HEROMED PRIVACY NOTICE

Effective date: 20 July 2026 | Version: 1.0

Service provider: HeroMed (Pty) Ltd | Principal operating location: Johannesburg, South Africa

Corporate and tax registration details are available through HeroMed's official company records and invoices.

This is HeroMed's current approved Privacy Notice. It explains HeroMed's role, the information processed, the safeguards applied and the responsibilities that remain with each Client when using the Service.

1. Purpose

1.1 This Privacy Notice explains how HeroMed collects, uses, shares, protects, retains and processes personal information, health information and practice information in connection with the HeroMed platform, website, services, support, integrations, billing, AI features and related activities. HeroMed is committed to handling information responsibly and in accordance with the privacy and data-processing obligations applicable to HeroMed's role.

1.2 This Notice is global-facing and may apply alongside South African POPIA, Australian privacy laws, GDPR/UK GDPR or other privacy laws depending on the location and role of HeroMed, the Client, users, patients and service providers.

1.3 HeroMed is built to support healthcare and regulated practice workflows. HeroMed applies a role-based and risk-based approach to privacy and data handling, recognising that requirements vary by jurisdiction, client type, feature, configuration and use case. HeroMed may make standard product-specific, data-processing, security or jurisdiction-specific terms available for certain regions, client categories, data types or features. Clients remain responsible for ensuring that their own use of the Service, patient notices, consents, workflows and local compliance obligations are appropriate for their practice and jurisdiction.

2. Roles

2.1 For Patient Data and practice records submitted by a Client, the Client is generally the responsible party/controller and HeroMed acts as operator/processor on the Client's instructions.

2.2 For HeroMed account, billing, website, support, security, marketing, platform administration, fraud-prevention and business operations data, HeroMed may act as responsible party/controller.

2.3 HeroMed does not generally collect Patient Data directly from patients for its own independent purposes. Patient Data is usually entered, uploaded, generated or controlled by the Client.

3. Information processed

- identity and contact details, including names, email addresses, phone numbers, addresses and identifiers;
- practice, provider, registration, user, staff, referral and administrator details;
- patient, clinical, treatment, appointment, consent, emergency contact and billing information;
- medical aid, insurer, claim, tariff, remittance, ICD, procedural, modifier, NAPPI and payment information;
- clinical notes, uploaded documents, images, forms, signatures, messages, transcripts, recordings and attachments;
- support tickets, emails, calls, chats, feedback, complaints and service communications;
- billing, subscription, payment, invoice, credit, token, usage and transaction information;
- technical, device, browser, IP address, log, cookie, analytics, security and usage information;
- AI prompts, inputs, outputs, edits, approvals, classifications, summaries and related usage information.

4. Sources of information

4.1 HeroMed may receive information from Clients, users, patients acting through Clients, forms, imports, uploaded files, support requests, integrations, medical schemes, switching providers, payment processors, communication providers, public sources and service providers.

4.2 The Client is responsible for ensuring that information submitted to HeroMed is collected lawfully, accurate where required, and supported by appropriate notices, consents, authorisations or other lawful bases.

5. Purposes of processing

- providing, operating, securing, maintaining, supporting and improving the Service;
- creating accounts, managing users, permissions, subscriptions, billing and payments;
- processing practice, patient, appointment, clinical, claim, communication and billing workflows;
- supporting AI, automation, transcription, extraction, summarisation and workflow assistance features;
- integrating with communication, payment, hosting, medical scheme, EDI, accounting, analytics and support providers;
- detecting abuse, fraud, security incidents, errors, downtime and technical issues;
- communicating service, billing, legal, product, support and administrative updates;
- complying with legal, tax, accounting, regulatory, dispute, audit and enforcement obligations;

- using aggregated, anonymised or de-identified data for analytics, security, benchmarking, product development and service improvement where individuals are not reasonably identifiable.

6. Lawful bases and special-category information

6.1 The lawful basis for processing depends on the context and may include performance of contract, Client instruction, consent where required, compliance with law, legitimate interests, protection of rights, security, and the provision or administration of healthcare-related services by the Client.

6.2 Patient Data and health information may be sensitive or special-category information. The Client remains responsible for the lawful basis, notices, consent, professional obligations and patient-facing compliance required for Client-controlled Patient Data.

6.3 Where HeroMed acts as processor/operator, HeroMed processes Client-controlled Patient Data on documented instructions from the Client, except where law requires otherwise or where processing is reasonably required to secure, support, administer or protect the Service.

7. AI and automation privacy

7.1 HeroMed may use AI, machine learning, transcription, extraction, classification, summarisation, drafting and automation tools as part of the Service.

7.2 HeroMed will not knowingly submit identifiable Patient Data or Client confidential information to consumer AI tools that use prompts, inputs or outputs to train public or general-purpose models, unless expressly authorised by the Client.

7.3 HeroMed may use business, enterprise, API-based or cloud AI providers and may process prompts, inputs, outputs, transcripts, approvals, edits and usage logs for support, billing, quality, audit, security, dispute and product-improvement purposes.

7.4 HeroMed may use anonymised, aggregated or de-identified information to improve the Service, analytics, security, workflow performance and product functionality, provided the information is not reasonably capable of identifying a patient, Client or practice.

7.5 AI, clinical-safety, automated-decision and medical-device frameworks vary by jurisdiction and by use case. HeroMed does not make feature-specific or jurisdiction-specific certification claims for AI Features unless HeroMed expressly publishes or agrees those claims for the relevant feature or arrangement.

8. Marketing and communications

8.1 HeroMed may send service, account, billing, product, security, legal and administrative communications to Clients and users.

8.2 HeroMed may send marketing or product communications where permitted by law. Recipients may opt out of marketing communications through available unsubscribe or official contact channels. Opting out of marketing does not stop important service, legal, billing or security communications.

8.3 HeroMed does not sell Patient Data and does not use identifiable Patient Data for third-party marketing.

9. Sharing information

9.1 HeroMed may share information with service providers, sub-processors, payment processors, hosting providers, AI providers, transcription providers, communication providers, support tools, analytics tools, backup providers, security providers, professional advisers, insurers, regulators, courts, law enforcement, medical scheme or EDI providers, and other parties where required to provide the Service, comply with law, protect rights, process payments, prevent fraud or support integrations requested by the Client.

9.2 HeroMed may disclose information where it believes in good faith that disclosure is necessary to comply with legal requirements, respond to lawful requests, enforce agreements, protect the Service, investigate abuse, prevent harm or manage disputes.

10. Sub-processors and third-party services

10.1 HeroMed may use reputable sub-processors and third-party providers to provide hosting, infrastructure, AI, transcription, communications, payments, support, analytics, backups, security and integrations. HeroMed uses reasonable care in selecting and managing material providers relevant to the operation of the Service.

10.2 Third-party services may have their own terms, privacy practices, availability limits, processing locations, sub-processors, security controls and change processes. These may change from time to time outside HeroMed's direct control.

10.3 HeroMed may provide information about material sub-processors through its website, documentation, support channels, data-processing terms or other reasonable means where legally required or reasonably necessary. HeroMed may add, replace or change providers as reasonably required to operate, support, secure or improve the Service. Unless applicable law or a signed agreement requires otherwise, ordinary provider changes do not require individual Client approval, and HeroMed is not required to publish a live supplier register or disclose security-sensitive, confidential or commercially restricted information.

11. Cross-border processing

11.1 Information may be hosted, stored, accessed, supported, backed up or processed in South Africa, Australia, the United States, the United Kingdom, the EEA or other jurisdictions where HeroMed or its providers operate.

11.2 HeroMed will take reasonable steps to apply contractual, technical and organisational safeguards designed to provide appropriate protection for cross-border processing, taking into account the nature of the Service, the data involved, the providers used and the purpose of the processing.

11.3 Cross-border processing may be supported by applicable law, binding agreements, data-processing terms, standard contractual clauses, UK transfer mechanisms, adequacy decisions, consent, necessity or other lawful transfer mechanisms.

11.4 Where Australian privacy laws apply, HeroMed will take reasonable steps appropriate to its role to support overseas handling of personal information consistently with applicable privacy obligations, unless an exception applies or the Client's own use, instructions, integrations or jurisdictional requirements require otherwise.

11.5 The Client remains responsible for ensuring that its use of the Service complies with local laws applicable to the Client, its patients, users, practice, consents, notices and jurisdiction.

11.6 Where a Client uses the Service from a jurisdiction that imposes additional transfer, localisation, consent, registration, representative or documentation obligations, the Client remains responsible for assessing those obligations and notifying HeroMed before submitting affected data where HeroMed action is required. Bespoke data residency, local hosting, local representatives, transfer impact assessments or jurisdiction-specific compliance programmes are outside the standard Service unless required by applicable law or expressly agreed by HeroMed.

12. Security

12.1 HeroMed maintains risk-based technical and organisational safeguards designed to protect information and support the secure operation of the Service. These safeguards may include access controls, secure hosting, backups, monitoring, permissions, supplier controls and operational security practices appropriate to the nature and scale of the Service.

12.2 Security controls are risk-based and may change over time. No system is completely secure. The Client must maintain secure devices, user controls, passwords, staff practices, network security, cyber insurance and internal policies appropriate to its own practice.

12.3 Security controls, provider arrangements and technical practices may evolve as technology, risk, law and operational requirements change. References to particular safeguards, providers or practices are descriptive and do not create a fixed security specification, warranty, certification commitment, audit commitment or obligation to maintain any particular tool, provider, architecture or control unless expressly included in applicable product or security terms.

12.4 Where HeroMed makes sensitive information available outside the main Service environment for support, export, onboarding, migration or communication purposes, HeroMed may apply reasonable protection measures. The Client must handle downloaded, exported or externally shared data securely once it leaves the Service environment.

13. Security incidents

13.1 If HeroMed becomes aware of a confirmed security compromise materially affecting Client Data, HeroMed will use reasonable efforts to assess the issue, reduce further risk where reasonably possible, preserve relevant information where practical, and communicate with affected Clients through appropriate channels where required by applicable law or reasonably necessary in the circumstances. Information may be provided progressively and updated as the investigation develops. Preliminary information may be incomplete and does not create a guarantee regarding the timing, format or completeness of incident communications.

13.2 Where the Client is the responsible party/controller, the Client remains responsible for notifications to patients, regulators or third parties unless applicable law requires HeroMed to notify directly. HeroMed may provide reasonable assistance where legally required and technically feasible, subject to verification, security, available information and reasonable fees for bespoke assistance.

14. Retention and deletion

14.1 HeroMed applies retention practices intended to support the Service, lawful record keeping, security and operational continuity. Information may be retained for as long as reasonably required for the Service, legal compliance, accounting, tax, billing, security, dispute, fraud-prevention, backup, audit and operational purposes.

14.2 After termination, HeroMed may retain Client Data for a limited transition period and may then delete, archive or anonymise production data, subject to backups, legal retention, accounting, dispute, security, fraud-prevention, audit and operational requirements.

14.3 HeroMed does not promise immediate or absolute deletion from all backups, logs, archives or third-party systems where retention is technically, legally or operationally required.

15. Access, correction and privacy rights

15.1 Depending on applicable law and context, individuals may have rights to request access, correction, deletion, objection, restriction, export, withdrawal of consent, complaint review or information about processing.

15.2 Requests must be submitted through the official contact details published on the HeroMed website or within the Service. HeroMed may require identity, authority, account and jurisdiction verification before actioning a request.

15.3 Where a request relates to Patient Data controlled by a Client, HeroMed may redirect the requester to the relevant Client or require the Client's instruction before acting.

15.4 HeroMed may refuse, limit or delay a request where permitted by law, including where a request is unauthorised, unverifiable, excessive, technically impractical, conflicts with legal obligations, compromises security, affects another person's rights, or relates to records controlled by a Client.

16. Cookies and website information

16.1 HeroMed may use cookies, analytics, pixels, logs and similar technologies to operate the website and Service, remember preferences, support login, measure usage, improve performance, detect fraud, secure the Service and support marketing where permitted.

16.2 Users may manage cookies through browser settings, but some website or Service functionality may not work properly without cookies. Where legally required, HeroMed may use cookie notices, preference tools or consent mechanisms.

17. External links

17.1 The HeroMed website or Service may link to third-party websites, resources, forms, portals, documentation or services. HeroMed is not responsible for third-party content, security, privacy practices, terms or conduct.

18. Children, minors and vulnerable persons

18.1 The Service is not directed to children for HeroMed's own marketing purposes. Where a Client uses the Service for minors, dependants or vulnerable persons, the Client remains responsible for lawful authority, consent, notices, professional obligations and patient-facing compliance.

19. South Africa POPIA information

19.1 Where POPIA applies, HeroMed processes personal information in accordance with the lawful bases and conditions recognised under POPIA, including Client instruction, contractual necessity, legal compliance, legitimate interests, consent where required, and protection of rights or security.

19.2 South African data subjects may submit POPIA access, correction, deletion, objection or complaint requests through the official contact details published on the HeroMed website or within the Service.

19.3 South African data subjects may also lodge a complaint with the Information Regulator using the current contact details published by the Information Regulator.

19.4 HeroMed will consider privacy complaints and requests submitted through official channels, may require verification, and may redirect Patient Data requests to the relevant Client where the Client is responsible party/controller.

20. South Africa PAIA information and manual

20.1 This section is intended to operate as HeroMed's consolidated PAIA information and public access manual for purposes of the Promotion of Access to Information Act, 2000, to the extent permitted by law. It should be read together with the rest of this Privacy Notice, the HeroMed Terms and Conditions, any applicable data-processing terms and the official contact details published on the HeroMed website or within the Service.

20.2 HeroMed is a private body for PAIA purposes unless a specific record is treated differently under applicable law. The fact that a category of record is listed in this Notice does not mean that any requester has an automatic right to access that record. Access remains subject to PAIA, POPIA, applicable privacy laws, confidentiality obligations, privilege, security, third-party rights, Client-controlled Patient Data, commercial sensitivity and any lawful ground of refusal.

20.3 The HeroMed Information Officer and authorised privacy, POPIA and PAIA contacts are available through the official contact details published on the HeroMed website or within the Service. PAIA and privacy requests must be submitted through those official channels. HeroMed may require the requester to use the prescribed PAIA form or another reasonable process, provide sufficient detail to identify the requester and requested record, identify the right being exercised or protected where required, provide proof of identity and authority, and pay prescribed or reasonable request, search, preparation, copying, transfer or access fees where permitted by law.

20.4 HeroMed may hold records in categories including company, governance and statutory records; contracts, order forms, subscriptions, invoices and payment records; Client account, user, support and service records; software, product, security, technical and operational records; supplier, sub-processor and integration records; tax, accounting and audit records; employment, contractor and professional-adviser records; website, marketing and communication records; legal, insurance, dispute and compliance records; and Client Data processed through the Service.

20.5 Client Data and Patient Data are generally controlled by the relevant Client. Where a PAIA or privacy request relates to records controlled by a Client, patient records, clinical records, billing records, practice records or data submitted by or on behalf of a Client, HeroMed may redirect the requester to the relevant Client, require the Client's instruction, verify authority, refuse or limit access where permitted by law, or provide only such assistance as is legally required and technically feasible.

20.6 Records may also be available, retained or processed under laws or regulatory frameworks applicable to HeroMed or its Clients, including company, tax, accounting, labour, electronic communications, consumer protection, data protection, access to information, cybercrime, healthcare, medical scheme, billing, professional and contractual obligations. This does not mean that all such records are held by HeroMed or are accessible under PAIA.

20.7 HeroMed may refuse, limit, redact, defer, condition or charge for access to records where permitted by law, including where disclosure would affect another person's privacy, reveal confidential or commercially sensitive information, compromise security, disclose privileged information, prejudice legal proceedings or investigations, impose an unreasonable or disproportionate burden, disclose third-party information, conflict with Client instructions or professional obligations, or relate to records that HeroMed does not control.

20.8 Where access is granted, HeroMed may provide records in a format reasonably determined by HeroMed, subject to technical feasibility, security, identity and authority verification, Client instruction where applicable, payment of permitted fees and protection of third-party rights. HeroMed is not required to create new records, answer general questions, compile bespoke reports, perform analysis, reconstruct deleted information, provide system access, disclose security-sensitive information or provide operational assistance beyond what PAIA or applicable law requires.

20.9 This consolidated PAIA section is made available electronically through HeroMed's website or Service and may be updated from time to time. Prescribed PAIA forms, guidance and fee information may be obtained from the Information Regulator or through official regulatory channels. Requesters should ensure they use the current prescribed form and process applicable at the time of the request.

21. Changes to this Notice

21.1 This Notice is HeroMed's current approved Privacy Notice from the Effective Date and replaces prior website versions to the extent applicable. HeroMed may update this Notice from time to time by publishing an updated version or notifying Clients where reasonably appropriate. Continued use of the Service after publication or notice indicates acceptance of the updated Notice where permitted by law.

22. Contact

22.1 HeroMed will maintain current official contact channels on its website or within the Service. Formal privacy, POPIA, PAIA, data-access, correction, deletion, complaint and security requests must be submitted through the applicable official channel. The HeroMed Information Officer and authorised contacts are available through those channels.

22.2 Personal contact details of individual staff, founders, directors or contractors must not be used for formal privacy, POPIA or PAIA requests unless HeroMed expressly publishes them for that purpose.