12 November 2026

Notification of a Security Compromise in terms of Section 22 of the Protection of Personal Information Act, 2013 (POPIA)

Right to Care NPC (**Right to Care** or **we**) is issuing this notice to inform potentially affected data subjects of a cybersecurity incident affecting its IT environment.

This notice explains what happened, the personal information that may have been affected, the possible consequences, the steps we have taken and practical measures you may consider taking to protect yourself.

What happened

On 3 November 2026, Right to Care identified a ransomware incident involving unauthorised access to its IT environment. Preliminary forensic findings indicate that an unauthorised threat actor identifying itself as "The Gentlemen" (the "**threat actor"**) gained access to parts of the environment and exfiltrated information before deploying ransomware.

The investigation has confirmed that the threat actor acquired certain Right to Care records without authorisation. The investigation into the full scope of the incident remains ongoing.

Why we are publishing this notice

Right to Care has determined that the affected information contains personal information relating to data subjects.

This notice provides information about the incident and the precautionary steps that potentially affected data subjects may take.

Personal information that may have been affected

The information potentially involved differs depending on the person and the records concerned. It may include some or all of the following:

- **Financial and payment records**: payment-related and other financial records.
- **Employment records**: CVs and HR and payroll-related records.
- **Health programme-related records**: consent forms and other records relating to Right to Care's health programmes.

The investigation remains ongoing to determine the full nature and extent of the personal information affected and the categories of data subjects concerned.

Not all of these categories apply to every potentially affected data subject. Right to Care will provide further information, where appropriate, if material findings change its understanding of the incident or the potential risks.

Possible consequences

Personal information accessed or acquired without authorisation may be used, alone or together with information obtained elsewhere, to facilitate identity theft, fraud, phishing, social-engineering attempts, impersonation, account compromise or other fraudulent activity.

At this stage, Right to Care has not identified evidence that the affected information has been published or otherwise misused. Nevertheless, because information was accessed and exfiltrated without authorisation, potentially affected data subjects should remain vigilant and take the precautions set out below.

What we have done

Following detection of the incident, Right to Care took steps to contain and investigate the incident, including:

- isolating the affected IT environment;
- engaging external digital-forensic, incident-response and legal advisers;
- conducting forensic analysis of affected systems;
- assessing the nature and extent of the unauthorised access and exfiltration;
- undertaking remediation measures to support the secure restoration of affected systems and prevent further unauthorised access; and
- confirming that its off-site backup server was not compromised.

Right to Care has also notified the Information Regulator of South Africa in accordance with POPIA.

The forensic investigation and remediation activities remain ongoing.

What you can do

We recommend that potentially affected data subjects remain vigilant and consider the following precautions:

- **Be alert to unexpected communications.** Treat unexpected emails, telephone calls, SMS messages, WhatsApp messages and social-media communications with caution, particularly where they create urgency or request personal, banking or authentication information.

- **Verify unusual requests independently.** Do not rely on contact details or links contained in a suspicious communication. Contact the relevant organisation using its official website, application or a number you already know and trust.

- **Protect confidential information.** Never disclose passwords, PINs, one-time passwords or other authentication information in response to an unsolicited communication.

- **Avoid suspicious links and attachments.** Check the sender’s address carefully and access websites or applications directly rather than following an unexpected link.

- **Monitor your financial accounts.** Review bank statements and account activity regularly and report unfamiliar transactions promptly.

- **Review your credit profile.** Consider obtaining a credit report from a registered credit bureau and checking it for unfamiliar accounts, applications or enquiries.

- **Strengthen account security.** Use strong, unique passwords and enable multi-factor authentication wherever available, particularly for email, banking and other important accounts.

- **Be cautious with identity documents.** Do not provide copies of identity documents, proof of address or banking details unless you have independently confirmed the recipient and the reason for the request.

- **Consider protective registration.** You may consider applying for free Protective Registration through the Southern African Fraud Prevention Service (SAFPS).

- **Report suspicious contact.** If anyone claims to possess Right to Care information or approaches you about this incident, do not engage, make payment or follow their instructions. Preserve the communication and report it to Right to Care using the contact details below.

Contact us

If you have questions about this notice or wish to report suspicious activity relating to the incident, please contact Right to Care using the details below:

Email: victor.litlhakanyane@righttocare.org

Telephone: 012 4927894

Right to Care recognises the importance of protecting personal information and regrets the concern this incident may cause. We remain committed to investigating the incident, addressing identified risks and taking appropriate measures to safeguard personal information.

Yours sincerely,

Dr Victor Litlhakanyane

Group CEO
For and on behalf of Right to Care NPC