Notification of security compromise under section 22 of the Protection of Personal Information Act, 2013 ("POPIA")

Sunninghill Radiology ("**our**" / "**we**" / "**us**") hereby notifies staff, clients, customers and other stakeholders of an information security compromise detected on 14 July 2025 ("**the incident**").

We are taking the necessary measures to contain, assess and remediate the security compromise and to restore the integrity of our information systems. We are being supported in this by a team of external legal and forensic experts.

This notification provides information relating to the incident, the measures we have taken to mitigate any possible adverse effects, and recommendations on proactive steps which any potentially affected data subject may consider taking to secure their personal information.

Overview of the incident

On 14 July 2025 we became aware that part of our server environment had been accessed unlawfully by an unknown third party. As a result of unauthorised access to a server managed by an external IT service provider, certain files containing patient information were accessed and exfiltrated.

A digital forensic investigation commenced immediately with the assistance of external specialists. This investigation is ongoing to determine the scope and impact of the incident.

We do not at this stage have a full picture of the exfiltrated data, but the affected personal information may include:

- Full names
- ID numbers
- E-mail addresses
- Telephone numbers
- Physical addresses
- Location information
- Information related to past or future treatment at Sunninghill Radiology

- Special personal information (as defined in POPIA) related to physical or mental health, such as information related to race, ethnicity, wellbeing, sexual orientation, disability, pregnancy.

The incident has not impacted our daily operations and we have secure access to all operational, financial and patient data.

What we have done

We take the confidentiality, privacy and security of data and personal information in our care very seriously. We have acted promptly, with the assistance of external experts, to investigate and resolve the incident as well as to notify our community and to report the incident to the Information Regulator. We have obtained specialist legal advice and will continue to take the necessary steps to comply with our legal obligations.

We have put emergency security safeguards in place to protect data and personal information under our control, including:

• External IT forensic specialists were called in to identify the root cause of the issue

• They have confirmed the software vulnerability is no longer active and the vulnerability has been patched.

• We have locked down all access to the affected system.

• The network has been tested and confirmed safe by the third party Forensic team.

Possible consequences to data subjects

The full extent of the incident and any impacted personal information is presently unclear, but investigations into this are ongoing.

Personal information contained in the impacted data may be used to attempt fraud or further security compromises, such as social engineering/impersonation attempts, phishing attacks and/or email compromises.

We encourage you, in accordance with best practice, to maintain these security measures:

- **Monitor Your Credit Profile.** To mitigate any fraudulent consequences, you can place a fraud alert on your credit report at any of the major credit bureaus.
- **Apply for Free Protective Registration.** You can register for a free Protective Registration listing with the Southern Africa Fraud Prevention Service (SAFPS) to help protect you against the risks of identity compromise: You can apply via the SAFPS website: www.safps.org.za in three different ways:

- Apply online www.safps.org.za
- Via Email by downloading an application form from www.safps.org.za/ and emailing it to protection@safps.org.za with the necessary supporting documents (you will need: certified copy of your ID or passport, proof of address, and the completed application form).
- SAFPS Call-Back: You can also submit your details through the SAFPS website www.safps.org.za/, and one of their agents will contact you to begin the process.

- **Safeguard your personal information.** Do not disclose personal information such as passwords and PINs when asked to do so by anyone via email, phone, text messages or fax. Verify all requests for personal information and only disclose it when there is a legitimate reason to do so.
- **Exercise extra vigilance online**. Carefully consider emails which contain embedded hyperlinks or unexpected attachments. Avoid clicking on links or downloading attachments from suspicious emails. Be cautious when sharing your ID, address, or bank information—especially in digital formats or with unfamiliar contacts.
- **Strengthen your security.** Change your passwords regularly, using lengthy passwords with complexity, and never share these with anyone else. If you use your the same password elsewhere, consider changing it to something strong and unique. Enable multi-factor authentication (MFA) for online accounts, especially financial services. Use a password manager to create and store strong, unique passwords for each account.
- **Protect your devices.** Perform regular anti-virus and malware scans on computers and mobile devices, using software that is up to date. Keep operating systems and apps up to date to protect against vulnerabilities.

For more information

We remain committed to safeguarding data and personal information in our care.

If you have any questions, concerns or require further assistance, please contact us at queries@shrad.co.za.