National Healthcare Group

AFFORDABLE · RELIABLE

PRIVACY POLICY

National Health Group (Pty) Ltd
2nd Floor, PPS Centurion Square, Cnr Heuwel Road and Gordon Hood Road, Centurion, 0046
info@nationalhealthcare.co.za www.nationalheathcare.co.za

WhatsApp +27 72 815 8226
Tel: +27 86 000 2402

National Health Group (Pty) Ltd (2015/130345/07), a registered Managed Care Organisation (MCO110) and Administrator (ADMIN72)
Directors: R Nauta (Executive Chairman), M Moyo (Channel Partner Executive), A Odendaal (Chief Executive Officer)
L Motlana (Non-Executive), T van den Berg (Non-Executive), K Starke-Dow (Alternate)

Reg No 2015/130345/07
National Health Group (Pty) Ltd

Privacy Policy	
This encompasses all privacy issues relating to POPIA	
Author:	**Linda Motaung**
Creation date:	01/08/2021
Revision date:	01/11/2026
Doc. Ref.:	Privacy Policy – NHG V2.0
Version:	2.0

Changelog

Version	Date	Author	Description
1.0	01/08/2021	Linda Motaung	First version.
2.0	01/11/2026	Tiffanie Rodger	Updated for amended POPIA Regulations (2025), new Information Regulator details, retention, cross-border, rights and deletion.

PRIVACY POLICY

National Health Group (Pty) Ltd, trading as National Healthcare Group ("the Group"), recognises the importance of protecting personal information and the constitutional right of its members to have their personal information kept private, confidential and used only for lawful purposes. As prescribed in the Protection of Personal Information Act 4 of 2013 (POPIA) and its Regulations, as amended on 17 April 2025, the National Healthcare Group adheres to all data protection laws and has implemented safeguards to keep the personal information of its members safe from unauthorised access.

Please read this Privacy Policy carefully to understand how your personal information will be handled by National Healthcare Group.

1. ABOUT THE GROUP

National Health Group (Pty) Ltd is a legally registered Managed Care Organisation and Healthcare Administrator, accredited by the Council for Medical Schemes, that provides affordable primary healthcare services to low-income employer groups, insurers and the medical scheme industry. Our services include benefit administration, managed care, a national network of healthcare providers and digital healthcare services, including consultations with nurses and doctors by WhatsApp and telephone. The Group is subject to the laws of South Africa that govern healthcare service providers and adheres to the ethical rules that protect the privacy and confidentiality of its members' personal information.

Contact details of the Group:

Company name:	National Health Group (Pty) Ltd, trading as National Healthcare Group
Registration number:	2015/130345/07
Physical address:	PPS Centurion Square, Corner Heuwel & Gordon Hood Roads, Centurion, 0046
Postal address:	**Postnet Suite 203, Private Bag X8, Elarduspark, 0047**
Telephone:	021 276 5600
Customer care:	0860 002 402 nhgcustomercare@nationalhealthcare.co.za
WhatsApp:	072 815 8226
Compliance e-mail:	compliance@nationalhealthcare.co.za
Website:	www.nationalhealthcare.co.za

2. INFORMATION OFFICER

Our Information Officer is registered with the Information Regulator and is responsible for our compliance with POPIA and the Promotion of Access to Information Act 2 of 2000 (PAIA).

Information Officer:	Adriaan Odendaal, Chief Executive Officer
Deputy Information Officer:	Mandlenkosi Moyo, Channel Partner Executive
E-mail:	compliance@nationalhealthcare.co.za
Telephone:	0860 002 402

3. DEFINITION OF TERMS

3.1 **"Data subject"** refers to the person (e.g., member or dependant) or entity to whom the personal information relates.

3.2 **"Personal information"** has the meaning assigned to it in POPIA and refers to information relating to an identifiable, living person and, where applicable, an existing juristic person. It includes information such as race, gender, pregnancy, age, health status and medical information, date of birth, identity number, contact details and confidential correspondence.

3.3 **"Special personal information"** includes information about a person's health, sex life, race or ethnic origin, religious or philosophical beliefs, trade union membership, political persuasion, biometric information and criminal behaviour. Most health information we process is special personal information.

3.4 **"Processing"** has the meaning assigned to it in POPIA and refers to any operation or activity concerning personal information, such as the collection, receipt, recording, storage, updating, alteration, use, distribution, erasure or destruction of the information.

3.5 **"Responsible party"** means the person or body that decides why and how personal information is processed. **"Operator"** means a person who processes personal information for a responsible party under a contract, without coming under its direct authority.

3.6 **"POPIA / POPI Act"** means the Protection of Personal Information Act 4 of 2013 and the Regulations relating to the Protection of Personal Information, 2018, as amended on 17 April 2025 ("the Regulations").

3.7 **"Information Regulator"** means the Information Regulator (South Africa) established under section 39 of POPIA.

3.8 **"We" / "us" / "the Group"** refers to National Health Group (Pty) Ltd (NHG), trading as National Healthcare Group.

3.9 **"Member" / "You" / "Customers"** refers to the data subject whose personal information is processed by the Group, including the dependants of a member.

3.10 **"Republic"** refers to the Republic of South Africa.

4. APPLICATION OF THE PRIVACY POLICY

This Privacy Policy applies to personal information that we have in our possession or under our control and personal information that we collect from or about our members, whether in person, on paper, by telephone, e-mail, SMS, WhatsApp, our website or any other digital channel. It sets out how we collect the information, the type of information collected, why it is collected, when it will be shared with others, the security measures that protect it, how long we keep it, and how you may access, correct or delete it.

5. OUR ROLE: RESPONSIBLE PARTY AND OPERATOR

We often administer healthcare benefits on behalf of a medical scheme, insurer or employer. In those cases, that scheme, insurer or employer is usually the responsible party for your personal information, and we process it as their operator in terms of our written agreement with them. Where we provide services to you directly, for example through our clinical line, WhatsApp service or website, we are the responsible party.

This affects some of your requests. If you ask us to delete information that we hold on behalf of a scheme, insurer or employer, we will refer the request to them and tell you that we have done so. We will help you exercise your rights in either case.

6. OUR COMMITMENT

We are committed to conducting our business lawfully in accordance with the privacy laws of the Republic and the eight conditions for lawful processing in POPIA. We will only process our members' personal information in accordance with the law to provide contracted healthcare services, and we will always keep it confidential.

We apply the following principles to protect our members' privacy:

- We only collect the personal information that is necessary;
- We only use personal information for the purposes specified in this Privacy Policy;
- We do not keep personal information longer than needed for lawful purposes;
- We keep personal information accurate and allow members to correct or delete it;
- We protect personal information with appropriate security safeguards; and
- We only share our members' personal information as specified in this Privacy Policy and as permitted in terms of the law.

7. COLLECTION OF PERSONAL INFORMATION

The Group collects personal information from employer groups, insurers and medical schemes as part of carrying out its contractual duties. The Group also collects personal

information directly from members when they register, use our clinical line or WhatsApp service, speak to our call centre, visit a network provider, or supply information on our website or social media platforms. Telephone calls may be recorded for quality, training and record-keeping purposes, and we will tell you when a call is recorded.

Personal information may also be collected from other sources when it is not possible to obtain it directly from members, or to protect their legitimate interests in the provision of healthcare. These sources include next-of-kin, treating healthcare practitioners and network providers (such as doctors, pharmacies, pathology and radiology practices), and publicly available sources.

Where we collect information about a child (for example a dependant under 18), we do so with the consent of a competent person, usually a parent or legal guardian, or where the law otherwise permits.

8. PROCESSING OF YOUR PERSONAL INFORMATION

Various laws permit the processing of personal information in the provision of healthcare services, including the National Health Act 61 of 2003, POPIA and the Medical Schemes Act 131 of 1998. Section 32 of POPIA allows medical schemes, insurers, medical scheme administrators and managed healthcare organisations to process health information where it is necessary for risk assessment, the performance of an insurance or medical scheme agreement or the enforcement of contractual rights. Health professionals and healthcare institutions may process health information where it is necessary for proper treatment and care.

We process the personal information listed below, if applicable in the circumstances, and retain it as part of our records:

8.1 **Records relating to the formation of the company:**

Documents related to the establishment of the company, CIPC documents, memorandum of incorporation, directors' and shareholders' records as required in terms of the Companies Act 71 of 2008; shareholders' agreement; shareholders' register; other statutory records; governance documents (e.g., company policies, minutes of meetings) and other related documents.

8.2 **Employment records:**

Employment contracts; conditions of employment and workplace policies; skills development plans and training records; salary register; relevant tax records; leave records; medical scheme membership records; pension and provident fund records; performance indicators and other correspondence. Relevant medical, disability and

occupational health information may be collected to care for employees and to meet health and safety obligations.

In the case of job applicants, the Group collects information such as titles, identity numbers, dates of birth, contact details, addresses, HPCSA / statutory council numbers, nationality, gender, race, qualifications, specialisation, vetting results and other information included in CVs. This information is destroyed if the applicant is not appointed, unless the applicant agrees that we may keep it. For successful applicants, the details form part of the employee file.

8.3 **Health administration records:**

Member and dependant details; medical records; photographs; healthcare benefits; consultation records and chat histories from our clinical line, WhatsApp and telephonic services; patient communication; names and contact details of next-of-kin; premium, billing and payment details; claim-related information such as procedures performed, treatment provided, medicine dispensed and relevant reports (e.g., radiological images and reports, pathology results); and other information on health-related services.

8.4 **Referral records:**

Doctor referral notes and other relevant reports.

8.5 **Clinical trial / research studies records:**

No records are kept by the Group related to clinical trials / research studies.

8.6 **Health and safety records:**

Health and safety reports and other regulatory compliance records required by law.

8.7 **Financial records:**

Financial statements; auditors' reports; accounting records; bank statements; invoices, statements and receipts; remittance advices; tax returns and related documentation.

8.8 **Records related to assets:**

Asset register; purchase records; licences; financing and lease agreements; sale and purchase agreements; delivery notes and orders.

8.9 **Agreements:**

Agreements and related documentation with service providers, contractors, consultants, suppliers, vendors, medical schemes, insurers, employer groups, network providers and other business-related agreements.

8.10 **Public and private body (e.g., regulators and medical schemes) records:**

Official accreditation documents; benefit schedules and other healthcare administration correspondence.

8.11 **Insurance records (including professional indemnity cover):**

Policies, cover, claims and related records.

9. CONSENT

Much of our processing is based on our contracts with employer groups, insurers and medical schemes, on our legal obligations and on section 32 of POPIA, rather than on consent alone. Where we rely on your consent, for example for direct marketing or optional services, you may withdraw it at any time by contacting us through any of the channels in section 1. Withdrawal does not affect processing that has already occurred, or processing that we may lawfully continue on another ground. If withdrawing consent means we can no longer provide a service, we will explain this to you.

10. OBJECTION TO PROCESSING

When we process personal information, it is to promote our members' healthcare interests and to ensure that their benefits are accessed and processed according to the relevant rules. You may object to our processing on reasonable grounds, and you may object at any time to processing for direct marketing.

Objections are free of charge. You may object using a form substantially similar to Form 1 of the Regulations, which is available from our Information Officer and the Information Regulator, or by hand, post, e-mail, SMS, WhatsApp or telephone. If you object by telephone, we will record the call and make the recording available to you. Should we agree with the objection, your personal information will only be processed as provided for in the law.

11. DIRECT MARKETING

We will only send you electronic direct marketing (for example by SMS, e-mail or WhatsApp) if you are an existing member and the marketing relates to similar products or services, or if you have given us your specific consent. An opt-out process on its own does not constitute consent. Every marketing message will tell you how to unsubscribe, free of charge, and we will act on your request promptly. Service messages about your cover, claims or consultations are not direct marketing.

12. PURPOSES OF PROCESSING YOUR PERSONAL INFORMATION

All information that the Group collects is collected to provide healthcare services in terms of our contractual agreements and the law. The information is used to:

- administer the contracted healthcare service, including membership, premiums and claims;

- provide managed care services, including clinical consultations by WhatsApp, telephone and in person;
- provide relevant information to a contracted third party, such as a network provider, who needs it to provide a healthcare service to members and beneficiaries;
- communicate with members about their cover, benefits, consultations and claims;
- detect and prevent fraud, waste and abuse;
- maintain quality, including recording calls and reviewing consultations for training and quality assurance;
- report to persons and bodies, as required and authorised in terms of the law or by the data subjects;
- manage employment and contracting matters relating to the Group's employees;
- support law enforcement structures, courts and tribunals where the law requires it;
- produce statistics and reports using de-identified information; and
- pursue any other lawful purpose related to the activities of the Group.

13. DISCLOSURE OF YOUR PERSONAL INFORMATION

We will share only relevant personal information about our members with our business partners if it is necessary and lawful in the provision of healthcare services. We share this personal information with service providers that help with our business activities, including benefit management, claims processing, payments and refunds, messaging and communication platforms, cloud hosting and IT support, and other healthcare administration services. We require these service providers, by written agreement, to keep our members' personal information secure and to use it only to provide services on our behalf.

We do not sell personal information or provide it to third parties for their independent use. As a healthcare administrator and managed care organisation, we do share personal information with the medical schemes, insurers and employer groups that we contract with, and with network providers, where the information is required to provide the healthcare service.

14. RECORD-KEEPING AND RETENTION

We keep personal information only for as long as we need it for the purpose for which it was collected, or for as long as the law, a contract or our legitimate interests require. Health records must be kept for longer periods under professional and legal rules. The main retention periods are set out below.

Record type	Minimum retention period	Source
Clinical and health records (including WhatsApp, telephonic and virtual consultation notes)	At least 6 years from the date the record became dormant (inactive)	HPCSA Booklet 9; National Health Act 61 of 2003
Health records of minors	Until the minor's 21st birthday, or 6 years after dormancy if longer	HPCSA Booklet 9
Health records of patients who are mentally incompetent	For the patient's lifetime	HPCSA Booklet 9
Occupational illness and injury records	20 years after treatment	Occupational Health and Safety Act 85 of 1993; HPCSA Booklet 9
Membership, benefit and claims administration records	For the period required by the contracting medical scheme, insurer or employer, and at least 5 years	Client contracts; Tax Administration Act 28 of 2011
Financial, premium, billing and tax records	5 years from submission of the relevant return	Tax Administration Act 28 of 2011, s29
Company and accounting records	7 years	Companies Act 71 of 2008, s24
Employee records	3 years after termination (longer where tax, pension or OHS law requires)	Basic Conditions of Employment Act 75 of 1997, s31
Unsuccessful job applications	Destroyed once the recruitment process ends, unless the applicant consents to longer retention	POPIA s14
Call recordings and chat logs that are not clinical records	**12 months**	POPIA s14; quality assurance
Direct marketing consent and opt-out records	For as long as we market to the person, plus 3 years	POPIA s69; proof of consent

When a retention period ends, we destroy or delete the information, or de-identify it so that it can no longer be linked to you, in accordance with our Data Deletion Policy and Procedure.

15. Information Sent Across the Borders of the Republic of South Africa

We primarily process and store our members' information in the Republic. Some of our service providers, including cloud hosting and messaging platforms such as WhatsApp, may store or process information on servers outside the Republic. We will only transfer personal information outside the Republic in accordance with section 72 of POPIA, namely where the recipient is subject to a law, binding corporate rules or a binding agreement that provides an adequate level of protection, where you consent, or where the transfer is necessary for the performance of a contract with you or in your interest.

Members living or travelling outside the Republic may need their personal information transferred to treating providers in another country. This will be done with the member's consent and within the boundaries of the relevant privacy laws.

16. SECURITY OF YOUR PERSONAL INFORMATION

We take appropriate, reasonable technical and organisational measures to protect personal information from loss, damage, unauthorised destruction and unlawful access or processing. These include access controls and passwords, encryption, secure hosting, regular back-ups, monitoring for security risks, physically secured offices and locked storage for paper records. We regularly review and update these safeguards in line with generally accepted information security practices.

Only employees and service providers who need access to member information to perform their functions are granted access. Our employees, suppliers and operators have signed agreements or undertakings to keep information confidential, apply appropriate security measures and process it only for the agreed purposes.

If we have reasonable grounds to believe that your personal information has been accessed or acquired by an unauthorised person, we will notify the Information Regulator through its eServices Portal and notify you in writing as soon as reasonably possible, as required by section 22 of POPIA. We will tell you what happened, what we are doing about it and what you can do to protect yourself.

17. YOUR RIGHTS

Subject to the law, you have the right to:

- be told that your personal information is being collected, and that it has been accessed or acquired by an unauthorised person;
- ask whether we hold personal information about you, and request access to it;
- ask us to correct, delete or destroy your personal information;
- object to the processing of your personal information on reasonable grounds, and object at any time to direct marketing;
- withdraw consent where we rely on consent;
- not be subject to a decision based solely on automated processing that has legal consequences for you, except as permitted by law; and
- lodge a complaint with the Information Regulator.

18. RIGHT TO ACCESS YOUR PERSONAL INFORMATION

On a reasonable request, and after we have verified your identity, you may ask us to confirm whether we hold personal information about you and request a copy of it, including the identity of third parties who have had access to it, subject to the restrictions in POPIA and PAIA. Requests for records should be made on PAIA Form 2 (Regulation 7 of the PAIA Regulations,

2021), which is available in our PAIA Manual, from our Information Officer and from the Information Regulator, and submitted to compliance@nationalhealthcare.co.za.

No request fee is payable when you ask for your own personal information. Reproduction fees prescribed under PAIA may apply, and we will tell you of any fee before we proceed. Please consult our PAIA Manual for further information.

19. Correction and Deletion of Your Personal Information

It is important that we always have accurate information about our members, as it could affect our services and communication. Please inform us as soon as any of your information changes.

You may ask us to correct or delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or to destroy or delete a record that we are no longer authorised to keep. Requests are free of charge. You may use a form substantially similar to Form 2 of the Regulations, or contact us by hand, post, e-mail, SMS, WhatsApp or telephone (telephone requests will be recorded). There must be sufficient detail to identify the information and the correction or deletion required.

Before we act on a request, we will verify that it comes from you or from a person authorised to act for you. We will respond in writing within 30 days of receiving your request, tell you what action we have taken, and, where the corrected information affects decisions about you, inform the persons to whom the information was disclosed.

We may not be able to delete all your information. We may lawfully keep information that we must retain by law (see section 14), that is needed to provide cover while your membership is active, or that is needed for a claim, dispute or investigation. In those cases, we will restrict the information so that it is only used for that purpose, and explain this to you. Our process is set out in our Data Deletion Policy and Procedure, and a member guide is available from customer care and on our website.

20. Website and Cookies

Our website may use cookies and similar technologies to make it work, to remember your preferences and to understand how it is used. You can control or disable cookies in your browser settings, but some parts of the website may then not work properly.

21. Changes to this Privacy Policy

National Health Group reserves the right, in its sole discretion, to revise or supplement this Privacy Policy from time to time to reflect changes in our business or the law. We will publish the updated Privacy Policy on our website, and it will be available at our offices. Any revised

version will be effective from the date it is posted on the website, so please refer to the website for the latest version.

If you have any questions concerning this Policy, please contact our Information Officer at compliance@nationalhealthcare.co.za.

22. Concerns and Complaints About the Processing of Your Personal Information

All enquiries, requests or concerns regarding this Policy or relating to the processing of personal information by the Group should be addressed to the Information Officer. We would appreciate the opportunity to respond to your concerns before you approach the Information Regulator. You may, however, lodge a complaint with the Information Regulator at any time:

Physical address:	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191
Postal address:	PO Box 31533, Braamfontein, Johannesburg, 2017
Telephone:	010 023 5200 / Toll-free: 0800 017 160
General enquiries:	enquiries@inforegulator.org.za
POPIA complaints:	POPIAComplaints@inforegulator.org.za or the eServices Portal
PAIA complaints:	PAIAComplaints@inforegulator.org.za (PAIA Form 5)
Website:	www.inforegulator.org.za

23. Laws Applicable to this Privacy Policy

This Privacy Policy is governed by the laws of the Republic of South Africa.