, data processing agreement, research consent, medical-device labelling, service-specific terms, fee schedule, support policy, facility policy, or third-party mandate applicable to a particular service. The more specific or legally mandatory term prevails to the extent of any inconsistency.

Nothing in these Terms limits any constitutional right, patient right, statutory remedy, professional duty, regulator power, non-excludable consumer right, health-record access right, confidentiality duty, emergency-care duty, or liability that cannot lawfully be limited under South African law.

The Information Officer has been registered with the Information Regulator in accordance with section 56 of POPIA, or such registration is in progress and will be completed as soon as is available.

2. Corporate identity and accountable officers

The Information Officer is responsible for the POPIA and PAIA accountability functions allocated to an information officer under Applicable Laws, including internal compliance frameworks, request handling, complaint routing,

breach governance and regulator engagement. The Clinical Governance Lead is responsible for clinical safety governance, practitioner-facing escalation, patient-safety review and coordination with the AI Safety or Medical Device Lead where a clinical or AI safety issue arises.

The absence of completed corporate details must not be treated as a waiver of any User's rights.

3. PonyaData purpose and operating model

PonyaData is designed to make medicine safer, healthcare practitioners happier and patients healthier by reducing administrative burden, reducing waste and adverse events, improving communication and presenting relevant information succinctly at the point of care.

PonyaData may be used in doctors' rooms, HCP offices, clinics, wards, hospitals, emergency units, outpatient units, multidisciplinary care teams and patient self-management journeys. It supports in-person care first, with optional remote-care and telehealth features where clinically suitable.

The platform is intended to help Practitioners and Practices with scheduling, triage, consultations, documentation, referral letters, discharge letters, sick notes, patient information letters, motivations to medical aids and funders, prescription support, medication-safety prompts, imaging and laboratory requests, billing support, secure communications, patient education, quality improvement and continuity of care.

PonyaData may support a patient-held or shared longitudinal health record. Patients may authorise access for Practitioners, hospitals, emergency teams, carers or new healthcare providers. Access must be role based, purpose limited, auditable and subject to the confidentiality and POPIA controls in these Terms.

4. Legal status of the Company, Practitioners and clinical services

Unless a service-specific document states otherwise, the Company provides technology, information-management, workflow, communication, security, analytics and AI-support services. The Company does not itself practise medicine merely by making the platform available.

Clinical Services are provided by Practitioners registered or authorised by the relevant statutory council or law, including where applicable the HPCSA, SANC, SAPC, AHPCSA, SADTC, SACSSP or another statutory health/professional council, and by health establishments acting within lawful scope. Practitioners remain responsible for clinical judgement, diagnosis, treatment, prescription, referral, discharge, certification, record-keeping and patient communication.

Where the Company employs, contracts with, supports or receives services from Practitioners, the arrangement must be structured so that it does not unlawfully interfere with professional independence, does not constitute prohibited corporate practice of medicine, does not create unlawful fee-splitting, and does not create perverse incentives.

If any PonyaData feature is or may be a regulated medical device, Software as a Medical Device, in-vitro diagnostic device, or component of a regulated device, the Company must complete and document the SAHPRA classification and regulatory pathway before marketing or deploying that feature for the regulated intended use. The public-facing document will be updated to identify the applicable SAHPRA status, authorisation, licence, intended use and limitations where required.

5. Definitions

Term	Meaning
Applicable Laws	All South African laws, regulations, guidelines, ethical rules, licence conditions, professional standards, regulator requirements, facility requirements and binding contractual requirements that apply to PonyaData.
AI Function	Any artificial intelligence, machine learning, algorithmic, automated, predictive, generative, rules-based or decision-support function used in or with PonyaData.
AI Function Register	The Company's controlled inventory of material AI Functions, including intended use, owner, version, data inputs, outputs, validation, SAHPRA

Term	Meaning
	status, risk class, human oversight, limitations, monitoring and incident controls.
Break Glass	A controlled emergency-access process that permits time-limited access to Health Information outside normal access pathways only where legally justified for emergency care or a serious threat to the Patient's life or health, disclosure required by law or court order, or security-incident containment limited to metadata unless clinical-content access is itself legally justified.
Clinical Services	Health advice, consultation, assessment, diagnosis, treatment, prescription, referral, monitoring, counselling, care coordination, record review or related services provided by or under the supervision of a Practitioner.
Company	PonyaData (Pty) Ltd, trading as or providing the PonyaData platform, unless a service-specific agreement names another responsible entity.
Global Health Record	A longitudinal patient-held or shared health record that may be accessed by authorised Practitioners or care teams locally or internationally according to Patient consent, emergency rules and Applicable Laws.
Health Information	Personal information about a person's physical or mental health, disability, medical history, treatment, care, biological samples, genetic or biometric information, prescriptions, referrals, results, images, symptoms, risk factors, claims, appointments, communications and clinical records.
Human-in-the-Loop	A workflow in which a competent human, usually a registered Practitioner for clinical matters, reviews, edits, accepts, rejects or overrides an AI output before the output is used for a material clinical or rights-affecting purpose.
Operator	A person or organisation that processes personal information for a Responsible Party under a contract or mandate and without determining the purpose of processing. Where the Company is listed as Operator in clause 17 or Schedule 1, the relevant row and the operator agreement form the documented processing instruction.
Patient	A person receiving, seeking or managing healthcare services through PonyaData, including a child or person represented by a parent, guardian, caregiver, curator or authorised representative.
Practice	A medical practice, healthcare practice, hospital, clinic, ward, outpatient unit, health establishment or other health-sector organisation that subscribes to or uses PonyaData for healthcare-related workflows. An employer, bureau, administrator, sponsor or funder is not a Practice merely because it pays for, requests or receives occupational-health, billing or administrative outputs.
Practitioner	A natural person who is registered, licensed or otherwise authorised under a South African statutory professional council or health law, including where applicable the HPCSA, SANC, SAPC, AHPCSA, SADTC, SACSSP or another statutory council, and who uses PonyaData within lawful scope of practice. A counsellor, assistant, employee, administrator or facility staff member is a Practitioner only to the extent that they are properly registered/authorised for the relevant clinical activity or act under lawful supervision and role limits.
Responsible Party	The party that determines the purpose of and means for processing personal information under POPIA. For current PonyaData services, the binding allocations are set out in clause 17 and Schedule 1. A party is a joint Responsible Party only where a service-specific agreement and patient-facing notice expressly say so.
User	Any Patient, Practitioner, Practice, Occupational Health Client, authorised administrator, caregiver, authorised representative, support user or other person who accesses or uses PonyaData, subject to the role and access limits in these Terms.
Competent Person	For POPIA children's-information purposes, a person legally competent to consent to the processing of a child's personal information for the relevant matter, including a parent, guardian or other legally authorised

Term	Meaning
	person, except where Applicable Laws recognise the child's own confidential consent or decision-making authority.
Mature Minor	A child who is legally able to consent to a healthcare service or confidentiality-sensitive healthcare matter under Applicable Laws, including where the child is at least 12 years old and has sufficient maturity and mental capacity for medical treatment, or where another statute gives the child independent confidential consent rights.
Restricted Confidential Entry	A record entry, result, note, prescription, referral, communication or consent record that must be segmented, masked or withheld from parent, guardian, caregiver or representative access because Applicable Laws or clinical ethics protect the Patient's confidentiality, including certain sexual-health, reproductive-health, HIV, contraception, termination-of-pregnancy, mental-health, abuse, violence or safeguarding records.
Representative Access	Access granted to a parent, guardian, caregiver, curator, administrator, next of kin, proxy user or other person acting for or assisting a Patient, subject to verification, role limits, patient consent where required, statutory confidentiality limits, segmentation/masking controls and audit logging.
Business User	A Practice, Practitioner, Occupational Health Client, bureau, administrator, funder, enterprise client or other juristic person or sole proprietor using PonyaData for business, professional or institutional purposes, excluding a Patient acting as a consumer or data subject.
Consumer	A Patient, caregiver or other natural person using PonyaData in a personal, household or healthcare-recipient capacity, and any other person who qualifies as a consumer under the Consumer Protection Act for a relevant transaction.
Occupational Health Client	An employer, workplace, mine, insurer, administrator, bureau, funder or sponsor that requests, funds or receives occupational-health services or outputs through PonyaData. An Occupational Health Client is not entitled to clinical-record access merely because it pays for or requests a service.
Occupational Health Practitioner	A Practitioner who is lawfully registered and authorised to provide occupational-health, medical surveillance, fitness-for-work, workplace health, employee-assistance or similar services within scope of practice and under applicable occupational health, employment, confidentiality and POPIA rules.
Direct Marketing	Any electronic or other communication that promotes or offers PonyaData services, partner services, paid features, campaigns, programmes, wellness offerings, research recruitment or other goods or services to a User, but excluding Service Messages necessary for care, security, account administration, billing, legal notices or the service requested by the User.
Service Message	A non-marketing message necessary or reasonably required for clinical care, account administration, appointments, reminders, billing, security, legal notices, data-subject requests, patient safety, Break Glass notifications, system maintenance or a service requested by the User.
Material Change	A change to these Terms, privacy practices, AI Functionality, clinical workflow, fees, patient rights, security model, cross-border processing, research use, or consumer-risk allocation that could materially affect a User's rights, obligations, privacy, safety, costs or use of PonyaData.

6. Constitutional commitments and non-discrimination

PonyaData will be designed and administered with regard to the Constitution of the Republic of South Africa, 1996, including the rights to equality and non-discrimination, dignity, privacy and access to healthcare services.

The Company and participating Practices must not unfairly discriminate against a User or Patient on any prohibited or analogous ground, including race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth, health status,

geographic location, socio-economic status, digital literacy or ability to pay, except where a lawful and clinically justified distinction is required.

Where reasonably practicable, PonyaData should support accessible communication, appropriate language options, disability accommodations, human support, low-bandwidth alternatives, and referral to alternative care channels where the digital channel is unsuitable.

No Patient may be denied clinically appropriate human review solely because the Patient asks questions about AI, requests an explanation, challenges data accuracy, declines optional research use, or reports a concern about a digital workflow.

7. Eligibility, registration and authorised users

A User may use PonyaData only if the User can lawfully enter into these Terms or is represented by a person who may lawfully act on the User's behalf. Children, incapacitated persons and persons requiring assisted decision-making must be supported in accordance with Applicable Laws, clinical ethics and the Patient's best interests.

A Practice must register for and maintain an active account before using services that require Practice-level access. The Practice is responsible for appointing authorised users, assigning correct user roles, removing users who no longer require access, reviewing user permissions, and ensuring that each authorised user complies with these Terms.

Users must provide accurate, complete and current account information. The Company may require proof of identity, registration, authority, facility affiliation, professional status, banking information, medical scheme details or other information reasonably required to provide services safely and lawfully.

Username, passwords, access tokens and authentication methods are personal to the authorised user. They must not be shared. Users must report suspected unauthorised access immediately and take reasonable steps to reduce harm.

8. Service-specific terms, third-party integrations and mandates

Some PonyaData services may have service-specific descriptions, terms, support commitments, fees, clinical workflows, consent screens, medical-device instructions, third-party terms, or integration mandates. Those documents form part of these Terms for the relevant service.

PonyaData may integrate with laboratories, imaging providers, pharmacies, hospitals, medical schemes, administrators, payment processors, funders, communication providers, hosting providers, cybersecurity vendors, AI vendors, emergency services, coding tools or other third parties. Third-party services are subject to their own terms where applicable.

Where a Practice requests PonyaData to submit, receive, route or process information with a third party on the Practice's behalf, the Practice grants the Company the mandate required to do so for the specified purpose. The Practice remains responsible for verifying the accuracy of third-party information, claims, codes, prescriptions, motivations, clinical content and billing information before relying on or submitting it.

The Company may update, improve, replace, suspend or withdraw features. Changes affecting patient safety, clinical continuity, personal information, AI functionality, regulated medical-device functions or material user rights must be managed with appropriate notice, risk assessment, change control and legal compliance.

9. Emergency care and urgent situations

PonyaData is not a substitute for emergency medical services. In any emergency or situation where delay may create serious risk to life, health, safety, pregnancy, mental health, disability, violence, abuse, self-harm, overdose, poisoning, severe pain, chest pain, breathing difficulty, stroke symptoms, severe bleeding, seizures, loss of consciousness, severe allergic reaction, suicidal intent, psychosis, or another urgent condition, the Patient must contact local emergency services or go to the nearest emergency unit, clinic or hospital.

PonyaData may assist emergency care by making relevant records available through Break Glass access where the Patient has a record on the platform and access is lawful, clinically justified and auditable. Break Glass access is governed by clause 20 and Schedule 5.

Messages, portal submissions, forms, questionnaires, AI prompts and appointment requests may not be read immediately and must not be relied on for emergency response unless the Company has expressly identified a specific emergency workflow for that purpose.

10. Patient responsibilities

Patients and authorised representatives must provide information that is accurate, complete and current, including symptoms, medical history, allergies, medicines, pregnancy status, diagnoses, disabilities, test results, imaging, contact details, location, identity information and emergency contacts where requested.

A Patient must tell the Practitioner if information in PonyaData is wrong, outdated, incomplete, generated by another person, imported from another system, or not intended for clinical use.

Patients remain responsible for seeking emergency care where necessary, attending consultations, arranging follow-up, using medicines as prescribed, reporting adverse events, asking questions if advice is unclear, and informing Practitioners of changes in condition.

Patients must protect their devices and login details, use the Programme in a private and safe setting where possible, and not share access with another person unless that person is authorised to help with their care.

11. Practice and Practitioner responsibilities, professional independence and ethical conduct

Practitioners must maintain current professional registration, scope of practice, qualifications, professional indemnity or insurance where required, and authority to practise in the relevant setting. Practices and health establishments must maintain required licences, certificates, facility approvals, accreditation, insurance and operational standards applicable to their services.

Practitioners and Practices must comply with the Health Professions Act, professional board rules, HPCSA ethical guidelines, National Health Act obligations, POPIA, facility licensing requirements, SAHPRA requirements where applicable, billing rules, medical scheme rules and all other Applicable Laws.

PonyaData must not be used to create or facilitate unlawful corporate practice of medicine, unlawful employment or control of Practitioners, fee-splitting, kickbacks, perverse incentives, over-servicing, fraudulent coding, improper referrals, unnecessary tests, unlawful prescriptions, misleading medical-aid motivations or billing misconduct.

No Practitioner may adopt a PonyaData-generated prescription, referral, motivation, sick note, discharge letter, request form, clinical note, triage outcome or patient communication unless the Practitioner has reviewed it, corrected it where necessary, and is satisfied that it is clinically appropriate, truthful and lawful.

A Practitioner may decide that an in-person assessment, specialist referral, emergency escalation, physical examination, diagnostic test or different care pathway is required. These decisions must be based on professional judgement and the Patient's best interests, not on platform convenience or commercial pressure.

11A. Occupational health, employer access and workplace information

PonyaData may support occupational-health, medical-surveillance, employee-assistance, workplace-fitness, injury-on-duty, insurer, sponsor or employer-funded workflows only through a separately configured and access-controlled occupational-health regime. An employer, bureau, administrator, sponsor, insurer or funder is not a Practice or Practitioner merely because it requests, pays for or receives an occupational-health output.

Occupational Health Clients may receive only the minimum lawful output required for the occupational purpose, such as fitness-for-work status, functional restrictions, accommodation recommendations, statutory surveillance certificates, attendance confirmation, billing information or other outcome-level information permitted by law.

They must not receive diagnoses, clinical notes, laboratory results, imaging, prescriptions, Global Health Record content, mental-health details, sexual-health information, HIV information or other clinical content unless the disclosure is specifically authorised by law, court order, valid informed consent, or another lawful basis and professional duty permits it.

An Occupational Health Practitioner or Practice must act as the clinical gatekeeper for occupational-health records and employer-facing outputs. Medical testing, medical surveillance, fitness assessments and disclosure of employee health information must comply with the Employment Equity Act restrictions on medical testing, the National Health Act confidentiality regime, POPIA, occupational health and safety laws, professional rules and any sector-specific rules such as mine health and safety rules where applicable.

Occupational-health and medical-surveillance records must be retained according to the governing occupational-health, occupational-safety, mine-health, hazardous-chemical, asbestos, lead, biological-exposure, noise, radiation, facility, professional or sector-specific rule. Where a specific regulation requires long-term retention, the applicable rule controls; medical-surveillance records may require 20 to 40 years or another prescribed period depending on the exposure and regulation. Any shorter platform default is overridden by the governing regulation and POPIA section 14 purpose limitation.

The platform must maintain occupational-health records in a walled workflow with role-based access, purpose limitation, separate notices/consents where required, audit trails, retention controls and employer-output controls. Employer dashboards must not provide direct access to clinical records unless a specific lawful disclosure route has been configured and documented.

12. Digital health consent and telehealth

PonyaData supports both in-person digital health workflows and telehealth. The Company must not present telehealth as the whole of the service where PonyaData is being used at physical touchpoints of care. Digital health consent should cover electronic records, secure messaging, AI-assisted drafts with human review, data sharing for care, billing support and patient-held record features. Telehealth-specific consent is required where care is provided at a distance.

Before a telehealth consultation, the Practitioner or platform workflow must, where clinically and ethically required, verify the Patient's identity and location, verify or disclose the Practitioner's identity and registration details, confirm the reason for the consultation, assess whether telehealth is suitable, explain material limitations and risks, and obtain documented informed consent in writing or in a recorded electronic format.

Telehealth risks include incomplete examination, technology failure, privacy risk, data transmission error, poor audio or video, misunderstanding, delayed response, inaccurate patient-supplied information, and the need to convert to in-person care. Patients must be told how to obtain urgent or in-person care where needed.

A Practitioner must not prescribe, certify, diagnose or treat solely on the basis of an online questionnaire where professional judgement, adequate history, a documented clinical evaluation, a physical examination or additional assessment is required. Prescription-support functions are safety tools only; final prescribing responsibility remains with the authorised prescriber.

Telehealth consents, recordings where lawful, messages, images, prescriptions, referrals, clinical notes, consent logs and instructions may form part of the health record.

Practitioners who provide telehealth or digital clinical services to a Patient located in South Africa must hold the South African professional registration, statutory authority and scope of practice required for that service, including HPCSA registration where applicable. A foreign clinician treating a Patient who is physically outside South Africa is a separate clinical relationship governed by the law and professional rules applicable to that treatment; any PonyaData Global Health Record disclosure to that clinician must be treated as Patient-directed sharing under clauses 14 and 18 unless the Company separately controls the transfer.

13. AI-assisted healthcare, human oversight and automated decisions

PonyaData may use AI Functions to assist with transcription, translation support, note drafting, summarisation, symptom capture, risk flagging, triage support, reminders, care-gap identification, medication and allergy alerts, clinical decision support, document analysis, patient education, quality monitoring, cybersecurity, fraud prevention and administrative routing.

AI Functions are assistive tools. They may be wrong, incomplete, biased, outdated, unsuitable for a particular Patient, affected by poor data quality, or used outside their intended purpose. AI output is not a final clinical record, diagnosis, treatment plan, prescription, referral, discharge decision, denial-of-care decision, claim submission or patient instruction unless reviewed and approved by an authorised human.

No AI Function output shall be adopted into a clinical record unless reviewed, edited where necessary, and approved by a registered Practitioner or other authorised human user acting within lawful scope. To the extent permitted by law, the Company disclaims liability as against Business Users for unreviewed AI outputs that are used contrary to these Terms, intended-use instructions, warnings or professional obligations. This does not exclude or limit liability to Patients or Consumers for the Company's own defective software, defective medication-interaction or safety engine, negligent design, inadequate warnings or instructions, security failures, regulated-device obligations, POPIA duties, CPA duties, or any other liability that cannot lawfully be excluded.

A Patient must not be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significant effects, unless permitted by POPIA and accompanied by appropriate safeguards, including meaningful human intervention, an opportunity to make representations, and information about the logic involved where legally required.

The Company must maintain an AI Function Register for material AI Functions. For clinical, patient-facing or rights-affecting AI Functions, the Company must maintain model-card or equivalent documentation covering intended use, data inputs, outputs, model or rule version, validation, known limitations, human oversight, confidence or uncertainty communication, local population considerations, bias assessment, cybersecurity, SAHPRA status, change control and post-deployment monitoring.

Patients and Practitioners must be informed when AI materially assists a clinical or access-affecting workflow. The explanation may be provided through an AI notice, patient-facing model-card summary, consent screen, clinical note, practitioner disclosure or support channel depending on the risk and context.

14. Patient-held and shared Global Health Record

PonyaData may allow a Patient to maintain, access, download and share a longitudinal Global Health Record with authorised care providers. This function is intended to improve continuity of care, especially where a Patient moves to a new care giver, attends an emergency unit, receives multidisciplinary care, or travels.

Access to a Global Health Record must be role based, purpose limited, auditable and revocable where legally possible. The Patient may authorise access for selected Practitioners, caregivers or facilities. A Practice or Practitioner may access only the information needed for a lawful clinical, administrative, billing, safety or legal purpose.

Where a Patient personally initiates or directs sharing of their Global Health Record with an overseas Practitioner, emergency unit, caregiver or other recipient, the workflow must record the Patient direction, recipient, scope, purpose, duration, warnings about foreign legal protections and any revocation. Patient-initiated sharing is distinct from a Company-controlled transfer for the Company's own support, vendor, research, analytics, AI validation or product-governance purposes. Where the Company controls the purpose or recipient of an identifiable Health Information transfer outside South Africa, clause 18 applies, including POPIA section 72 safeguards and, where applicable, section 57 prior authorisation before transfer to a non-adequate jurisdiction.

Foreign Practitioner access through the Global Health Record is not a shortcut around South African professional-registration rules. If a Practitioner is treating, advising, prescribing for or otherwise providing Clinical Services to a Patient located in South Africa, the Practitioner must have the South African registration or lawful authority required for that service. If the Patient is travelling or resident outside South Africa and chooses to share

records with an overseas treating clinician, that sharing is Patient-directed disclosure; the overseas clinician is responsible for complying with the law and professional duties of the place where the service is provided.

Imported records, patient-entered information and third-party information should be treated as potentially incomplete until reviewed by a Practitioner. Users must not alter, delete or suppress clinically material information in a way that could mislead care providers or endanger the Patient.

14A. Children, mature minors and representative access

Children's Personal Information and paediatric Health Information receive additional protection. PonyaData must process a child's Personal Information only where POPIA section 34 and section 35, the Children's Act, health-specific statutes, clinical ethics and the applicable section 27 or section 32 special-information authorisation allow the processing.

Where a parent, guardian, caregiver, curator or other representative acts for a child, the Company, Practice or Practitioner must verify the representative's identity and authority before Representative Access is granted. Verification must be proportionate to the risk and may include identity proof, relationship or guardianship proof, facility records, court orders, consent records, or other lawful evidence. Representative Access must be role based, purpose limited, logged and reviewable.

Representative Access does not give a parent, guardian or caregiver automatic access to every record about a child. PonyaData must support segmentation, masking or restriction of Restricted Confidential Entries where a child has an independent confidentiality right or where disclosure would be unlawful, unsafe, contrary to the child's best interests, or inconsistent with a Practitioner's professional duties.

A Mature Minor pathway must be available where Applicable Laws allow the child to consent independently to medical treatment or a confidentiality-sensitive health service. This includes, where the legal requirements are met, medical treatment for a child aged 12 or older with sufficient maturity and mental capacity, and specific statutory confidentiality contexts such as termination of pregnancy, HIV testing, contraception, sexual-health care, mental-health care, abuse or violence-related care. The Practitioner must document the maturity/capacity assessment and any confidentiality limits that apply.

For a patient-held or shared Global Health Record, guardian or caregiver access must be configured so that Restricted Confidential Entries are excluded, masked or separately permissioned unless disclosure is legally required, authorised by the Patient where legally competent, authorised by a court or law, or clinically justified under an applicable statutory exception. Emergency access to Restricted Confidential Entries is governed by clause 20 and Schedule 5.

Before a Patient reaches majority, the Company and relevant Practice must provide a transition-of-control process so that the Patient's account, consents, sharing permissions and Representative Access can be reviewed and, where appropriate, transferred to the Patient at 18 years of age. The transition must preserve lawful clinical records, audit trails, legal holds and any continuing statutory confidentiality limits.

Where there is conflict between a representative's request and a child's legally recognised confidentiality or best interests, the Practice or Practitioner responsible for care must make or confirm the clinical/legal decision, and the Company must enforce the access decision as Operator or platform Responsible Party according to clause 17 and Schedule 1.

15. Personal information, Health Information and lawful-basis architecture

The Company, Practices and Practitioners will process personal information and Health Information in accordance with POPIA, the National Health Act, professional confidentiality duties, applicable health-information regulations and Schedule 1. The binding role allocation in clause 17 and Schedule 1 identifies the Responsible Party and

Operator for current service and data flows; a materially new processing flow involving identifiable Health Information is not covered unless a service-specific addendum identifies the Responsible Party, Operator, section 11 basis, special-information authorisation, retention rule, cross-border position and patient-facing notice before that processing begins.

POPIA requires a layered analysis. For all personal information, the relevant Responsible Party must satisfy the general conditions for lawful processing, including a justification under section 11. Health Information is special personal information: for identifiable Health Information, a section 11 justification is necessary but is not sufficient. The processing must also be authorised under the special-personal-information regime, including section 27 and, where applicable, section 32 for health or sex-life information.

Contract performance, the Responsible Party's legitimate interests, service efficiency, product improvement or clinical-safety interests may support ordinary personal information processing where section 11 allows it, but none of those grounds is a standalone gateway for identifiable Health Information. Identifiable Health Information may be processed only where a section 27 authorisation, section 32 authorisation, specific consent, legal obligation, legal-claims basis, applicable research authorisation with safeguards, Regulator authorisation or another applicable statutory basis permits it.

Where the Company acts as an Operator for a Practice, Practitioner or health establishment, the Company processes Health Information only on that Responsible Party's documented instructions and under appropriate confidentiality, security and operator controls. Where the Company determines its own purposes for identifiable Health Information, including analytics, AI governance, product improvement, model validation, support review, safety monitoring or commercialisation, it must document the applicable section 11 basis and the separate section 27 or section 32 authorisation. If no such special-information authorisation applies, the Company must use genuinely de-identified information or obtain appropriate specific consent before processing identifiable Health Information for that purpose.

Where consent is relied on, the Patient or competent person may withdraw consent prospectively, subject to lawful retention, clinical record duties, completed processing, medical-device safety duties, legal claims, public-interest duties, research ethics requirements and other Applicable Laws. Data subject rights include rights to request access, correction or deletion where legally available, object to certain processing, withdraw consent where consent is relied on, request human review of applicable automated decisions, complain to the Information Officer, and complain to the Information Regulator.

16. Confidentiality, health records and data integrity

Patient confidentiality is a core condition of PonyaData. Health Information, health status, treatment information, consultation information and clinical records must be kept confidential. Disclosure without the Patient's written consent is limited to disclosures required by a court order or law, disclosures where non-disclosure represents a serious threat to public health, and access or disclosure by a health worker or health care provider where authorised by the National Health Act, necessary for a legitimate purpose in the ordinary course and scope of duties, and in the Patient's interests. More restrictive rules for children, Mature Minors and Restricted Confidential Entries prevail where applicable.

Mental-health status, mental healthcare information and records relating to care, treatment or rehabilitation under the Mental Health Care Act must be handled under the National Health Act, POPIA, professional confidentiality rules and the Mental Health Care Act confidentiality regime. Access to mental-health records must be need-to-know, role based and clinically justified, and disclosure to representatives, employers, funders or other third parties must be restricted where law, professional duties, Mature Minor confidentiality, safety or the Patient's rights require restriction.

The platform must maintain appropriate electronic records and audit trails. Records should preserve who created, viewed, changed, approved, signed, exported or disclosed material information, when this occurred, and the reason where required.

Drafts, AI outputs, templates and imported data become part of the clinical record only when saved, approved, signed, incorporated or otherwise treated as part of the Patient's record by an authorised human user or applicable workflow. The system should distinguish drafts from final or approved clinical content.

Patients may request access to their records through the process described in Schedule 1. Access may be subject to identity verification, lawful limitations, third-party privacy, clinical safety, record-keeping duties, legal holds and PAIA or POPIA procedures.

Health records must be retained according to Schedule 8 and POPIA section 14. PonyaData does not adopt an indefinite-preferred retention model. Each Responsible Party must retain Personal Information and Health Information only for the longer of the applicable statutory or professional minimum, a contractually required period, a Patient- or Competent-Person-consented period, or a documented purpose-justified period approved through clinical governance and lawful under POPIA section 14. When retention is no longer authorised, the Responsible Party must ensure secure deletion, destruction or genuine de-identification, and the Company must execute those instructions where it acts as Operator.

Where a Patient elects to maintain a patient-held or shared Global Health Record after the ordinary clinical or statutory retention period, the continued retention of that Patient-held copy must be framed and recorded as Patient-consented retention of the Patient's own record, subject to POPIA, section 14 limits, withdrawal mechanics, clinical-record duties, legal holds, safety requirements and the children/majority-transition controls in clause 14A.

16A Each Business User must keep confidential and not disclose to any third party any non-public information concerning Ponyadata's software, systems, platform architecture, proprietary methodologies, AI configurations, pricing structures, internal processes, tools, templates, trade secrets and business information disclosed in connection with the use of Ponyadata ('Platform Confidential Information'). This obligation survives termination for a period of 5 years.

16B Nothing in these Terms prevents Ponyadata or its personnel from using general knowledge, skills and experience (including ideas, concepts, know how and techniques) retained in the unaided memories of its personnel, provided this does not include the reproduction of identifiable personal information, Health Information, or verbatim Patient records.

17. Responsible Party and Operator roles

This clause is the binding Responsible Party / Operator allocation clause for current PonyaData services. It is not a placeholder and does not defer accountability. A service-specific addendum may alter an allocation only if it expressly identifies the affected data flow, the changed role, the POPIA basis, the special-information authorisation for Health Information, the responsible Information Officer contact, and the patient-facing notice that applies before the new processing starts.

The Responsible Party identified for a data flow is accountable for POPIA openness notices under section 18, data-subject request handling, retention decisions, cross-border-transfer decisions under section 72, and security-compromise notification under section 22 for that flow. Where the Company is Operator, it must process only on documented instructions and must assist the Responsible Party with these duties.

Current service / data flow	Binding role allocation and accountability
Platform account data, authentication, access controls and platform security metadata	Company is Responsible Party. Identity-verification, hosting, cybersecurity and communications vendors are Operators for the Company. The Company handles POPIA notices, access/correction requests, retention, section 72 transfers and section 22 notifications for this flow.
Practice onboarding, authorised users, permissions and role administration	Practice is Responsible Party for deciding who its authorised users are and what roles they receive. Company is Responsible Party for platform credential controls and account-security infrastructure.

	Company is Operator when enforcing Practice instructions about users, roles and access levels.
Clinical records, consultations, prescriptions, referrals, results, notes, discharge summaries, sick notes and patient letters	Practice, Practitioner or health establishment is Responsible Party for clinical care and clinical records. Company is Operator when it hosts, routes, structures, stores, backs up, displays, summarises or assists with those records for care on documented instructions.
Scheduling, reminders, queues, telehealth logistics and secure messaging	Company is Responsible Party for platform logistics, appointment workflows, reminders and service-delivery metadata. Practice or Practitioner is Responsible Party for clinical consultation content and care communications. Company is Operator for clinical content carried through messaging or telehealth workflows.
Patient-held or shared Global Health Record and patient-directed sharing	Company is Responsible Party for sharing permissions, consent/revocation records, Representative Access configuration, segmentation/masking controls, access controls and audit logs. Originating Practice/Practitioner remains Responsible Party for records it created. Receiving care providers are Responsible Parties for their own care use after Patient-authorised or lawful disclosure. Patient-directed international sharing is distinct from Company-controlled overseas transfers. Company is Operator for hosting and transmitting clinical records and for enforcing documented clinical/legal masking instructions.
Break Glass emergency access	Company is Responsible Party for Break Glass access-control design, event logs, patient-notification workflow, Information Officer review and security assessment. Emergency Practitioner, emergency unit or health establishment is Responsible Party for the clinical decision to use the information for emergency care or serious threat to the Patient's life or health. Company is Operator for disclosure of underlying clinical records held for an originating care provider, except for Company-controlled access logs and security metadata.
AI-assisted clinical workflow, documentation, safety alerts and triage support	Practice/Practitioner is Responsible Party for clinical use, human review, adoption into clinical records and clinical decisions. Company is Operator when running AI Functions for care or documentation on instructions. Company is Responsible Party for AI Function Register, model-card records, platform safety monitoring and compliance records that it determines for its own governance.
De-identified or aggregated analytics	Company is Responsible Party for the de-identification process, aggregate analytics it determines, re-identification risk controls and prohibitions on re-identification. Information that is genuinely de-identified and not reasonably re-identifiable falls outside POPIA, but the Company remains contractually accountable for maintaining the safeguards.
Identifiable analytics, AI validation, product improvement, research, publication or external collaboration	Company is Responsible Party only where it determines the purpose and has a documented POPIA section 11 basis plus a section 27 or section 32 special-information authorisation, specific consent, Regulator authorisation, legal obligation or ethics-approved waiver. Otherwise the Company must use genuinely de-identified information or act only as Operator under documented instructions.
Billing, claims, medical-aid motivations, funder communications and payments	Practice/Practitioner is Responsible Party for clinical billing, coding, motivations and claims content. Medical scheme, insurer or funder is Responsible Party for benefits administration after receipt. Company is Responsible Party for PonyaData invoices, subscriptions and payment account data. Company is Operator when routing Practice claims or funder communications on instructions.
Support, maintenance, data migration, troubleshooting and incident support	Company is Responsible Party for support account data, ticket administration, platform diagnostics and its own security/compliance logs. Company is Operator for clinical or Health Information accessed to support, migrate, repair or

	troubleshoot a Practice/Practitioner workflow on documented instructions.
Cross-border access, third-party processors, integrations and security tools	The Responsible Party for the source data flow is accountable for approving and documenting any POPIA section 72 transfer and any POPIA section 57 prior-authorisation trigger. Company is Responsible Party for transfers of Company-controlled account, billing, security or governance data. Company is Operator for transfers of Practice-controlled clinical records and must not cause the transfer unless instructed or legally required. Company-controlled transfer of identifiable Health Information or children's Personal Information to a non-adequate jurisdiction requires section 57 prior authorisation or restructuring. Foreign practitioner access for treating a Patient located in South Africa requires the relevant South African registration or lawful authority; overseas treatment of a Patient outside South Africa through Patient-directed sharing is treated as Patient-directed disclosure, not Company-authorised South African telehealth.
Security compromises, breach notifications and data-subject requests	The Responsible Party for the affected data flow has primary POPIA section 22 notification and data-subject-rights accountability. Company is the primary notifier where Company is the Responsible Party. Where the Company is the Operator, it must promptly notify and assist the relevant Responsible Party. For mixed incidents, the Company will coordinate investigation and notices without obscuring the allocation of accountability.
Children, Mature Minors, Restricted Confidential Entries and Representative Access	Practice/Practitioner or health establishment is the Responsible Party for clinical decisions about a child's capacity, consent, confidentiality, Restricted Confidential Entries and disclosure to representatives. Company is Responsible Party for platform account permissions, Representative Access tooling, masking/segmentation controls and audit logs. Company is Operator when enforcing a Practice/Practitioner instruction about child-record access, masking, transition to majority, or disclosure.
Occupational health workflows, medical surveillance, fitness-for-work and employer outputs	Occupational Health Practitioner/Practice is the Responsible Party for occupational-health clinical records, medical surveillance, fitness assessments and clinical disclosure decisions. Occupational Health Client/employer is a Responsible Party only for its own employment-administration data and lawful outcome-level information it receives. Company is Operator for occupational-health clinical records hosted or routed on instructions and Responsible Party for its own account, access-control, audit and support records. Employer access must be walled and normally limited to fitness/outcome-level information.
Service Messages, communication preferences and Direct Marketing	Company is Responsible Party for Company Service Messages, marketing consents, opt-outs, suppression lists and Company Direct Marketing. Practice/Practitioner is a Responsible Party for Practice-originated care or administrative messages. The company is an operator where it sends Practice messages on instructions. Identifiable Health Information must not be used for Direct Marketing unless a specific lawful consent/special-information authorisation permits it.

Practice agreements, practitioner terms, operator agreements, data-processing agreements, data-sharing agreements, hosting agreements and service-specific schedules must incorporate this matrix or a materially identical version. In the event of conflict, the more specific written agreement controls only for the identified flow and only if it preserves POPIA-compliant accountability, patient notice, security, breach reporting, retention, cross-border and data-subject-rights obligations.

18. Cross-border transfers and South Africa based processing

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, 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.

19. Cybersecurity, security safeguards and breach response

The Company will implement reasonable and appropriate technical and organisational measures to protect personal information and Health Information. Minimum safeguards are set out in Schedule 7 and include encryption in transit, encryption at rest where appropriate, role-based access, least privilege, multifactor authentication for privileged or high-risk access, audit trails, secure development, change control, backups, vulnerability management, logging, monitoring, incident response, supplier due diligence and workforce confidentiality training.

Users must not share credentials, bypass security controls, access records without authority, export data unlawfully, upload malware, scrape the platform, attempt to reverse engineer protected features, misuse APIs, or use another person's account without authorisation.

Suspected unauthorised access, loss, compromise, incorrect record linkage, misdirected communication, data corruption, ransomware, security weakness, suspected AI safety issue, device issue or clinical safety incident must be reported promptly through the contact routes in clause 32.

Where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, the Responsible Party identified in clause 17 and Schedule 1 for the affected data flow has the primary POPIA section 22 notification duty. The Company is the primary section 22 notifier for Company-Responsible-Party flows, including platform accounts, platform security logs, billing account data, support-ticket administration and Company-controlled AI governance records. Where the Company is Operator for Practice- or Practitioner-controlled clinical records, it must escalate to the relevant Responsible Party, the Information Officer or delegated privacy lead, and the security lead within 24 hours of discovery or reasonable suspicion, assist with containment and investigation, and support notifications to the Information Regulator and affected data subjects. Where a mixed incident affects multiple flows, the Company will coordinate a single incident process and clear responsibility map, while preserving each Responsible Party's statutory accountability.

Security-compromise notification must run from awareness or reasonable grounds to believe that a compromise may have occurred, not from final confirmation. Notification must not be delayed merely because an investigation is incomplete, unless a permitted law-enforcement, safety, legal or regulator reason justifies delay. The Company internal target is to notify the Information Regulator and affected data subjects as soon as reasonably possible and, where legally notifiable and reasonably feasible, within 72 hours after the Responsible Party or Company becomes aware of, or has reasonable grounds to believe, a notifiable compromise may have occurred, with follow-up notices as facts develop. The Company must preserve evidence, contain harm, keep incident records, cooperate with affected Responsible Parties and Operators, and implement remediation.

20. Break Glass emergency access

Break Glass access may be used only where ordinary access is unavailable or insufficient and access is reasonably necessary for one of the following limited purposes: emergency care or a serious threat to the Patient's life or health; disclosure or access required by law or court order; or security-incident containment, investigation and remediation limited to metadata, access logs or technical security data unless access to clinical content is itself legally justified.

Break Glass must not be used for ordinary support, product improvement, billing disputes, convenience, routine quality review, non-urgent investigations, commercial analysis, AI training, curiosity, or any open-ended exceptional purpose approved only by the Company. If the purpose can be handled through ordinary role-based access, consent, a Practitioner instruction, a court order, a regulator process or a data-subject request, Break Glass must not be used.

Break Glass access must be time limited, role based, justified, logged and reviewed. The access log should record the user, identity, role, organisation, Patient, date, time, information accessed, reason, session duration, actions taken, and any disclosure or export.

Where Break Glass access occurs, the Patient will be notified as soon as reasonably practicable unless notification would prejudice the Patient's safety, emergency care, a lawful investigation, legal duties, the rights or safety of another person, or a regulator or law-enforcement process. All Break Glass events will be logged and reviewed by the Information Officer or delegated privacy officer and, where clinically relevant, by the Clinical Governance Lead. A Restricted Confidential Entry may be included in Break Glass access only where the same limited purpose and legal justification apply to that entry.

Break Glass access is not automatically a security compromise. However, if the access was unauthorised, excessive, fraudulent, negligent, compromised, or involved personal information accessed or acquired by an unauthorised person, the incident must be assessed under POPIA section 22 and Schedule 7.

21. Research, analytics, quality improvement and AI development

The Company may use de-identified or aggregated information for service performance, quality improvement, patient safety, operational analytics, product improvement, bias monitoring, cybersecurity, fraud prevention,

reporting and AI performance monitoring, provided the information is handled lawfully and cannot reasonably identify a Patient.

Ordinary clinical care data must not be repurposed for identifiable research, publication, external validation, AI training, AI fine-tuning, commercialisation, or sharing with research collaborators unless there is a lawful basis, transparency, proportionality, POPIA compliance, required consent or waiver, research ethics approval where required, and appropriate contractual safeguards.

Patients must provide specific consent for research beyond ordinary care unless a competent Research Ethics Committee grants a lawful waiver or another legal basis applies. Refusing research participation must not prejudice ordinary care, unless the relevant service is clearly a research-only service and this is disclosed before participation.

Research involving human participants, identifiable Health Information, sensitive data, human biological material, clinical data sets, AI in a clinical setting, or risk to participants must be reviewed and approved by a competent REC, HREC, IRB or equivalent ethics committee where required before the research begins.

Research collaborations and secondary-use projects must use appropriate Data Transfer Agreements, Data Sharing Agreements, Data Processing Agreements or Material Transfer Agreements where data or human biological material is shared. These agreements must address purpose limitation, security, retention, destruction, publication, intellectual property, benefit sharing, onward transfer, cross-border safeguards, breach notification and POPIA compliance.

22. SAHPRA-regulated medical devices, AI safety and post-market controls

Pending completion of any applicable SAHPRA classification assessment, the Company does not represent that any AI Function or software component constitutes a registered or authorised medical device. No Practitioner or User should rely on any function for a regulated medical-device purpose until the Company has confirmed in writing that the relevant classification, authorisation and labelling requirements have been met.

23. Prescriptions, certificates, referrals, discharge letters and funder motivations

PonyaData may assist in generating or routing prescriptions, medication-safety checks, sick notes, certificates, referral letters, discharge summaries, patient information letters, imaging requests, laboratory requests, medical-aid motivations, funder communications and similar documents.

All such outputs are drafts or workflow aids until reviewed and approved by an authorised Practitioner or authorised Practice user. The responsible Practitioner must verify the clinical basis, accuracy, lawfulness, completeness and professional appropriateness of the output before signature, submission, issue or reliance.

A Practitioner may issue a prescription, sick note, certificate, referral, discharge letter or motivation only where there is an adequate clinical basis and the Practitioner complies with professional rules, scope of practice, medicine-control rules, ethical billing rules and applicable funder requirements. PonyaData must not be used to fabricate clinical facts, exaggerate medical need, manipulate codes, hide contraindications, or bypass professional judgement.

Where a prescription, scheduled-medicine order, sick note, medical certificate, referral, discharge document, funder motivation or other regulated document requires a signature, PonyaData must enforce a compliant signature workflow before issue, transmission, submission or release. The document must be executed with an advanced electronic signature where ECTA requires one, or with another signature method that is lawful for the document type under the Medicines and Related Substances Act regulations, ECTA, the Basic Conditions of Employment Act, professional rules and any applicable regulator or funder requirements. The workflow should log the signer identity, professional role, registration where applicable, signature method, date and time, document version, document hash or equivalent integrity control, recipient and transmission channel. A pasted image of a signature is not sufficient unless it forms part of a legally compliant signature process.

24. Fees, billing, medical aids, refunds and cooling-off rights

Fees, taxes, payment methods, cancellation charges, refund rules, subscription terms, claim-support terms and included services will be displayed before purchase, subscription or booking where applicable. A fee schedule or service-specific schedule forms part of these Terms.

The Company does not guarantee that a medical aid, insurer, employer, sponsor, public programme or funder will pay for a service, reimburse a Patient, approve a claim, accept a code, authorise treatment, or accept a motivation. Unless expressly stated otherwise, the Patient or Practice is responsible for fees not paid by a third party.

For a qualifying online consumer transaction for PonyaData services where the Electronic Communications and Transactions Act applies and no statutory exclusion applies, the Consumer may cancel without reason and without penalty within seven days after conclusion of the services agreement, subject to any lawful charge for services already begun with the Consumer's express consent before the end of the cooling-off period. This right does not automatically apply to excluded transactions, business-to-business services, custom or once-off professional services, or healthcare/professional services already fully or partly performed with the Consumer's consent where the law permits exclusion or proportionate charging.

Where an agreement results from direct marketing and the Consumer Protection Act applies, the Consumer may cancel within the statutory five-business-day direct-marketing cooling-off period by sending a written or recorded cancellation through the app, portal, email or physical notice address in clause 32, identifying the User, service, order and contact details. Refunds, deductions and timing will be handled as required by ECTA, the CPA and the service-specific schedule.

24A. Service messages and direct marketing communications

PonyaData may send Service Messages needed for care, appointments, reminders, account administration, billing, security, legal notices, data-subject requests, patient safety, system maintenance, Break Glass notifications or a service requested by the User. Service Messages are not Direct Marketing and may continue even if a User opts out of marketing, to the extent necessary for the service, safety, legal compliance or clinical continuity.

Direct Marketing is separate from Service Messages. The Company must not send electronic Direct Marketing to a Patient or Consumer unless POPIA section 69, the CPA and any other Applicable Laws permit it. As a baseline, Direct Marketing to new Users requires opt-in consent, and every marketing message must identify the sender and provide a simple, free or low-cost opt-out or unsubscribe mechanism. Existing-customer marketing may be used only where the law permits it, for similar products or services, after the User was given a reasonable opportunity to object at collection and in each subsequent message.

Identifiable Health Information, children's information, Restricted Confidential Entries, mental-health information, sexual-health information, HIV information, reproductive-health information or occupational-health information must not be used for Direct Marketing unless a specific, informed, voluntary and recorded consent permits that precise use and no professional, statutory or ethical rule prohibits it. Refusal or withdrawal of marketing consent must not prejudice access to ordinary care or core platform services.

Users may change marketing preferences, withdraw consent or opt out through the app, portal, unsubscribe link, support channel or Information Officer contact. The Company must keep an auditable record of marketing consents, opt-outs, suppression lists and campaign purposes, and must distinguish Company marketing from Practice communications sent by the Company as Operator on documented instructions.

25. Support, service availability, continuity and data export

The Company will use reasonable efforts to keep PonyaData available and secure, but does not guarantee uninterrupted availability, error-free operation, immediate response, or compatibility with every device, browser, network, operating system, third-party system or electricity supply.

The platform may be unavailable due to maintenance, upgrades, cybersecurity controls, network failure, electricity outage, supplier failure, force majeure, regulatory action, patient-safety concerns, device-safety concerns, or events beyond reasonable control. Where downtime may affect patient safety, clinical continuity or access to records, the Company should use reasonable efforts to provide appropriate notices, workarounds or escalation routes.

Upon termination, expiry or lawful request, the Company should provide export of relevant Practice or Patient data in a reasonably usable electronic format within a reasonable period, subject to identity verification, outstanding lawful fees for export services, retention duties, legal holds, third-party rights, clinical safety, security and Applicable Laws. Patient access to health records must not be denied unlawfully merely because a commercial account is in dispute.

Data deletion, destruction or de-identification after termination must comply with Schedule 8 and must not compromise legal record-keeping, clinical continuity, patient safety, research ethics obligations, medical-device obligations or legal holds.

26. Accounts, acceptable use and user content

Users must use PonyaData lawfully, professionally, respectfully and only for authorised healthcare-related purposes. Users must not upload false, malicious, unlawfully obtained, defamatory, discriminatory, abusive, exploitative, violent or irrelevant content, and must not upload another person's information without authority.

Users must not interfere with security, use malware, scrape data, attempt unauthorised access, reverse engineer protected features, benchmark publicly without written approval, train competing systems on protected outputs, misuse patient information, harass staff or Practitioners, impersonate another person, or use PonyaData in a way that endangers a Patient.

The User grants the Company and relevant Practitioners the rights needed to host, copy, transmit, process, display, store, analyse, route and use User content for the purposes permitted by these Terms, the Privacy Notice and Applicable Laws. This does not transfer ownership of personal information or clinical records to the Company.

27. Intellectual property and platform licence

PonyaData, including its software, user interface, workflow, documentation, non-patient content, branding, templates, model cards, AI configurations, analytics, reports, designs, databases and intellectual property, is owned by the Company or its licensors except where otherwise stated.

Subject to these Terms and payment of applicable fees, the Company grants each authorised User a limited, revocable, non-exclusive, non-transferable licence to use PonyaData for the intended healthcare-related purpose and within the assigned role permissions.

No User may copy, adapt, reverse engineer, disassemble, attempt to extract source code or model weights, bypass controls, scrape, resell, white-label, benchmark publicly, train competing models on protected outputs, or use PonyaData to build a competing service, except as permitted by law or a written agreement.

Nothing in this clause prevents a Patient from exercising legal rights to access personal information or health records, or a Practitioner from fulfilling lawful clinical, ethical or record-keeping duties.

28. Suspension and termination

A User may stop using PonyaData at any time, subject to outstanding fees, record-retention duties, clinical continuity, research consents, device obligations, legal holds and Applicable Laws.

The Company may suspend or terminate access where reasonably necessary for safety, security, non-payment, suspected fraud, unauthorised access, breach of these Terms, misuse, legal compliance, regulator instruction, protection of Patients, protection of Practitioners, or protection of systems.

Suspension or termination must be handled in a way that respects clinical continuity, patient safety, emergency access and lawful health-record access. Where appropriate and lawful, the Company or Practice should provide reasonable handover information or instructions for continued care.

Clauses dealing with confidentiality, privacy, records, fees, intellectual property, limitation of liability, disputes, governing law, audit logs, research governance and accrued rights survive termination.

29. Warranties, disclaimers, liability and indemnity

PonyaData will be provided with reasonable care and skill. Digital healthcare depends on accurate information, suitable technology, appropriate clinical judgement, secure networks, patient follow-through, user training, compliant electronic signatures and external providers. The Company cannot guarantee a particular clinical outcome, diagnosis, prescription, referral, test result, recovery, claim outcome, medical-aid approval, user satisfaction or Practitioner availability.

PROMINENT CONSUMER NOTICE: Certain clauses in these Terms explain ordinary digital-health, telehealth, AI, emergency, third-party, account-security and data-sharing risks, and may limit or allocate risk where the law allows. Where the Consumer Protection Act or another law requires a risk-limiting, liability-limiting, indemnity, assumption-of-risk or unusual-risk term to be drawn to a Consumer's attention, the Company must present the term in plain language, conspicuously, before or at the time of acceptance, and obtain any required acknowledgement, click-through, initials or consent. A risk-limiting term will not be enforced against a Consumer to the extent that it was not presented or agreed in the manner required by law or is unfair, unreasonable, unjust or prohibited.

Nothing in these Terms excludes or limits liability for fraud, wilful misconduct, gross negligence, unlawful processing of personal information, death or personal injury caused by negligence where such liability cannot be excluded, breach of non-excludable statutory rights, professional duties that cannot be limited, liability under the Consumer Protection Act that cannot be limited, or any liability that cannot legally be excluded or limited.

The Patient and Consumer indemnity is limited. A Patient or Consumer is not required to indemnify the Company, Practitioners or service providers merely for ordinary use of PonyaData, ordinary clinical outcomes, exercising data-subject rights, lodging complaints, or receiving defective goods or services. A Patient or Consumer may remain responsible for their own fraud, intentional unlawful conduct, impersonation, deliberate unauthorised disclosure of another person's information, intentional security breach or other liability that Applicable Laws permit.

The indemnity in favour of the Company applies only to Business Users. A Business User must indemnify the Company, its directors, employees, Operators and service providers against third-party claims, losses and reasonable costs arising from that Business User's unlawful use, breach of these Terms or a service agreement, unauthorised disclosure of another person's information, unlawful employer access, unlawful occupational-health disclosure, impersonation, fraud, abuse, intentional security breach, misuse of AI outputs, unlawful clinical practice, unlawful billing, fee-splitting, perverse incentives or use outside documented instructions, except to the extent caused by the indemnified party's own unlawful conduct, negligence, defective product, breach of duty or non-excludable statutory liability.

The Company acknowledges that the Consumer Protection Act may impose strict liability for harm caused by unsafe goods, product failure, product defect or inadequate instructions or warnings where that Act applies, and that such liability cannot be contracted out of against Consumers where the Act prohibits exclusion. If any PonyaData software, AI Function, medication-interaction engine, device integration or regulated device component causes harm because of the Company's own defect, unsafe feature, negligent design, inadequate warnings or failure to comply with Applicable Laws, these Terms do not deprive a Patient or Consumer of mandatory remedies. The Company will use commercially reasonable steps to maintain appropriate cyber, professional, technology errors-and-omissions and product-liability insurance proportionate to PonyaData's risk profile. The Company shall maintain cyber-risk, technology errors-and-omissions, and public-liability insurance with aggregate limits of not less than R2 000 000 per claim and in the aggregate, or such higher amount as is proportionate to the risk profile of the services offered.

For Business User claims only, and subject to the exclusions below, the Company's aggregate monetary liability arising from or relating to PonyaData in any 12-month period is capped at the greater of: (a) ten times the fees

actually paid or payable by that Business User to the Company for PonyaData services during the 12 months immediately preceding the first event giving rise to the claim; or (b) ZAR 5 000 000. Where the Business User has used PonyaData for less than 12 months, the cap is calculated on the annualised fees payable under the relevant subscription or service agreement. This cap does not apply to fraud, wilful misconduct, gross negligence, death or personal injury caused by negligence where not legally limitable, confidentiality breaches that cannot lawfully be limited, POPIA liabilities that cannot lawfully be limited, CPA or product-liability exposure that cannot lawfully be limited, intellectual-property infringement indemnities expressly accepted by the Company, or any other liability that Applicable Laws prohibit limiting.

To the maximum extent permitted by law and subject to the preceding consumer and non-excludable-liability protections, neither party is liable to the other for indirect, consequential, punitive or special damages, loss of profit, loss of business, loss of goodwill, or loss arising from third-party networks or services, except where the loss is caused by fraud, wilful misconduct, gross negligence, intentional breach of confidentiality, unlawful data processing or another non-excludable liability.

30. Complaints, dispute resolution, jurisdiction and consumer protection

The Company will maintain complaint channels for technical, billing, privacy, AI, telehealth, clinical, accessibility, cybersecurity, Break Glass, research and safety complaints. Complaints should be sent to the contact points in clause 32 with enough detail for investigation.

Clinical complaints may also be raised with the responsible Practitioner, Practice, health establishment, relevant professional board, the HPCSA or another competent authority. Privacy complaints may be raised with the Information Officer and the Information Regulator. Medical-device or AI/ML-enabled medical-device safety concerns may be escalated to SAHPRA where applicable. Research concerns may be raised with the relevant REC, HREC, IRB or NHREC route where applicable. Medical-scheme, funder, claims, managed-care or benefits disputes may be raised with the relevant scheme or funder internal dispute process and, where applicable, the Council for Medical Schemes.

Ordinary contractual disputes should first be escalated in good faith to senior representatives for resolution within 14 days. If unresolved, the parties should consider mediation. Arbitration under the rules of the Arbitration Foundation of Southern Africa, seated in Johannesburg, applies only to business-to-business disputes between the Company and Business Users, unless a separate written agreement lawfully provides otherwise. No Patient or Consumer is required by these Terms to arbitrate, to use Johannesburg as a forum, or to give up access to any competent court, regulator, ombud, professional body or statutory complaint process.

These Terms are governed by the laws of the Republic of South Africa. Business-to-business disputes may be referred to a competent South African court or to AFSA arbitration as described above. Patients and Consumers may elect any competent forum available under law, including a Magistrates' Court, High Court where applicable, consumer court, ombud, the Information Regulator, the HPCSA or other professional body, SAHPRA, the Council for Medical Schemes where the dispute concerns a medical scheme/funder/claim matter, a research ethics complaints route, or another competent authority.

Nothing in this clause prevents urgent or interim relief, regulator reporting, patient-safety escalation, POPIA complaints, HPCSA complaints, SAHPRA reporting, REC complaints, criminal reporting, or any non-excludable consumer remedy.

31. Changes to these Terms

The Company may amend these Terms from time to time. Changes may be made to reflect legal, regulatory, clinical, security, operational, service, pricing, AI, device, privacy or technology changes.

The Company will give at least 30 days' advance notice of any Material Change, unless the change is urgent for security, patient safety, legal compliance, regulator instruction, fraud prevention or service continuity, in which case the Company may implement the change sooner and notify Users as soon as reasonably possible. Notice

may be provided by app notice, portal notice, email, SMS or other recorded channel appropriate to the risk and User type.

Continued use after the effective date of a notified Material Change may constitute acceptance only where that is lawful and fair for the User type and change. The Company must obtain affirmative re-consent or refreshed acceptance where a Material Change materially affects privacy practices, cross-border processing, research use, Direct Marketing, AI functionality, automated-decision safeguards, patient-held sharing, children's/representative access or another matter for which Applicable Laws require consent, explicit acknowledgement or a new notice. If a User does not accept a Material Change, the User may stop using the relevant service, subject to record-retention duties, clinical continuity, data export, outstanding fees, legal holds and Applicable Laws.

32. Contact details and legal notices

Purpose	Contact details
Company legal notices	info@ponyadata.co.za ; 7 Acacia Road, Duxberry, Morningside, 2191, 0823998678
Information Officer / POPIA / PAIA requests	info@ponyadata.co.za ; Matthew Trusler, 7 Acacia Road, Duxberry, Morningside, 2191; 0823998678
Clinical governance / patient safety	Dr Jessica Trusler, jessica@ponyadata.co.za , 0829024929
Technical support	info@ponyadata.co.za ; 0823998678; 7am-10pm,
Billing support	info@ponyadata.co.za ; 0823998678; 8am-5pm
Cybersecurity incident reporting	info@ponyadata.co.za ; 0823998678; 7am-10pm,
AI safety or medical-device incident reporting	info@ponyadata.co.za ; Matthew Trusler, 7 Acacia Road, Duxberry, Morningside, 2191 : 0823998678
Research participant complaints	Relevant REC / HREC / IRB / NHREC contact route, where applicable - <i>not applicable currently</i>
Emergency care	Do not use the platform as the first response. Contact local emergency services or go to the nearest emergency unit, clinic or hospital.
PAIA Manual / access to records	<i>The Company's PAIA manual has been compiled and is published at ponyadata.com/paia-manual/. It is also available on request from the Information Officer and at the Company's registered office ;7 Acacia Road, Duxberry, info@ponyadata.co.za</i>

Legal notices sent by the Company may be delivered through PonyaData, email, SMS, in-app notification, portal notice, physical delivery, or another contact method provided by the User, subject to Applicable Laws. Users must keep contact details updated.

The Company must maintain and publish a PAIA manual under section 51 of the Promotion of Access to Information Act. The PAIA manual must be available at ponyadata.com/paia-manual/, from the Information Officer, and at any physical location required by law. It must describe the Company's records, request procedure, POPIA processing purposes, data-subject categories, recipient categories, planned transborder flows, security measures and any other prescribed information. PAIA and POPIA requests should be routed to the Information Officer contact above.

33. General provisions

Severability. Each provision of these Terms is separate. If a court, regulator, tribunal or competent authority finds any provision unlawful, invalid or unenforceable, the remaining provisions continue to apply, and the affected provision must be interpreted or amended as far as legally possible to achieve its lawful commercial, privacy and clinical-safety purpose.

Entire agreement and order of precedence. These Terms, the applicable schedules, service-specific terms, privacy notice, consent screens, practice agreement, practitioner agreement, data-processing agreement, research consent, medical-device labelling and fee schedule form the agreement for the relevant service. If there is a conflict, mandatory law prevails first, then clinical consent/professional duties and medical-device instructions for clinical matters, then the privacy notice and data-processing terms for privacy matters, then service-specific terms, then these Terms.

Non-waiver. A delay or failure by a party to enforce a right is not a waiver of that right. A waiver is effective only if recorded in writing by the party granting it, and applies only to the specific matter waived.

Assignment, cession and transfer. A User may not assign, cede, delegate or transfer rights or obligations under these Terms without the Company's prior written consent, except where Applicable Laws require otherwise. The Company may assign, cede, delegate, transfer or subcontract its rights or obligations to a successor, affiliate, purchaser, restructuring entity, operator, hosting provider or service provider, provided this does not unlawfully reduce patient rights, POPIA protections, clinical-record access, security safeguards or professional accountability. Material transfers affecting Consumers, Patients or personal information must be notified where required by law.

Force majeure. The Company is not responsible for delay or failure caused by events beyond its reasonable control, including power failure, network outage, cloud or telecoms failure, cyberattack, strike, natural disaster, epidemic, war, civil unrest, court order, regulator action, supplier failure or emergency. This does not remove duties that cannot be suspended by law, including reasonable steps for patient safety, security-compromise response, clinical-record protection, statutory notices and continuity planning where feasible. If an event of force majeure continues for more than 90 consecutive days, either Party may terminate the affected service on 30 days' written notice without liability, subject to data export, clinical continuity, record-retention and patient-safety obligations.

Interpretation. Headings are for convenience only. Words such as 'including' mean 'including without limitation'. The singular includes the plural and the plural includes the singular. A reference to a law includes that law as amended, replaced or supplemented. Where these Terms require something to be done in writing, a data message satisfies that requirement where ECTA and Applicable Laws permit it.

Third-party services. Third-party integrations, laboratories, pharmacies, medical schemes, payment processors, hosting providers, AI vendors and other suppliers may have separate terms and legal duties. The Company is not responsible for a third party's independent clinical, funding, regulatory or professional decision unless Applicable Laws or a written agreement make the Company responsible.

Schedule 1 - POPIA Privacy Notice and Lawful-Basis Schedule

This Schedule is the user-facing POPIA privacy notice. It includes the binding Responsible Party / Operator allocation for current PonyaData services and the layered lawful-basis table.

1. Responsible parties and operators

The role allocation in clause 17 and the table in paragraph 3 of this Schedule is binding for current services. The Company is not the Responsible Party for clinical care or clinical records merely because it provides the technology, hosts the record, runs an AI Function, routes a message, supports a workflow, or stores a backup. For those clinical flows, the Company acts as Operator unless the table expressly allocates a separate Company Responsible-Party purpose. Where the Company is Responsible Party for identifiable Health Information, it must document the section 11 basis, the separate section 27 or section 32 special-information authorisation, any children's-information authorisation, and any cross-border section 72 / section 57 requirement, or use genuinely de-identified information.

2. Categories of personal information

- Identity and contact details: name, ID/passport number, date of birth, sex or gender where clinically relevant, address, phone, email, next of kin, emergency contact and authorised representative details.
- Account and technical data: login credentials, device data, IP address, access logs, audit trails, consents, permissions, preferences, support tickets and security events.
- Health Information: symptoms, diagnoses, medical history, allergies, medications, pregnancy status, disabilities, mental health information, sexual health information, images, documents, remote monitoring data, prescriptions, results, referrals, clinical notes, discharge summaries, sick notes and communications.
- Professional and Practice data: professional registration, scope of practice, Practice details, facility affiliation, role, permissions, billing identifiers, service account details and user activity.
- Payment and funding data: invoices, payment status, payment tokens or processor references, medical aid details, claims support information and billing references.
- Marketing and communication-preference data: opt-in records, opt-out records, unsubscribe events, campaign logs, communication preferences, suppression lists and consent versions.
- AI and analytics data: prompts, outputs, risk flags, confidence or uncertainty indicators, model or rule version, review decisions, overrides, usage logs and safety-monitoring metadata.
- Research information: only where lawful and ethically approved, data sets, consent records, protocol references, de-identification keys, DTA/DSA/MTA records and REC/HREC/IRB approvals.
- Children and representative-access data: competent-person consent records, authority-verification records, maturity/capacity assessments, Representative Access permissions, Restricted Confidential Entry flags, masking decisions, transition-to-majority notices and related audit logs.

Occupational health data: medical surveillance information, fitness-for-work assessments, workplace health records, injury-on-duty documents, functional limitations, accommodation recommendations, employer-facing outcome records, and audit logs for occupational-health access controls. Clinical occupational-health content must remain walled from employer access except where lawful disclosure is specifically authorised.

3. Purposes, ordinary-personal-information lawful bases and special-information authorisations

This table separates three issues that must not be conflated: first, who is the Responsible Party or Operator for the data flow; second, the section 11 basis for ordinary personal information; and third, the additional section 27 or section 32 authorisation required before identifiable Health Information or other special personal information may be processed. A purpose must not proceed with identifiable Health Information unless all applicable columns are satisfied for the Responsible Party named for that flow, or the information has been genuinely de-identified so that it cannot reasonably be re-identified.

Legitimate interests and contract performance must not be read as standalone grounds for processing identifiable Health Information. They may appear in the section 11 column for ordinary account, technical, billing, support or security data, but the special-information column must still be satisfied for Health Information.

This table is the published role and lawful-basis register for current services. The Company must maintain an internal data-flow register that is consistent with it. A materially new data flow, AI Function, data category, hosting model, recipient, research use or cross-border access path involving identifiable Health Information is not authorised by these Terms unless the Company issues a service-specific notice or addendum that updates the role allocation, lawful basis, special-information authorisation, retention rule, cross-border position and operator or data-sharing agreement before the new processing starts.

Purpose / data flow	Binding Responsible Party / Operator allocation	Section 11 basis for ordinary Personal Information	Section 27 / section 32 special-information authorisation for identifiable Health Information	Company limits for identifiable Health Information
Patient account, identity verification and access management	Company is Responsible Party for Patient and Practitioner platform account registration, authentication, identity/access verification, credential management, access controls and security metadata. Practice is Responsible Party for its own authorised-user selections and role approvals. Company is Operator for carrying out Practice user-management instructions.	s11(a) consent where used; s11(b) contract or pre-contract steps; s11(c) legal obligation; s11(f) legitimate interests for ordinary access, security and fraud-prevention data only.	Usually not required where only ordinary account data is processed. If account or identity data includes Health Information, rely on s27(a) consent, s27(b) rights or obligations in law, or s32 only for qualifying health-sector processing.	Do not collect health-status markers for access management unless necessary. Use Health Information for access control only as Operator for the care provider or with documented consent/special authorisation.
Clinical care, consultation, recordkeeping and continuity	Practice, Practitioner or health establishment is Responsible Party for Clinical Services, clinical records, clinical communications, prescriptions, referrals, results, discharge summaries, sick notes and continuity of care. Company is Operator when it hosts, routes, structures, displays, stores, backs up, summarises or presents those records for care on that Responsible Party's instructions.	s11(a) consent where obtained; s11(b) contract where applicable; s11(c) legal obligation; s11(d) protection of the Patient's legitimate interests for care-related ordinary PI.	s32(1)(a) where medical professionals, healthcare institutions or facilities process health information necessary for proper treatment or care, or administration of the professional practice/institution; s27(a) consent; s27(b) rights or obligations in law where applicable.	As Responsible Party, Company may not rely on s32 unless it qualifies for the relevant processing. Otherwise process as Operator under instructions or obtain consent / another s27 authorisation.
Scheduling, reminders, secure messaging and telehealth logistics	Company is Responsible Party for platform-level booking, reminder delivery, queue management, user notifications and service logistics. Practice/Practitioner is Responsible Party for clinical consultation content, attendance decisions, triage instructions and care communication. Company is Operator for clinical content carried in messaging	s11(a) consent for communication preferences; s11(b) contract; s11(c) legal obligation for records; s11(f) legitimate interests for ordinary service-delivery and security metadata.	s32(1)(a) for clinical communications processed by qualifying care providers for treatment/care or administration; s27(a) consent for Company-controlled identifiable clinical content; s27(b) rights/obligations in law where applicable.	Use clinical message content only for delivery, support, safety, audit and care purposes disclosed to the Patient. Minimise sensitive content in ordinary reminders and non-secure channels.

Purpose / data flow	Binding Responsible Party / Operator allocation	Section 11 basis for ordinary Personal Information	Section 27 / section 32 special-information authorisation for identifiable Health Information	Company limits for identifiable Health Information
	or telehealth workflows.			
Prescribing, medication safety, triage, referrals, test requests, discharge letters, sick notes and patient letters	Practitioner/Practice is Responsible Party for clinical decisions, prescriptions, medication-safety review, triage, referrals, test requests, discharge letters, sick notes, patient letters and records. Company is Operator for generating drafts, routing requests, checking interactions and storing outputs on instructions. Company is Responsible Party for limited platform safety-governance logs created for its own compliance and AI/device oversight.	s11(a) consent where obtained; s11(c) legal/professional obligations; s11(d) protection of Patient interests; s11(b) contract for service administration.	s32(1)(a) for proper treatment/care and administration by qualifying providers; s27(a) consent; s27(b) establishment, exercise or defence of rights/obligations in law where relevant.	AI alerts and templates are support tools only. Company Responsible-Party safety logs must be minimised, pseudonymised where feasible, and tied to consent, legal obligation or another s27/s32 authorisation.
Patient-held or shared Global Health Record and patient-directed sharing	Company is Responsible Party for patient account permissions, sharing consents, Representative Access, segmentation/masking controls, access-control infrastructure, audit trails and revocation workflow. The originating Practice/Practitioner remains Responsible Party for clinical records it created. Receiving Practitioners or facilities are Responsible Parties for care use after Patient-authorised or lawful emergency disclosure. Company is Operator for hosting, transmitting and masking clinical records on documented instructions.	s11(a) consent; s11(b) contract; s11(d) protection of Patient interests; s11(c) legal obligation for records/audit where applicable.	s27(a) consent for patient-directed sharing; s32(1)(a) for receiving providers using the information for treatment/care or administration; s27(b) rights/obligations in law for lawful emergency or legal disclosures.	Record consent/direction, access scope, recipient, time period, revocation and masking/segmentation rules. Apply section 72 safeguards to cross-border sharing facilitated by the Company and analyse section 57 where the Company controls a transfer to a non-adequate jurisdiction. Exclude Restricted Confidential Entries from representative or patient-directed sharing unless legally justified.

Purpose / data flow	Binding Responsible Party / Operator allocation	Section 11 basis for ordinary Personal Information	Section 27 / section 32 special-information authorisation for identifiable Health Information	Company limits for identifiable Health Information
Break Glass emergency access	Company is Responsible Party for Break Glass access-control design, event logs, patient-notification workflow, Information Officer review and security assessment. The emergency Practitioner/unit/health establishment is Responsible Party for deciding and documenting clinical emergency use. Company is Operator for disclosure of underlying clinical records held on behalf of the originating care provider.	s11(d) protection of Patient interests for emergencies; s11(c) legal obligation where access/disclosure is required by law or court order; s11(a) consent where feasible but not required where a lawful emergency/legal basis applies. Security-incident containment should rely on s11(c)/(f) for metadata and security data only.	s32(1)(a) where qualifying providers process information necessary for proper treatment or care; s27(b) where necessary for the establishment, exercise or defence of a right or obligation in law; disclosure required by law or court order; and serious-threat/public-health bases only where the National Health Act or other law permits. Restricted Confidential Entries require the same limited legal justification.	All Break Glass access must be time-limited, reason-coded, logged, reviewed by the Information Officer or delegate, and notified to the Patient unless lawful reasons justify delay or withholding. Do not use Break Glass for ordinary support, product improvement, billing, non-urgent investigation or Company-approved exceptional purposes.
Billing, claims, medical-aid motivations, payments and debt administration	Practice/Practitioner is Responsible Party for clinical billing, coding, motivations and claims content. Medical scheme/insurer/funder is Responsible Party for benefits administration after receipt. Company is Responsible Party for PonyaData platform invoices, subscriptions and payment account data. Company is Operator when routing Practice claims, funder motivations or billing communications on instructions.	s11(a) consent or authorisation; s11(b) contract; s11(c) legal obligation; s11(f) legitimate interests for ordinary payment recovery and account administration only.	s32(1)(a) for administration of the professional practice/institution; s32(1)(b) for insurers, medical schemes, administrators and managed-care organisations where necessary; s27(a) consent; s27(b) rights/obligations in law.	Use the minimum clinical detail required for claims or motivations. Company may not repurpose identifiable claims Health Information for unrelated analytics or commercial purposes without consent/special authorisation.
Security, audit trails, fraud prevention, incident response and data integrity	Company is Responsible Party for platform security monitoring, access logs, audit trails, vulnerability management, incident detection and platform-wide incident response. Practice/Practitioner is Responsible Party for local account governance, authorised-user	s11(c) legal obligation, including POPIA security safeguards; s11(f) legitimate interests for ordinary security/audit data; s11(d) protection of Patient interests.	If logs contain Health Information, rely on s32(1)(a) for provider administration/care, s27(b) for legal rights/obligations or claims, s27(a) consent where required, or de-identification/pseudonymisation where feasible.	Avoid storing clinical content in logs unless necessary. Mask, truncate or pseudonymise where possible; restrict security-log access and retain according to Schedule 8.

Purpose / data flow	Binding Responsible Party / Operator allocation	Section 11 basis for ordinary Personal Information	Section 27 / section 32 special-information authorisation for identifiable Health Information	Company limits for identifiable Health Information
	management and clinical-record audit decisions. Company is Operator when providing incident support for Practice-controlled clinical records.			
AI-assisted clinical workflow, documentation, summarisation and safety alerts	Practice/Practitioner is Responsible Party for clinical use of AI outputs, human review, adoption into clinical records and clinical decisions. Company is Operator when running AI Functions to support care or documentation on instructions. Company is Responsible Party for AI Function Register, model-card documentation, platform safety monitoring and compliance records it determines for its own governance.	s11(a) consent/transparency where required; s11(b) service contract/operator delivery; s11(c) legal/device/safety obligations; s11(f) legitimate interests for ordinary operational metadata only.	s32(1)(a) for qualifying care-provider processing necessary for treatment/care or administration; s27(a) consent for Company Responsible-Party processing of identifiable Health Information; s27(b) legal rights/obligations where applicable.	No AI output may be adopted without human review. Do not use identifiable Health Information for Company AI training, fine-tuning or product improvement unless consent, a lawful s27/s32 authorisation or genuine de-identification applies.
AI governance, validation, bias monitoring, product improvement and model-performance monitoring	Company is Responsible Party for product-governance analytics, AI validation, bias monitoring, model-performance monitoring and product improvement that it determines. Practice/Practitioner is Responsible Party for internal clinical quality review that it determines. Company uses de-identified data by default and processes identifiable Health Information for Company Responsible-Party purposes only where consent, section 27/32 authorisation, legal obligation, Regulator authorisation or ethics-approved waiver applies.	s11(a) consent where identifiable data is used; s11(c) legal/device/safety obligations; s11(f) legitimate interests for ordinary operational and technical metadata only.	For identifiable Health Information, legitimate interests are not sufficient. Use s27(a) consent, s27(d) historical/statistical/research purposes with public interest and sufficient safeguards where applicable, s27(b) legal rights/obligations, Regulator authorisation, or a qualifying s32 basis only where the Company falls within it for the specific processing.	Default to de-identified or aggregated data. Any identifiable-data exception requires documented approval by the Information Officer and Clinical Governance/AI Safety Lead, plus transparency, minimisation and access controls.
De-identified analytics,	Company is Responsible Party for	If genuinely de-identified, POPIA	If genuinely de-identified, no Health Information gateway is	Maintain a de-identification

Purpose / data flow	Binding Responsible Party / Operator allocation	Section 11 basis for ordinary Personal Information	Section 27 / section 32 special-information authorisation for identifiable Health Information	Company limits for identifiable Health Information
quality improvement and local disease-context reporting	the de-identification process, de-identification controls, re-identification risk assessment and aggregate/de-identified analytics it determines. Practice/Practitioner is Responsible Party for de-identification or quality improvement it determines. Genuinely de-identified information falls outside POPIA, but contractual re-identification prohibitions still apply.	does not apply. If pseudonymised or indirectly identifiable, use the applicable s11 basis such as s11(a), s11(c) or s11(f) for ordinary PI.	required. If re-identifiable or pseudonymised, the relevant s27/s32 authorisation remains required.	standard, re-identification risk assessment, output suppression rules, access controls and a prohibition on attempted re-identification.
Research, publication, external collaboration, AI training or fine-tuning, and external validation	Research sponsor named in the protocol is Responsible Party for research purposes. Company is Responsible Party where it sponsors or determines the research, publication or AI-training purpose. Practice, university, collaborator or funder is Responsible Party for research purposes it determines. Company is Operator only where it processes research data solely on documented instructions under a DTA/DSA/DPA/MTA.	s11(a) specific informed consent; s11(c) legal/ethics obligations where applicable; s11(f) only for ordinary administrative research records, not as a basis for identifiable Health Information.	s27(a) consent; s27(d) historical, statistical or research purposes where public interest/necessity and sufficient safeguards apply, including lawful REC/HREC/IRB waiver where available; s27(b) rights/obligations in law; section 35 for children where applicable. Section 32 is not a general research gateway for a technology supplier.	No identifiable Health Information for research, publication, AI training/fine-tuning or external validation without specific consent or an ethics-approved lawful waiver and documented POPIA basis. Use DTA/DSA/MTA, section 72 safeguards and section 57 prior authorisation where a Company-controlled transfer of special or children's information to a non-adequate jurisdiction is triggered.
Legal, regulatory, professional, complaints, insurance and claims handling	Company, Practice, Practitioner, insurer, regulator or professional body is a separate Responsible Party for its own legal, regulatory, professional, complaints, insurance and claims-handling purposes. Company is Operator where it assists a care provider or facility with disclosure, records, audit pack or regulator response on	s11(c) legal obligation; s11(f) legitimate interests for ordinary dispute/compliance data; s11(a) consent where used.	s27(b) establishment, exercise or defence of rights or obligations in law; s32(1)(a) for provider administration; s27(a) consent where required; other regulator/statutory authorisation where applicable.	Restrict access to legal, compliance, clinical governance and regulator-response personnel. Apply legal holds and disclose only what is necessary and lawful.

Purpose / data flow	Binding Responsible Party / Operator allocation	Section 11 basis for ordinary Personal Information	Section 27 / section 32 special-information authorisation for identifiable Health Information	Company limits for identifiable Health Information
	documented instructions.			
Support, maintenance, data migration and troubleshooting	Company is Responsible Party for support account data, ticket administration, platform diagnostics and its own security/compliance logs. Company is Operator for clinical or Health Information accessed to support, migrate, repair or troubleshoot a Practice/Practitioner workflow on documented instructions.	s11(b) contract or pre-contract steps; s11(c) legal/security obligations; s11(f) legitimate interests for ordinary support, diagnostics and service-integrity data only.	For identifiable Health Information, rely on the originating provider's s32(1)(a) processing where Company acts as Operator; otherwise s27(a) consent, s27(b) legal rights/obligations, Regulator authorisation or another lawful special-information gateway.	Support access to clinical content must be minimised, reason-coded, logged, role-restricted and time-limited. Do not copy clinical content into support tickets unless necessary; mask or pseudonymise where feasible.
Cross-border access, third-party processors, integrations and security tools	The Responsible Party for the source data flow is accountable for authorising and documenting any section 72 transfer and section 57 prior-authorisation trigger. Company is Responsible Party for transfers of Company-controlled account, billing, security or governance data. Company is Operator for transfers of Practice-controlled clinical records and must not cause the transfer unless instructed by the Responsible Party or required by law. Patient-directed Global Health Record sharing is separately logged as patient-directed sharing.	s11(a) consent where required; s11(b) contract where necessary for a requested service; s11(c) legal obligation; s11(f) ordinary supplier/security governance data only.	For identifiable Health Information, satisfy the relevant section 27/32 gateway for the underlying processing plus POPIA section 72 transfer safeguards. If the Company controls transfer of special personal information or children's Personal Information to a third party in a country without adequate protection under section 72, obtain section 57 prior authorisation under section 58 before transfer, or restructure through genuine de-identification, patient-directed disclosure, adequate-protection recipient, or another lawful route. 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	No routine cross-border processing of identifiable Health Information is intended. Record country, recipient, purpose, safeguard, retention, Responsible Party approval, adequacy assessment, section 57 decision and patient notice. Use DTA/DSA/DPA/MTA controls where applicable.

Purpose / data flow	Binding Responsible Party / Operator allocation	Section 11 basis for ordinary Personal Information	Section 27 / section 32 special-information authorisation for identifiable Health Information	Company limits for identifiable Health Information
			taken reasonable steps to mitigate risk	
Children, Mature Minors, Restricted Confidential Entries and Representative Access	Practice/Practitioner or health establishment is Responsible Party for clinical consent, maturity/capacity, confidentiality and disclosure decisions. Company is Responsible Party for platform permissions, Representative Access tooling, masking/segmentation controls, transition-to-majority workflow and audit logs. Company is Operator when enforcing provider instructions about child records.	s11(a) consent by the child where legally competent or by a Competent Person; s11(c) legal obligation; s11(d) protection of the child's legitimate interests where applicable; s11(b) contract/service administration for ordinary account data only.	POPIA sections 34 and 35 must be satisfied for children's Personal Information. Health Information also requires s27/s32 authorisation, including s32(1)(a) for qualifying care providers where necessary for treatment/care or administration, s27(a) consent, s27(b) legal rights/obligations, or a lawful research/public-interest authorisation with safeguards. Mature-minor and statutory confidentiality rules may require withholding from representatives.	Verify Competent Person or representative authority; document mature-minor/capacity decisions; segment/mask Restricted Confidential Entries; prevent automatic guardian access to protected sexual-health, reproductive-health, HIV, contraception, termination-of-pregnancy, mental-health, abuse or safeguarding entries; transition account control at majority.
Occupational health, medical surveillance, fitness-for-work, employee-assistance and employer reports	Occupational Health Practitioner/Practice is Responsible Party for occupational-health clinical records and clinical disclosure decisions. Occupational Health Client/employer is Responsible Party only for employment-administration data and lawful outcome-level information it receives. Company is Operator for occupational-health clinical records processed on instructions and Responsible Party for platform account, access, audit and support records it determines.	s11(a) consent where required; s11(b) contract for ordinary service administration; s11(c) legal obligation where occupational health and safety or employment law requires processing; s11(d) protection of the employee/Patient's legitimate interests where applicable. s11(f) may support ordinary employer account or security data only, not as a standalone gateway for identifiable Health Information.	For Health Information, use s32(1)(a) where qualifying health professionals, institutions or facilities process the information for proper treatment/care or administration; s27(a) consent; s27(b) rights or obligations in law, including lawful occupational health or safety duties; or another specific authorisation. Medical testing and health disclosures must also satisfy the Employment Equity Act and professional confidentiality duties.	Maintain a walled occupational-health workspace. Employer-facing access is normally limited to fitness/outcome status, functional restrictions, accommodation recommendations, attendance/billing information or statutory reports. Do not disclose diagnoses, clinical notes, results, prescriptions, Global Health Record content or Restricted Confidential Entries to an employer unless specifically lawful and documented.
Service Messages, communication preferences and Direct Marketing	Company is Responsible Party for its own Service Messages, marketing consents, suppression lists and Direct Marketing. Practice/Practitioner	Service Messages: s11(b) contract/service steps, s11(c) legal obligation, s11(d) protection of the Patient's interests or s11(f) ordinary	Health Information must not be used for Direct Marketing unless a specific section 27/s32 authorisation and explicit, voluntary, informed consent permits the precise use and no health, professional or ethical rule	Do not target marketing based on diagnoses, medicines, mental health, sexual health, HIV, reproductive health, children's records, Restricted

Purpose / data flow	Binding Responsible Party / Operator allocation	Section 11 basis for ordinary Personal Information	Section 27 / section 32 special-information authorisation for identifiable Health Information	Company limits for identifiable Health Information
	is Responsible Party for Practice-originated clinical or administrative communications. Company is Operator when sending Practice communications on documented instructions.	legitimate interests where applicable. Direct Marketing: s11(a) consent and POPIA section 69 opt-in/soft opt-in where permitted; CPA section 11 opt-out rights must be honoured.	prohibits it. Children's information requires POPIA section 35 authorisation and appropriate consent.	Confidential Entries or occupational-health records unless legally reviewed and specifically consented. Keep Service Messages separate from marketing and maintain suppression lists.

4. Health Information and special personal information

Health Information is special personal information and receives additional protection. It will be processed only where the table above identifies both the relevant section 11 basis and the separate section 27 or section 32 authorisation for the relevant Responsible Party, and only to the extent necessary for the disclosed purpose, by authorised persons subject to confidentiality, with appropriate security controls and auditability.

The Company will not use identifiable Health Information for marketing unrelated products, sale to third parties, external AI training, AI fine-tuning, publication, commercial data products or unrelated product improvement unless a separate lawful basis and special-information authorisation apply, with transparency, specific consent or a lawful REC/HREC/IRB waiver where required, ethics approval where required, and contractual safeguards. Where those requirements are not met, the Company must use genuinely de-identified information.

5. Recipients and disclosure

- Practitioners, nurses, pharmacists, allied health professionals, administrators and support staff involved in care or platform operation.
- Hospitals, clinics, emergency services, laboratories, imaging providers, pharmacies, specialists, referring practitioners and receiving practitioners where clinically required or Patient-authorised.
- Hosting, software, cybersecurity, payment, communication, AI, analytics, support and professional-service providers under confidentiality and security obligations.
- Medical schemes, insurers, funders or sponsors where authorised or required for billing, benefits administration, managed care or legal duties, using the minimum Health Information necessary.
- Occupational Health Clients or employers only through the occupational-health regime in clause 11A and the role-allocation table, normally limited to fitness/outcome-level information, functional restrictions, accommodation recommendations, attendance/billing data or statutory reports. Employers must not receive full clinical records, diagnoses, results, prescriptions, Global Health Record content or Restricted Confidential Entries unless a specific lawful disclosure route applies.
- Regulators, courts, law enforcement, professional bodies, SAHPRA, the Information Regulator, research ethics committees or other authorities where required or permitted by law.
- Research collaborators only under required consent or waiver, ethics approval, de-identification where feasible, data-sharing agreements and POPIA safeguards.

6. Data subject rights

A data subject may request access to personal information, correction of inaccurate information, deletion or destruction where legally available, objection to certain processing, withdrawal of consent where consent is the legal basis, human review of applicable automated decisions, and details of third parties who have received information where required by law. Requests must be sent to the Information Officer contact in clause 32.

The Company may require identity verification and may refuse or limit a request only where permitted by law, for example to protect another person's rights, preserve clinical records, comply with legal duties, protect patient safety, enforce legal claims or maintain records that may not lawfully be deleted.

6A. Children, Mature Minors and Representative Access

Where a Patient is a child, processing must satisfy both the ordinary POPIA conditions and the children's-information authorisation in POPIA section 35, in addition to the special-information authorisation for Health Information. Competent-person consent must be obtained and verified unless an applicable law allows the child to consent independently, the processing is necessary for a right or obligation in law, an ethics-approved public-interest research exception with safeguards applies, or another section 35 authorisation applies.

When a Practitioner determines that a child is a Mature Minor for a particular service or that a statute protects a child's confidential consent, PonyaData must support record segmentation and masking so that parent, guardian, caregiver or other representative access excludes Restricted Confidential Entries unless disclosure is legally required or otherwise lawfully authorised. This includes configured protections for relevant sexual-health, reproductive-health, HIV, contraception, termination-of-pregnancy, mental-health, abuse, violence or safeguarding entries.

Representative Access permissions must be reviewed periodically and at material events, including change of guardian, dispute, safeguarding concern, withdrawal of consent where permitted, and the Patient reaching 18 years of age. At majority, the Patient must be offered account-control transition, review of sharing permissions and continuation or revocation choices subject to lawful clinical-record retention and legal holds.

7. Retention and deletion

Records will be retained according to Schedule 8 and POPIA section 14. Indefinite retention is not the default or preferred rule. The Responsible Party allocated to the relevant data flow is accountable for documenting the statutory or professional minimum, any longer purpose-justified clinical governance period, any contract or legal-hold period, and any Patient- or Competent-Person-consented patient-held record period. Where the Company is Operator, it must enforce the Responsible Party's documented retention, export, deletion, de-identification and legal-hold instructions while retaining Company-controlled security, audit, support and incident records only where independently lawful.

8. Cross-border transfers

No routine cross-border transfer of identifiable Health Information is intended. If a cross-border transfer or access occurs, the Responsible Party allocated to the source data flow must record the purpose, recipient, country, safeguard, POPIA section 72 basis, underlying section 27/32 special-information authorisation, children's-information authorisation where relevant, retention period and data-subject notice. Before any Company-controlled transfer of identifiable Health Information, special personal information or children's Personal Information to a third party in a foreign country that does not provide adequate protection as contemplated by section 72, the Company must obtain POPIA section 57 prior authorisation from the Information Regulator under section 58, or restructure the transfer so that it is patient-directed, genuinely de-identified, routed to an adequate-protection recipient, or otherwise lawfully authorised and documented. Where the Company is Operator, it must not initiate or authorise the transfer without the Responsible Party's documented instruction or a legal requirement, and must assist with notices, transfer impact assessments, contracts, section 57 analysis and breach response. Patients should be notified of material cross-border transfers and the level of protection or safeguards where required. Practitioner access for treating a Patient located in South Africa requires South African registration or statutory authority where required, including HPCSA registration where applicable. Patient-initiated sharing with an overseas treating clinician while the Patient is outside South Africa is Patient-directed disclosure, not a Company-controlled transfer, provided the Company does not determine the overseas recipient or purpose beyond executing the Patient's instruction.

Schedule 2 - Digital Health and Telehealth Informed Consent

This Schedule covers general digital health use and adds telehealth-specific wording when the consultation occurs remotely.

A. Digital health consent for all users

1. I understand that PonyaData is used to capture, organise, store, share and present health information to support my care or the care of the Patient I represent.
2. I understand that PonyaData may be used during in-person care at a practice, clinic, ward, hospital or outpatient unit, and may also support remote care or telehealth where clinically suitable.
3. I consent to relevant electronic records, messages, appointment data, clinical notes, prescriptions, referrals, test requests, results, discharge letters, sick notes, patient information letters, medical-aid motivations, billing records, consent records and audit logs being created and stored as part of the health record.
4. I understand that authorised Practitioners and care-team members may access relevant parts of my record for care, continuity, emergency treatment, referrals, billing, quality and legal compliance, subject to confidentiality and access controls.
5. I understand that PonyaData may use AI-assisted tools to draft notes, summarise information, identify safety alerts, triage risk, support documentation and improve workflow, but AI does not replace the Practitioner and material clinical outputs must be reviewed by a human before adoption.
6. I understand that I should check information I provide, tell the Practitioner if anything is inaccurate or missing, and seek urgent or emergency care where needed.
7. I understand that no electronic system is risk free, but reasonable security measures will be used to protect my information.
8. I understand that I may ask questions, request access or correction, raise privacy concerns, and use complaint routes described in the Terms.

B. Additional consent for telehealth or remote consultations

9. I understand that telehealth means healthcare provided at a distance by electronic communication, including video, audio, messaging, images, remote monitoring or document review.
10. I understand that the Practitioner or platform may need to confirm my identity, my location, the Practitioner's identity and registration details, the reason for the consultation, and whether telehealth is suitable for my condition.
11. I understand that telehealth may not allow a full physical examination and may be affected by connectivity issues, device problems, misunderstanding, incomplete information, privacy risks, data errors or delayed response.
12. I agree to provide accurate and complete information and to tell the Practitioner if my symptoms worsen, if I am in an emergency, if I am in a different location, or if I do not understand the advice given.
13. I understand that the Practitioner may decide that I need in-person care, emergency care, a test, a specialist, a different practitioner, a physical examination, or no prescription or certificate.
14. I understand that a prescription, certificate, diagnosis or treatment should not be issued solely on the basis of an online questionnaire where a proper clinical evaluation is required.
15. I consent to the telehealth consultation and to relevant electronic communications, prescriptions, referrals, test requests, reports, images, messages, clinical notes and consent records being stored in my health record.
16. I understand that I may decline telehealth or stop the consultation, but I remain responsible for seeking urgent or emergency care where necessary.

Schedule 3 - AI-Assisted Healthcare Notice and AI Governance Terms

1. What AI may do

- Prepare drafts or summaries for human review.
- Identify possible risk factors, care gaps, medication interactions, allergies, red flags or follow-up needs.
- Assist with triage, documentation, patient education, translation support, administrative routing, billing support or coding support.
- Analyse structured or unstructured data, remote monitoring information, images or documents where validated and authorised for the intended use.
- Support quality improvement, safety monitoring, bias detection, cybersecurity monitoring and product performance analysis.

2. What AI may not do

- Replace the Practitioner's clinical judgement.
- Make the final diagnosis, treatment, prescription, referral, emergency, discharge, denial-of-access or clinical-prioritisation decision.
- Be used outside its intended use, validated population, risk class, language, data condition, clinical setting or approved workflow.
- Be used to unfairly discriminate, deny human review, manipulate billing, fabricate clinical facts or create perverse incentives.
- Be adopted into a clinical record without human review and approval.

3. AI Function Register and model cards

The Company must maintain an AI Function Register for material AI Functions. For each clinical, patient-facing, access-affecting or high-risk function, the Register or associated model card should include:

- Function name, owner, version, vendor, deployment date and retirement date.
- Intended use, prohibited uses, users, affected Patients, clinical setting and workflow location.
- Data inputs, output type, uncertainty or confidence communication, and known limitations.
- Human oversight design, required reviewer, escalation rules and override process.
- Validation evidence, local South African disease-context assessment where relevant, performance metrics and data-quality requirements.
- Bias, fairness, accessibility, language and generalisability assessment.
- SAHPRA classification status and medical-device controls where applicable.
- Cybersecurity, privacy, logging, monitoring, model drift, change control, post-deployment review and incident response.
- Patient-facing transparency summary where the function materially affects care, access or rights.

4. Human review and liability allocation

No AI Function output shall be adopted into a clinical record unless reviewed, edited where necessary, and approved by a registered Practitioner or other authorised human user acting within lawful scope. A Practitioner who chooses to rely on an AI output remains professionally responsible for the clinical decision, subject to the Company's responsibility for its own platform, governance, security, regulated-device obligations, product safety, medication-interaction engine design, instructions, warnings and contractual duties.

The Company disclaims liability, to the extent permitted by law and primarily as against Business Users, for unreviewed AI outputs used contrary to these Terms, warnings, model cards, intended-use instructions or professional obligations. This disclaimer does not exclude liability to Patients or Consumers for the Company's own defective software, defective safety or medication-interaction engine, inadequate warnings, regulated-device failures, POPIA duties, CPA duties or any liability that cannot lawfully be excluded.

5. Patient rights and safeguards

- Patients may ask whether AI materially assisted a clinical decision or communication.
- Patients may request meaningful information about the AI Function's purpose, data inputs, limitations, uncertainty, human oversight and known risks where required and feasible.
- Patients may report suspected inaccurate, unsafe, biased or unexplained AI output.
- Patients may request human review of a decision that materially affects them and is based on automated processing.
- Patients may decline optional research or external AI training uses without losing ordinary care.

Schedule 4 - Practice and Healthcare Practitioner Addendum

- The Practice must appoint an account owner, maintain accurate Practice details, manage authorised users, review role permissions, remove departed users, and ensure that user access matches job function and clinical need.
- The Practitioner must maintain current registration with the relevant statutory professional council or other lawful authority, qualifications, scope of practice, indemnity or insurance where required, and authority to practise in South Africa and in the relevant facility, service, province, telehealth or occupational-health context.
- A Practitioner providing remote or digital clinical services to a Patient located in South Africa must hold the South African registration and statutory authority required for that service, including HPCSA registration where applicable.
- A foreign clinician who receives Patient-directed Global Health Record access to treat a Patient outside South Africa is responsible for the law and professional duties applicable to that overseas care relationship.
- The Practice must maintain facility licences, certificates, registrations, OHSC or other compliance requirements, medical scheme practice numbers, billing permissions, data-protection controls, staff training and insurance required for its services.
- The Practitioner must verify the Patient's identity and location where clinically and ethically required, confirm consent, assess telehealth suitability, take an appropriate history, document relevant findings, and preserve an adequate health record.
- The Practitioner must not prescribe, certify, diagnose or treat without an adequate clinical basis, and must not rely solely on a questionnaire or AI output where professional judgement or clinical evaluation is required.

The Practitioner must use the PonyaData signature workflow for any regulated prescription, scheduled-medicine order, sick note, medical certificate or other document requiring signature, and must not issue or transmit it until the required advanced electronic signature or other legally compliant signature method has been completed and logged.

- The Practitioner must critically review AI outputs, understand intended use and limitations, override unsafe or unsuitable outputs, document material reliance where appropriate, and remain accountable for clinical decisions.
- The Practice and Practitioner must not use PonyaData to facilitate unlawful fee-splitting, perverse incentives, over-servicing, unnecessary tests, improper referrals, fraudulent claims, billing misconduct or corporate interference with clinical independence.

Where PonyaData is used for occupational-health services, the Practice, Practitioner and Occupational Health Practitioner must keep occupational clinical records separate from employer-facing outputs and must disclose only lawful fitness/outcome-level information to Occupational Health Clients unless a specific lawful disclosure route permits more.

- The Practitioner must protect access credentials, prevent unauthorised record access, use secure channels, maintain confidentiality, report suspected breaches, and cooperate with audits, complaints, patient-safety investigations and regulator requests.
- The Practice and Practitioner must notify the Company promptly of professional complaints, registration restrictions, adverse events, suspected device issues, AI safety concerns, data breaches, conflicts of interest, facility-compliance concerns or circumstances that may affect safe use of PonyaData.

Schedule 5 - Break Glass Emergency Access Terms

Control	Requirement
Permitted purposes	Only: emergency care or serious threat to the Patient's life or health; access or disclosure required by law or court order; or security-incident containment, investigation and remediation limited to metadata, access logs or technical security data unless clinical-content access is itself legally justified. No open-ended Company-approved exceptional purpose is permitted.
Access conditions	Role-based access, identity verification, reason capture, time-limited session, least-privilege view, MFA for high-risk users where feasible, and access only to information relevant to the limited lawful purpose. Restricted Confidential Entries remain masked unless the Break Glass justification lawfully extends to that entry.
Logging	Record user identity, role, organisation, Patient, date, time, reason, information accessed, actions taken, export/disclosure, duration and review status.
Patient notification	Notify the Patient as soon as reasonably practicable unless notification would prejudice Patient safety, emergency care, a lawful investigation, legal duties, another person's rights or safety, or a regulator/law-enforcement process. Where the Patient is a child or Mature Minor, notification must respect the confidentiality and representative-access rules in clause 14A.
Review	The Information Officer or delegate reviews all Break Glass events. Clinical Governance Lead reviews clinically material or safety-related events. Suspicious events are escalated to incident response.
Security compromise assessment	If access appears unauthorised, excessive, negligent, fraudulent or compromised, assess under POPIA section 22 and Schedule 7.
Discipline and enforcement	Unauthorised Break Glass use may result in account suspension, Practice notification, regulator complaint, disciplinary action, civil claims or criminal reporting where appropriate.

Schedule 6 - Research, Analytics, Data Sharing and Model Development Controls

1. Baseline rule

Ordinary clinical care data must not be repurposed for identifiable research, publication, external sharing, commercial data products, AI model training, fine-tuning or validation unless there is a lawful basis, transparency, proportionality, required consent or waiver, POPIA compliance, ethics approval where required, and appropriate contractual controls.

2. De-identified analytics

The Company may use de-identified or aggregated data for safety monitoring, product improvement, local disease-context optimisation, quality improvement, clinical workflow improvement, operational reporting and bias monitoring if the information cannot reasonably identify a Patient and safeguards prevent re-identification.

3. Research ethics

Where a project involves human participants, identifiable Health Information, human biological material, clinical data sets, AI in a clinical setting, or risk to participants, it must be reviewed by a competent REC, HREC, IRB or equivalent ethics body where required. The protocol should address social value, scientific validity, participant selection, consent, privacy, confidentiality, data management, AI transparency, explainability, accountability, fairness, bias, risk mitigation and benefit sharing.

4. Specific consent and waivers

Patients must provide specific consent for research beyond ordinary care unless a competent ethics committee grants a lawful waiver or alteration of consent and POPIA requirements are met. Consent for care is not automatically consent for research, publication, external AI training, commercialisation or cross-border research sharing.

5. Agreements

- Use a Data Transfer Agreement or Data Sharing Agreement where data alone is shared.
- Use a Data Processing Agreement where a party processes personal information for another party.
- Use a Material Transfer Agreement where human biological material is transferred.
- Use separate agreements for data and material transfers where required or advisable.
- Include purpose limitation, permitted users, security, access controls, onward-transfer limits, retention, destruction, breach notification, IP, publication, benefit-sharing, audit, cross-border transfer safeguards and POPIA compliance.

6. AI model development

AI training, fine-tuning, validation and monitoring data sets should be governed by documented data provenance, lawful basis, minimisation, de-identification where appropriate, representativeness, bias assessment, data quality checks, role-based access, secure environments, logging, reproducibility, model evaluation, human review and a process to address harm or bias discovered after deployment.

Schedule 7 - Cybersecurity and Incident Response Schedule

1. Minimum technical and organisational safeguards

- Encryption in transit for communications carrying personal information or Health Information.
- Encryption at rest for Health Information and sensitive backups where appropriate to the risk.
- Role-based access control, least privilege, unique user accounts and periodic access reviews.
- Multifactor authentication for administrators, privileged users, remote access and other high-risk workflows where feasible.
- Audit trails for clinical records, Break Glass, exports, consent events, AI-output adoption, user administration and security events.
- Secure software development lifecycle, code review, change control, vulnerability management, patching and penetration testing appropriate to risk.
- Data minimisation, pseudonymisation, de-identification and segregation of duties where feasible.
- Backups, disaster recovery, business continuity, restore testing and ransomware resilience controls.
- Logging, monitoring, anomaly detection and alerting for high-risk access or data movement.
- Confidentiality undertakings, staff screening where appropriate, security training and disciplinary controls.
- Supplier due diligence, operator agreements, security questionnaires, incident-reporting obligations and sub-processor controls.
- Physical security and device-security requirements for Company-controlled environments and guidance for Practices using PonyData.

2. Incident response process

Phase	Minimum requirement
Detect and report	Users, staff and suppliers must report suspected security, privacy, AI safety, clinical safety or device incidents promptly through the stated channel.
Triage	Assess severity, information involved, affected systems, patient-safety risk, whether personal information was accessed or acquired by an unauthorised person, and whether a Responsible Party or Operator must be notified.
Contain	Preserve evidence, contain unauthorised access, disable compromised accounts, revoke tokens, isolate systems, stop unlawful disclosures and protect patients.
Escalate	Escalate suspected personal-information compromises to the Information Officer within 24 hours of discovery, awareness or reasonable suspicion where feasible. Escalate clinical safety and AI/device events to the Clinical Governance Lead and AI Safety or Device Lead.
Notify	Where POPIA section 22 applies, notify the Information Regulator and affected data subjects as soon as reasonably possible after the Responsible Party has awareness or reasonable grounds to believe that a compromise may have occurred. The internal target is notification within 72 hours of awareness/reasonable belief where legally notifiable and reasonably feasible, with updates as facts develop. Notify Responsible Parties, Operators, suppliers, insurers, professional bodies, SAHPRA or other authorities where required. Do not wait for final confirmation before starting the notification analysis.
Remediate	Fix root causes, reset credentials, patch vulnerabilities, improve controls, correct records, communicate protective steps and monitor for recurrence.
Review	Complete a post-incident review, update risk assessments, update training, update policies, and record lessons learned.

3. Notification contents

A notification to affected data subjects should, where appropriate and lawful, include the nature of the compromise, the information involved, recommended protective measures, steps taken by the Company, contact details, and any further information required by POPIA or the Information Regulator. Notifications may be updated as further information becomes available.

Schedule 8 - Retention and Deletion Schedule

If a longer period is required by law, professional guidance, contract, funder rule, facility policy, research approval, litigation hold, medical-device duty, occupational-health regulation, medical-surveillance exposure rule or clinical safety, the longer period applies.

Record category	Retention period rule	Notes
Adult patient health records and clinical communications	Retain for at least the applicable statutory/professional minimum, including at least 6 years from dormancy / last clinical encounter, unless a longer period is required or documented under POPIA section 14.	Includes consultations, prescriptions, referrals, discharge summaries, sick notes, results, images, clinical messages, consent records and material AI-output approvals. A longer clinical governance period must be purpose-justified and recorded; otherwise delete, destroy or de-identify when no longer authorised.
Minor patient records	Retain for at least the later of 6 years from dormancy / last clinical encounter and the Patient's 21st birthday, unless a longer period is required by law, legal hold, contract, consent, or a documented clinical-governance purpose under POPIA section 14.	Paediatric records must preserve Restricted Confidential Entry segmentation and masking rules. Longer retention is not automatic; document the clinical, medico-legal or statutory reason, then delete, destroy or de-identify when no longer authorised.
Patients without legal capacity or mentally incompetent patients	Retain for the applicable statutory/professional minimum and any longer period required or purpose-justified for lawful clinical,	Apply representative-access safeguards, dignity, best interests and capacity-review controls. Avoid lifetime retention unless a

Record category	Retention period rule	Notes
	medico-legal, legal-hold, contract or consent reasons under POPIA section 14.	documented lawful basis requires or justifies it.
Occupational health records	Defer to the governing regulation or statutory duty. Depending on the exposure and sector, retain for 20 to 40 years or another prescribed period under applicable occupational health and safety, hazardous chemical, asbestos, lead, biological exposure, noise, radiation, mine health and safety, employment, facility, professional or legal-hold requirements. If no specific long-term rule applies, retain only for the documented period necessary under POPIA section 14 and clinical/professional governance.	Applies where PonyaData processes occupational-health records, medical-surveillance records or workplace-related health records. The stated 20–40 year range is not a universal default; the exact rule must be set by the applicable regulation and exposure category. Keep clinical occupational-health records walled from employer access; employer-facing outputs should be retained separately and limited to lawful outcome-level information.
Clinical trial and regulated research records	As required by protocol, REC/HREC/IRB approval, GCP, SAHPRA, funder, sponsor and Applicable Laws.	Do not delete during an audit, inspection, legal hold or continuing participant-safety requirement.
Research consent, DTA/DSA/MTA and de-identification key records	For the period approved by the REC/HREC/IRB and required by law; otherwise at least 6 years after project closure or longer if risk, publication or audit requires.	Keys linking de-identified data to Patients should be separated and access restricted.
AI Function Register, model cards, validation, safety and change-control records	For the life of the AI Function plus at least 6 years after retirement, or longer where SAHPRA/device rules, litigation or safety duties require.	High-risk or regulated functions may require longer post-market surveillance and vigilance records.
AI prompts and outputs affecting clinical records	Retain as part of the clinical record where adopted or material to care. Draft logs not adopted: unless required for safety, audit or incident investigation.	Must distinguish draft from approved clinical content.
Break Glass logs	At least 6 years after the event, or longer if linked to a clinical record, complaint, breach, investigation or legal hold.	Patient notification and review outcomes should be retained with the access log.
Security logs and access logs	At least 12 to 24 months for routine logs; at least 6 years for logs linked to clinical records, breaches, investigations or legal holds.	
Breach and incident records	At least 6 years after closure or longer if required by regulator, insurer, litigation or clinical safety.	Includes investigation, notices, remediation and lessons learned.
Billing, VAT, tax and payment records	At least 5 years or longer if required by tax, accounting, funder, claim, dispute or contract rules.	Do not retain full card data unless legally and PCI compliant.
Support tickets and administrative communications	At least 12 to 24 months depending on sensitivity, contract, complaint and audit needs.	If a support ticket includes clinical content, retain as clinical record.
Backups	Rolling deletion according to documented backup policy, unless legal hold or restore requirement applies.	Backup restoration must not unlawfully reintroduce deleted data.
De-identified or aggregated data	May be retained while it remains genuinely de-identified or aggregated, the purpose remains lawful and documented, re-identification is not reasonably possible, and re-identification is contractually and technically prohibited.	Review re-identification risk periodically. If the information becomes re-identifiable, apply POPIA retention limits and the relevant special-information authorisation.
Patient-held or shared Global Health Record retained at Patient election	May be retained beyond the ordinary clinical minimum only for the Patient-consented period or until consent is withdrawn, subject to clinical-record duties, legal holds, safety obligations, children/majority-transition rules and any other lawful retention basis under POPIA section 14.	Consent, revocation, export, deletion/de-identification and representative-access settings must be logged.

Source	Terms implementation
Constitution of the Republic of South Africa, 1996: sections 9, 10, 14 and 27	Clauses 3, 6, 9, 12, 13, 15 and 16 commit to access-supporting design, dignity, equality, privacy, non-discrimination, emergency signposting, human review and respectful care.

Source	Terms implementation
National Health Act 61 of 2003	Clauses 12, 15, 16, 20 and Schedules 2, 5 and 8 address informed consent, emergency treatment, confidentiality, creation and maintenance of health records, access to health records, protection of health records, research governance and the narrowed Break Glass purposes consistent with sections 14 to 17.
Health Professions Act 56 of 1974 and professional board rules	Clauses 4, 11, 12, 13, 23 and Schedule 4 preserve practitioner accountability, professional registration, ethical conduct, scope of practice, patient confidentiality and clinical governance.
POPIA Act 4 of 2013	Clauses 14, 14A, 15 and 17 to 24A and Schedule 1 address layered lawful processing, special personal information, children's information, Responsible Party/Operator allocation, section 22 breach notification from awareness/reasonable belief, section 57 prior authorisation, section 69 Direct Marketing opt-in/opt-out, section 71 automated-decision safeguards and section 72 cross-border transfer controls.
POPIA section 22 and section 56	Clauses 2 and 19 and Schedule 7 require Information Officer identification, breach escalation, Information Regulator and data-subject notification, incident records and remediation.
HPCSA Booklet 9: Keeping of Patient Records	Clause 16 and Schedule 8 include record content, access, digital integrity, minimum retention, longer retention for minors where required, deletion/de-identification when retention is no longer authorised, and auditability.
HPCSA Booklet 10: Guidelines for Good Practice in Telehealth	Clause 12, clause 14 and Schedule 2 require telehealth suitability, identity/location verification, informed consent, risk disclosure, record keeping, confidentiality, prescribing safeguards and the rule that Practitioners serving Patients located in South Africa must hold required South African/HPCSA registration where applicable.
HPCSA Booklet 20: Ethical Guidelines on the Use of AI in Healthcare	Clauses 11, 13, 21, 22 and Schedule 3 require AI to support and not replace clinical judgement, informed disclosure, human oversight, fairness, transparency, accountability and professional responsibility.
HPCSA ethical rules on corporate practice, perverse incentives, billing and certificates	Clauses 4, 11, 23 and Schedule 4 prohibit unlawful corporate interference, fee-splitting, perverse incentives, over-servicing, improper referrals, billing misconduct and certificates without adequate clinical basis.
SAHPRA AI/ML-enabled medical devices guidance MD08-2025/2026	Clauses 4, 13, 22 and Schedule 3 require intended-use definition, classification, quality management, validation, clinical evidence, bias/generalisation assessment, cybersecurity, change control, post-market monitoring and incident reporting.
South Africa National AI Policy Framework, 2024	Clauses 3, 6, 13, 19, 21, 22 and Schedule 3 align with human-centred AI, transparency, explainability, fairness, bias mitigation, accountability, strong governance and cybersecurity.
NHREC South African Ethics in Health Research Guidelines, 2024	Clause 21 and Schedule 6 require ethics review, POPIA alignment, REC/HREC/IRB approval where required, DTA/DSA/MTA controls, AI research transparency, fairness, risk mitigation and participant protection.
Electronic Communications and Transactions Act 25 of 2002	Clauses 1, 23, 24, 31 and 33 address electronic acceptance, data messages, writing, compliant electronic signatures, advanced electronic signatures where required, ECTA seven-day cooling-off rights for qualifying online consumer services and service-specific exclusions
Consumer Protection Act 68 of 2008	Clauses 24, 24A, 29, 30 and 31 preserve mandatory consumer rights, direct-marketing cooling-off rights where applicable, transparent pricing,

Source	Terms implementation
	plain-language risk notices, section 49-style prominent notice mechanics, limits on unfair/prohibited terms, section 11 opt-out rights, consumer carve-outs from arbitration/indemnities, product-liability exposure under section 61 where applicable, complaint routes and non-excludable remedies.
Children's Act 38 of 2005: section 129 and child-health consent rules	Clause 14A and Schedule 1 require Competent Person verification, mature-minor/capacity assessment, confidentiality-aware representative access, masking of Restricted Confidential Entries and transition of account control at majority.
Choice on Termination of Pregnancy Act 92 of 1996 and confidentiality-sensitive reproductive health statutes	Clause 14A and Schedule 1 require confidential handling, segmentation and masking for records where a minor or other Patient has a statutory right to independent consent or confidentiality, including termination-of-pregnancy, sexual-health, HIV and contraception-related records where applicable.
Medicines and Related Substances Act 101 of 1965 and General Regulations	Clause 23 and Schedule 4 require prescriptions, scheduled-medicine orders and related regulated documents to comply with medicine-control rules, including legally compliant electronic-agent and signature workflows before issue or transmission.
Basic Conditions of Employment Act 75 of 1997: section 23 medical certificates	Clause 23 and Schedule 4 require sick notes and medical certificates to be issued only on an adequate clinical basis and signed through a legally compliant workflow before issue or transmission.
Employment Equity Act 55 of 1998: medical testing and employee health information	Clause 11A, Schedule 1 and Schedule 8 create an occupational-health regime with practitioner gatekeeping, walled clinical records, employer-output limits and restrictions on medical testing and employer access to employee health information.
Promotion of Access to Information Act 2 of 2000: section 51 private-body manual	Clause 32 and Schedule 11 require the Company to publish and maintain a PAIA manual, route PAIA/POPIA requests to the Information Officer and include record categories, processing purposes, recipient categories, planned transborder flows and security-measure descriptions.
Mental Health Care Act 17 of 2002: mental-health confidentiality	Clause 16, clause 14A and Schedule 1 require mental-health status and mental healthcare records to be handled under the MHCA confidentiality regime, POPIA, the National Health Act and professional duties, with need-to-know access and restrictions on representative, employer or third-party disclosure.
Occupational Health and Safety Act 85 of 1993 and medical-surveillance regulations	Clause 11A, Schedule 1 and Schedule 8 require occupational-health medical-surveillance records to follow the governing regulation, including 20-40 year or other prescribed retention periods depending on exposure/sector, with practitioner gatekeeping and walled employer access.
Medical Schemes Act 131 of 1998 and Council for Medical Schemes complaints	Clause 30 recognises scheme/funder/claims dispute routes, including internal scheme/funder processes and escalation to the Council for Medical Schemes where applicable.
POPIA section 69 and CPA direct-marketing rules	Clause 24A and Schedule 1 distinguish Service Messages from Direct Marketing, require opt-in/soft opt-in only where permitted, honour opt-outs, maintain suppression lists and prohibit health-data-based marketing without specific lawful consent and special-information authorisation.