National Healthcare Group

AFFORDABLE · RELIABLE

DATA DELETION POLICY AND PROCEDURE

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

Data Deletion Policy and Procedure	
Deletion, destruction and restriction of personal information on request, in terms of POPIA	
Author:	**Tiffanie Rodger**
Creation date:	01/11/2026
Revision date:	–
Doc. Ref.:	Data Deletion Policy – NHG V1.0
Version:	1.0

DATA DELETION POLICY AND PROCEDURE

National Health Group (Pty) Ltd, hereinafter referred to as National HealthCare Group, respects the right of its members to ask for their personal information to be deleted. This Policy sets out when we delete personal information, when we must keep it, how we verify who is asking, and the steps every employee must follow so that a deletion request is handled lawfully, securely and within 30 days.

No personal information may be deleted, destroyed or restricted on request unless the requester's identity has been verified in terms of section 7 of this Policy.

1. PURPOSE

This Policy gives effect to section 24 of the Protection of Personal Information Act 4 of 2013 (POPIA) and regulation 3 of the Regulations relating to the Protection of Personal Information, as amended on 17 April 2025, which allow a data subject to request, free of charge, the correction, deletion or destruction of personal information. It also gives effect to section 14 of POPIA, which requires that records not be kept longer than necessary.

This Policy supports the Group's Privacy Policy (Version 2.0) and PAIA Manual (2026). The member-facing guide is attached as Annexure A, and standard messages as Annexure B.

2. SCOPE

This Policy applies to:

- all personal information of members, dependants, applicants, website and WhatsApp users and other data subjects held by the Group, in any format;
- all systems and records, including the administration and claims systems, clinical and consultation records, WhatsApp and SMS platforms, call recordings, e-mail, spreadsheets, paper files and back-ups;
- personal information held for the Group by operators (service providers), who must delete it on the Group's instruction; and
- all employees, contractors and clinical staff who receive or handle a deletion request.

Requests from employees about their own employment records follow the same principles and are handled by Human Resources with the Information Officer.

3. DEFINITION OF TERMS

3.1 **"Deletion"** means permanently removing personal information from a live system so that it cannot be retrieved in the ordinary course of business.

3.2 **"Destruction"** means permanently destroying a record, including shredding paper records and securely wiping electronic media.

3.3 **"De-identification"** means removing information that identifies the data subject, or could be used or manipulated to identify them, so that it can no longer be linked to them.

3.4 **"Restriction"** means marking and isolating personal information so that it is only stored and used for the purpose that requires it to be kept (for example a legal retention period or a dispute), and not for any other purpose, including marketing.

3.5 **"On-file contact details"** means the mobile number and e-mail address recorded on the member's profile before the request was received.

3.6 **"Privacy Desk"** means the employees designated by the Information Officer to log, verify and process data subject requests.

3.7 **"Legal hold"** means an instruction from the Information Officer that records must not be deleted because of a claim, complaint, dispute, investigation or legal proceedings.

4. LEGAL FRAMEWORK

- POPIA sections 5, 11, 14, 22, 23, 24, 32 and 72;
- Regulations relating to the Protection of Personal Information, 2018, as amended on 17 April 2025 (Form 2: Request for correction or deletion of personal information or destroying or deletion of record of personal information);
- Promotion of Access to Information Act 2 of 2000 and the PAIA Regulations, 2021;
- National Health Act 61 of 2003 and the HPCSA Guidelines on the Keeping of Patient Records (Booklet 9);
- Medical Schemes Act 131 of 1998, Tax Administration Act 28 of 2011, Companies Act 71 of 2008, Basic Conditions of Employment Act 75 of 1997 and Occupational Health and Safety Act 85 of 1993; and
- the Group's agreements with medical schemes, insurers and employer groups.

5. POLICY PRINCIPLES

5.1 **Requests are free and may be made through any channel**

A member may request deletion by e-mail, WhatsApp, SMS, telephone, post or in person. We offer Form 2 but must not refuse a request because it was not made on the form; the Privacy Desk completes the form on the member's behalf where needed. Telephone requests must be recorded and the recording kept with the request. No fee may be charged.

5.2 **When we delete**

We delete, destroy or de-identify personal information where it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or where we are no longer authorised to keep it under section 14 of POPIA.

5.3 **When we restrict instead of delete**

We may keep personal information, restricted to the purpose that requires it, where:

- a law or professional rule requires us to keep it (see the retention schedule in section 10);
- the member's cover is still active and the information is needed to provide cover or pay claims;
- it is needed for an open claim, complaint, dispute, fraud investigation or legal proceedings (legal hold);
- the medical scheme, insurer or employer that is the responsible party instructs us to keep it; or
- the member agrees that we may keep it.

5.4 **Active cover**

Full deletion is not possible while a member's cover is active, because we cannot administer cover or pay claims without the member's information. The Privacy Desk must explain the options: (a) cancel cover through the employer, insurer or scheme first and then request deletion; (b) delete optional information only, such as marketing preferences and non-clinical chat history; or (c) restrict processing. Marketing must stop immediately in every case.

5.5 **Information held on behalf of a scheme, insurer or employer**

Where the Group holds the information as an operator, the responsible party decides on deletion. The Privacy Desk must refer the verified request to the responsible party within 5 business days, tell the member that it has done so, and act on the responsible party's written instruction.

5.6 **Clinical records**

Clinical records, including WhatsApp, telephonic and virtual consultation notes, may not be deleted before the end of their retention period. They are restricted and destroyed when the period ends. Only the Information Officer, after consulting the Clinical Lead, may approve an exception.

5.7 **Back-ups**

Information deleted from live systems will not be restored from back-ups for any purpose other than disaster recovery. Back-ups expire on their normal cycle of 90 days. If a back-up is restored, deletions must be re-applied before the system goes live.

5.8 **Operators**

Operators that hold the member's information for the Group (for example messaging platforms, network providers, IT and cloud providers) must be instructed in writing to delete it and to confirm deletion within 10 business days.

5.9 **Proof of deletion**

We keep a minimal record of each request (reference number, name, policy number, date received, what was deleted, what was kept and why, and date completed) as proof of compliance. This record is kept for 5 years and used for no other purpose.

5.10 **No disclosure before verification**

Until a requester is verified, employees may not confirm whether the Group holds information about any person, or disclose any information.

6. WHO MAY REQUEST DELETION

- The member, for themselves and for dependants under 18;
- An adult dependant, for their own information only;
- A person with written authority from the member (for example a power of attorney), or a court-appointed curator; and
- The executor of a deceased member's estate, with letters of executorship and a death certificate.

Requests made by anyone other than the member are always handled under the enhanced verification standard in section 7.4.

7. IDENTITY VERIFICATION STANDARD

Deletion is permanent, so the verification standard is higher than for a routine query. The guiding rule is that a request must be proved by something the member has and something the member knows, and then confirmed by the member on a contact channel already on file.

7.1 **Why a WhatsApp message or ID number alone is not enough**

A request sent by WhatsApp from the mobile number on file is good evidence that the sender has the member's phone. It is not proof of identity on its own: phones are often shared within households, and a number can be taken over through SIM-swap fraud.

An identity number and date of birth are known to employers, family members and anyone who has seen the member's ID document, so they are weak on their own.

For this reason a WhatsApp request from the number on file counts as the "has" factor only, and is combined with the checks below. Clinical line staff may receive and log a deletion request, but must hand it to the Privacy Desk and may not action it.

7.2 Standard verification (all deletion and destruction requests)

All three steps must be completed and recorded:

Step	What the Privacy Desk does	Pass criteria
A. Possession	Confirms the request came from, or sends a one-time code to, the mobile number or e-mail address on file. Never sends a code to a new number or address supplied in the request.	Code returned correctly within 24 hours, from a contact detail on file for at least **30** days.
B. Knowledge	Asks three questions and checks the answers against the record: policy number, date of birth, and one item that is not printed on the ID or membership card (e.g. employer name, date of last consultation, or last premium amount).	All three answers correct. Two failed attempts move the request to enhanced verification.
C. Confirmation	Sends the member, on the on-file channel, a summary of what will be deleted, what must be kept and why, and the consequences (e.g. cover cannot continue).	Member replies "CONFIRM DELETE" within **10** business days. No reply: request closed and member informed.

7.3 Lower-risk requests

Opting out of marketing requires no verification and must be actioned immediately. Correcting contact details or deleting a single item of non-clinical information requires step A and two knowledge questions.

7.4 Enhanced verification

Enhanced verification applies where any of the following is present:

- the mobile number or e-mail on file was changed in the last **30** days, or a SIM swap is suspected;
- the request comes from a number or address that is not on file;
- the request is made on behalf of someone else, or concerns a deceased member;
- step A or B failed; or
- anything about the request seems unusual (for example urgency, pressure or inconsistent details).

Under enhanced verification the Privacy Desk must: call the member back on the number on file (never on a number supplied in the request); obtain a copy of the requester's identity document and, where relevant, proof of authority; and obtain the Information Officer's written

approval before deletion. ID copies obtained for verification are deleted once the request is closed.

8. PROCEDURE

Day 1 is the business day on which the request is received through any channel. The written response must be sent within 30 days of receipt.

Step	Action	Owner	Timeframe
1	Receive and log the request in the Data Subject Request Register with a reference number (DDR-YYYY-NNN). Record the channel; save the recording or message.	Any employee → Privacy Desk	Same business day
2	Acknowledge receipt on the channel used, quoting the reference number and the next steps (Annexure B, message 1).	Privacy Desk	Within 2 business days
3	Verify identity under section 7. If verification cannot be completed after two attempts over 10 business days, close the request and inform the member on the on-file channel.	Privacy Desk	Within 5 business days
4	Locate the information in every system on the checklist in section 9, including operators.	Privacy Desk with system owners	Within 10 business days
5	Assess what can be deleted and what must be restricted (section 5). Check for a legal hold, open claims or complaints, and whether NHG is the operator. Refer to the responsible party where required.	Information Officer or Deputy	Within 12 business days
6	Send the confirmation summary (step C, Annexure B, message 3) and wait for “CONFIRM DELETE”.	Privacy Desk	Within 15 business days
7	Delete, destroy, de-identify or restrict in each system. Instruct operators in writing.	System owners	Within 5 business days of confirmation
8	Quality check: a second person confirms that searches no longer return the member’s information (other than restricted records).	Privacy Desk (second person)	Before the response is sent
9	Send the written outcome: what was deleted, what was kept, why, when it will be destroyed, and the right to complain to the Information Regulator (Annexure B, message 4 or 5).	Privacy Desk, signed off by Information Officer	Within 30 days of receipt
10	Close the register entry and file proof of deletion.	Privacy Desk	On sending the response

If the 30-day deadline is at risk, the Privacy Desk must escalate to the Information Officer by day 20.

9. SYSTEMS CHECKLIST

Every deletion must be checked against each system below. System owners must keep this list up to date.

System or record	Typical personal information	Action on a verified deletion request
Membership and administration system	Member and dependant details, policy, premiums	Delete if cover has ended and retention has expired; otherwise restrict
Claims system	Claims, treatment and payment details	Restrict until retention period ends
Clinical and consultation records	Nurse and doctor notes, prescriptions, referrals	Restrict until retention period ends (section 5.6)
WhatsApp / messaging platform	Chat history, phone number, media	Delete non-clinical chats; clinical chats kept as clinical records; instruct platform provider
Telephony and call recordings	Recordings, call logs	Delete non-clinical recordings unless needed for a complaint or dispute
E-mail and CRM	Correspondence, tickets	Delete, except correspondence forming part of a retained record
Marketing lists (SMS, e-mail)	Contact details, preferences	Remove immediately; keep the opt-out flag so the member is not contacted again
Finance system	Debit orders, bank details, invoices	Restrict for 5 years for tax purposes, then delete
Reports and data warehouse	Extracts, analytics	Delete or de-identify
Paper files	Forms, letters	Shred, or restrict where retention applies
Operators and network providers	Information shared to provide services	Written instruction to delete; written confirmation within 10 business days
Back-ups	Copies of the above	Expire on normal cycle (section 5.7)

10. RETENTION SCHEDULE

The following minimum retention periods apply. When a period ends, the information is destroyed or de-identified without waiting for a request.

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

Record type	Minimum retention period	Source
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

11. Roles and Responsibilities

Role	Responsibility
Information Officer	Owns this Policy; approves deletions where an exception or enhanced verification applies; signs off responses; reports to the Board.
Deputy Information Officer	Acts for the Information Officer; assesses retention and responsible-party questions; manages the Request Register.
Privacy Desk	Logs, acknowledges, verifies and coordinates requests; sends responses; keeps proof of deletion.
Clinical line and customer care staff	Recognise a deletion request, log it and hand it to the Privacy Desk the same day. Do not delete, promise deletion or disclose information.
System owners (IT, Claims, Finance, Clinical)	Carry out deletion or restriction in their systems and confirm in writing.
Clinical Lead	Advises on clinical record retention and exceptions.

12. Records, Reporting and Training

- The Request Register records every request, channel, verification steps, decisions, dates and outcome.
- The Information Officer reports the number of requests, timeliness and any late responses to the executive committee.
- All customer care, clinical line and Privacy Desk staff are trained on this Policy at induction and annually.
- A sample of closed requests is checked each quarter to confirm that deletions were completed in every system.

13. COMPLAINTS

A member who is unhappy with the outcome may contact the Information Officer at compliance@nationalhealthcare.co.za, or lodge a complaint with the Information Regulator (POPIAComplaints@inforegulator.org.za or the eServices Portal at www.inforegulator.org.za).

14. REVIEW

This Policy will be reviewed annually, or sooner if POPIA, its Regulations, our products or our systems change.

ANNEXURE A: MEMBER GUIDE – HOW TO REQUEST DELETION OF YOUR PERSONAL INFORMATION

You have the right to ask us to delete your personal information. It is free. Follow the steps below.

1. Send us your request

Use any of these channels:

- **WhatsApp:** send “Delete my data” to **072 815 8226** from the mobile number registered on your policy.
- **E-mail:** nhgcustomercare@nationalhealthcare.co.za with the subject line “Data Deletion Request”.
- **Telephone:** 0860 002 402. Calls are recorded.
- **Post or in person:** PPS Centurion Square, Corner Heuwel & Gordon Hood Roads, Centurion, 0046

You may use the Information Regulator’s Form 2, but you do not have to. We will complete it for you.

2. Tell us who you are and what you want deleted

- Your full name;
- Your policy or membership number;
- The mobile number or e-mail address linked to your policy;
- Whether you want all your personal information deleted, or only specific information (for example marketing messages or chat history); and
- Whether the request includes your dependants under 18. Adult dependants must ask for themselves.

3. Confirm it is you

Before we delete anything, we must make sure the request comes from you:

- We will send a one-time code to the mobile number or e-mail address already on your policy.
- We will ask you a few security questions about your policy.
- Before we delete, we will send you a summary of what will be deleted and what we must keep. Reply “CONFIRM DELETE” to go ahead.

We will never ask for your banking PIN or passwords. We only ask for a copy of your ID if extra checks are needed, for example if your contact details changed recently or someone is asking on your behalf.

4. What happens next

- **Acknowledgement:** we confirm receipt within 2 business days and give you a reference number.
- **Outcome:** we reply in writing within 30 days of receiving your request.
- **Confirmation:** we tell you what was deleted, what we had to keep, why, and for how long.

Important things to know

- **Deletion is permanent.** Deleted information cannot be recovered.
- **Active cover:** we cannot provide cover or pay claims without your information. If you want all your information deleted, your cover must first be cancelled through your employer, insurer or medical scheme. We will explain your options.
- **Health records:** the law requires us to keep clinical records, including WhatsApp and telephone consultations, for at least 6 years (longer for children). We keep them securely, use them for nothing else, and delete them when the period ends.
- **Other legal records:** we must keep some financial and tax records for 5 years. They will never be used for marketing.
- **Your scheme or insurer:** if we hold your information on behalf of your medical scheme, insurer or employer, we will pass your request to them and let you know.
- **Marketing:** you can stop marketing messages at any time, straight away, without deleting anything else.

Need help?

For questions about your privacy rights or a request, contact our Information Officer at compliance@nationalhealthcare.co.za. If you are not satisfied, you may complain to the Information Regulator at POPIAComplaints@inforegulator.org.za or www.inforegulator.org.za.

ANNEXURE B: STANDARD MESSAGES

Adapt for the channel used. Do not include health information in any message.

Message 1 – Acknowledgement

Hi [Name]. We have received your request to delete your personal information. Your reference is [DDR-YYYY-NNN]. To protect you, we first need to confirm it is you. We will be in touch within 5 business days. National HealthCare.

Message 2 – Verification

Hi [Name]. To confirm your identity for request [ref], please reply with the 6-digit code we have just sent to your registered [mobile number / e-mail], your policy number and your date of birth. We will also ask one more security question. We will never ask for your banking PIN or passwords.

Message 3 – Confirmation of scope

Hi [Name]. Thank you, your identity is confirmed. If you go ahead, we will delete: [list]. We must keep: [list], because [reason], until [date]; it will be locked and not used for anything else. [If cover is active: your cover cannot continue without this information.] Deletion is permanent. Reply CONFIRM DELETE within 10 business days to go ahead, or STOP to cancel.

Message 4 – Completion

Dear [Name]. Your request [ref] is complete. On [date] we deleted: [list]. We have kept: [list], because [legal reason], and it will be destroyed on or about [date]. We have also asked [operators / your scheme or insurer] to delete your information. If you have questions, contact our Information Officer at compliance@nationalhealthcare.co.za. You may also contact the Information Regulator at POPIAComplaints@inforegulator.org.za.

Message 5 – Unable to delete / referred

Dear [Name]. We have considered your request [ref]. We cannot delete [information] because [reason, e.g. it is a clinical record we must keep until (date) / your cover is active / your information is held on behalf of (scheme, insurer or employer), to whom we have referred your request on (date)]. We have [restricted the information so it is used only for that purpose / stopped all marketing]. If you disagree, contact our Information Officer at compliance@nationalhealthcare.co.za or the Information Regulator at POPIAComplaints@inforegulator.org.za.