



PRIVACY POLICY

1. What is this document about?

This Privacy Policy stipulates how the Icon Group of Companies processes your personal information. This includes why we collect information about you, the type of information we collect, how we collect it, with whom we will share it, the security measures we use to protect the information, and how you may obtain access to and correct your information. **You should read this Privacy Policy carefully. Every provision is important and material. If something is unclear to you, please ask that it be explained.**

2. About the Icon Group of Companies

The Icon Group of Companies ('the Icon Group') facilitates the provision of oncology treatment to patients at various oncology treatment facilities and provides managed care services related to oncology. Several group companies provide support services to the treatment facilities and practitioners who provide treatment at these facilities.

3. Companies Covered by this Privacy Policy

This Privacy Policy applies to Icon Healthcare Holdings (Pty) Ltd and every company or other entity that is, from time to time, directly or indirectly owned or controlled by, under common ownership or control with, or otherwise forms part of the Icon Group (collectively, the "Icon Group Companies"). It applies to all current Icon Group Companies and automatically extends to any company or other entity that is acquired, incorporated, established or otherwise becomes part of the Icon Group after the effective date of this Privacy Policy, for so long as that company or entity forms part of the Icon Group and to the extent that it processes personal information in connection with the activities of the Icon Group.

The contact details of the Icon Group companies and oncology treatment facilities are available at <https://iconsa.co.za/>.

4. Explanation of Terms Used

- 4.1 **“Data subject”** refers to the person (e.g., patient) or entity to whom the personal information relates.
- 4.2 **“Personal information”** has the meaning assigned to it in POPIA and refers to information relating to identifiable, living human beings (natural persons) and identifiable, existing juristic persons. It includes race, gender, pregnancy, age, health status, medical information, date of birth, identity number, contact details, and confidential correspondence.
- 4.3 **“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.
- 4.4 **“POPIA”** means the Protection of Personal Information Act (Act 4 of 2013) and its Regulations.
- 4.5 **“We” / “us” / “our” or “the Companies”** refers to the Icon Group of Companies.
- 4.6 **“Website”** means the website of the Icon Group of Companies, namely www.iconsa.co.za
- 4.7 **“You” / “your”** refers to the data subject (i.e., the individual or entity) whose personal information is processed by us.

5. Information and Deputy Information Officers

Information Officer: Murray Izzett
Telephone Number: 021 944 3600
E-mail address: murray.izzett@iconsa.co.za

Deputy Information Officer: Akbarallie Abbas
Telephone Number: 021 944 3600
E-mail address: aabbas@iconsa.co.za

Access to Information General Contact: Colette Cloete
Email: ccloete@iconsa.co.za

6. Our Commitment

We understand that your personal information is important to you and that you may be anxious to disclose it. Your privacy and the security of your information are just as important to us, and we want to make sure you understand how your information will be processed. We take our commitment to protecting your personal information seriously. We will, therefore, only process your personal information, which includes collecting, using, storing, or disclosing it, as permitted by law or with your consent, and will always strive to keep your information confidential. We have implemented several processes to make sure that your personal information is used in the right way.

7. When Providing Information about Others

You must make sure that if you provide personal information about any individual (such as a spouse or child) or entity to us, you may lawfully do so (e.g., with their consent). We will accept that you may share the information with us lawfully. You should ensure that the persons (or entities) whose information is shared understand how we will use and disclose their information. This is also set out in this Privacy Policy.

8. Purposes of Processing Personal Information

The Icon Group process the personal information of data subjects for the following purposes:

- (a) to conduct and manage the companies in its Group in accordance with the law, including the administration of the companies and claiming and collecting payment for services rendered from relevant funders, patients, and/or responsible persons / entities,
- (b) for communication purposes,
- (c) for the maintenance of company records and patients' medical records,
- (d) for employment and related matters of employees,
- (e) for reporting to persons and bodies as required and authorised in terms of the law or by the data subjects,
- (f) for historical, statistical and research purposes,
- (g) to enforce our rights, including legal defence purposes, and
- (h) for any other lawful purpose related to the activities of the companies.

9. Collection of Personal Information

9.1 General

We collect personal information about you which is necessary for a specific purpose.

We obtain personal information directly from you when -

- You become a director, shareholder or employee of a group company.
- You become a client of a group company.
- You become an employee of a group company.
- You become a patient of Dr SJ Fourie and Partners Inc., any oncology treatment facility operated by Icon or a practice or practitioner to whom we provide managed care services.
- You provide us with information or services.
- You contact us electronically or supply personal information on our website.
- You refer patients to us.

- You receive services as a patient from us.
- We procure products or services from you as a supplier, service provider or vendor.

We may collect publicly available personal information about you. We may also collect personal information from other sources, for example, when it is not possible to obtain the information directly from you or when it is necessary to protect your legitimate interests, such as ensuring your safety, as well as that of our staff and other visitors to our companies, and for legal defence purposes.

9.2 Applicants for Employment

We may collect information about applicants for employment from personnel agencies and vetting agencies.

9.3 Patients and their Next-of-Kin

We collect patients' radiological images and reports, pathology results, and other relevant information from referring and treating healthcare practitioners, as well as hospitals where patients are admitted, if necessary for the provision of treatment. We collect information about patients' next-of-kin and other individuals who may act on their behalf as necessary to enable a patient to receive treatment at one of our facilities.

9.4 Dependants of Employees

We collect information about the dependants of employees when our employee benefits will also benefit them.

9.5 Referring Healthcare Practitioners

We may collect information about referring healthcare practitioners from their staff, Medpages and patients.

10. Processing of Personal Information

Various laws permit the processing of personal information of patients, including the National Health Act, the Health Professions Act, POPIA, and the Medical Schemes Act. Employment and labour laws permit the processing of employees' information.

We have CCTV cameras at some of our treatment facilities and Head Office premises that record the movement of all persons for security purposes. Except for these recordings, filming or photographing of any person at any of our facilities or premises is strictly prohibited.

10.1 Directors and Shareholders:

We generally process the following personal information about directors and shareholders, as may be necessary, and retain it as part of our records:

- Names and surnames, titles, identity numbers, contact details, physical and postal addresses, telephone numbers, nationalities, gender, race, qualifications, registered professions, registration numbers, CVs and

photos,

- Financial and payment information, including bank details, and
- Correspondence.

10.2 Employees and Job Applicants:

We generally process the following personal information about employees and job applicants, as may be necessary, and retain it as part of our records:

- Names, titles, contact details, addresses, telephone numbers, identity numbers, dates of birth, age, race, gender, nationality, language, marital status, qualifications, profession, references and CVs,
- HPCSA or other statutory council number, position or role at the company, job descriptions, bank details, relevant health and disability information, vetting reports (qualifications and criminal records), employment-related information, including all information supplied on the employment contract and in supporting documentation, disciplinary-related information, leave records, absenteeism information, remuneration and employment benefits, tax numbers and related tax information, next-of-kin details and information on dependants,
- Membership of professional societies,
- Professional indemnity cover,
- Signatures of official signatories of a company and their FICA documentation,
- Records created in the performance of their duties,
- Health and safety-related incidents, and
- Correspondence.

10.3 Patients

We generally process the following personal information about patients, if necessary, and retain it as part of our records:

- Contact or other identifying information, such as name, address, telephone number, date of birth, identity number, age, gender, nationality and correspondence,
- Health information, including health status, medical history and other information received from referring and other treating healthcare practitioners, reports of special investigations,
- Contact details and other relevant information about next-of-kin, the persons who may provide consent on behalf of patients and those responsible for the payment of accounts, including details of the patient's medical scheme, health insurer or other funder,
- Accounts and payment details,
- Employment details (e.g. employer and its contact details),
- Correspondence, and
- Any other information recorded on patient documentation, such as consent forms.

10.4 Referring and Treating Healthcare Practitioners

We generally process the following personal information about healthcare practitioners who refer patients to us or who treat the patients, if necessary, and retain it as part of our records:

- Names and contact details, title, qualifications, specialisation, practice code numbers, interests and other information included on referral notes, and
- Correspondence.

10.5 Suppliers, Vendors and Other Third Parties

We generally process the following personal information about suppliers, vendors and other third parties (including medical schemes, hospitals, healthcare facilities, regulators and next-of-kin of patients, employees and guarantors of patients), if necessary, and retain it as part of our records:

- Person or entity's name and contact details,
- Names, titles and contact details of relevant persons or office bearers,
- Agreements and related information,
- Practice code numbers,
- Invoices,
- Official documentation, including newsletters and statements,
- Market information, and
- Correspondence.

Other personal information of data subjects, beyond what is stated above, may be collected and processed if required in the circumstances, subject to the provisions of the law.

11. Consent

Where you must consent to the processing of your personal information, you may withdraw your consent at any time. This does not affect information that we have already processed. If you withdraw your consent, we will only process your information as permitted by law. This may impact the services that you require from us. This will be discussed with you at the time if it is necessary.

12. Objection to Processing

When we process your personal information to protect your legitimate interests or based on the legitimate interests of a company or those of a third party to whom we supply the information, you may object, if it is reasonable to do so in the circumstances. An example of processing to protect a legitimate interest of a data subject is when we record the contact details of a patient's or employee's next-of-kin to enable us to contact them in an emergency concerning the patient or employee. An example of processing based on our legitimate interest is when we share your information with a group company that provides support services to us. We will carefully consider the relevant interests before processing personal information based on the legitimate interest

of any party. You must complete a specific form to object, which is available at the reception of the various group companies or from the Information Officer. You can discuss options to submit an objection electronically with the Information Officer. If you object and we agree with your objection, your personal information will only be processed as permitted by law. This does not affect your personal information that we have already processed.

13. Sharing and Disclosure of Personal Information

We will share the personal information of data subjects in general with the following persons and entities if it is necessary and lawful in the circumstances:

- Law enforcement and government agencies or other related third parties: From time to time, we may be required to provide personal information to a third party to comply with a subpoena, court order, government investigation, reporting obligation, or another legal (including complaint) process. If we disclose your personal information in this way, we will reasonably attempt to provide you with advance notice, unless we are prohibited from doing so or if it is not appropriate in the circumstances.
- Corporate transactions: If we become insolvent or are involved in a merger, acquisition, reorganisation, or sale of all or a portion of our business or assets, we may share or transfer your personal information as part of such corporate transaction.
- Our staff: If required for their roles and functions.
- Service providers (such as our IT support team) and relevant ICON group companies that provide support services to our companies: Only if it is necessary, subject to confidentiality undertakings and legislation protecting the privacy of your personal information.
- Our accountants and/or auditors.
- Our professional advisers (including legal advisers); and
- Our insurers (including medical indemnity cover providers), if required in the unlikely event of a claim.

Specific sharing of the personal information may include –

In respect of Patients:

- Treating or referring practitioners. Personal information (including medical records) will be shared with oncologists affiliated with ICON, such as ICON network providers, when a patient visits an affiliated oncologist for treatment, unless the patient objects. This will ensure a seamless patient experience and prevent unnecessary delays in treatment.
- Persons who may lawfully act on your behalf and those who are responsible for paying your accounts.
- Hospitals (in-patients).
- Next-of-kin.
- Relevant funders such as the patient's medical scheme, the Road Accident Fund, the Compensation Commissioner or the employer (injuries on duty). Patients' personal information (including medical information) will be shared with their medical schemes if necessary for authorisation and the allocation of

benefits for the proposed treatment.

- Debt collectors or attorneys, if we must collect outstanding accounts.

In respect of Referring and Treating Healthcare Practitioners

- Relevant funders.
- Patients.
- Hospitals.

In respect of Clinical and Other Staff (including Job Applicants) of a company:

- Entities performing peer review (healthcare practitioners).
- Next-of-kin in emergencies.
- Funders.
- Patients.
- Vetting and employment agencies (if applicable).
- Banks.
- Professional societies.
- Peer review bodies.
- Hospitals.
- The public (information on the company's website).
- Relevant public and private bodies (such as the South African Health Products Authority and the Board of Healthcare Funders of Southern Africa [BHF]).

In respect of Suppliers, Vendors and Other Third Parties:

- Banks.
- Funders.
- Patients.

14. Social Networking Platforms

We may use social networking platforms such as LinkedIn, X (formerly Twitter), and Facebook to communicate with the public and healthcare providers about our services. When you communicate with us through these services, the relevant social networking service may collect your personal information for its own purposes. These platforms have their own privacy policies. You should consult their privacy policies and documents for information about their privacy practices.

15. Security of Your Personal Information

We are committed to ensuring the security of your personal information to protect it from unauthorised

processing and access as well as loss, damage or unauthorised destruction. There are inherent risks associated with the electronic transfer (e.g., via email) and storage of personal information. We will take all reasonable steps to protect your information. We have implemented and will continually review and update information protection measures to ensure the security, integrity, and confidentiality of your information, following industry best practices. These measures include the physical securing of hard-copy records, multi-factor authentication to access electronic records, encryption of information and devices, and off-site data backups. Additionally, only employees and service providers who require access to your information to fulfil their duties and provide services to us are granted access to your information. They must also sign agreements with us regarding the protection of your information. They may only use your information to render services to us. We will inform you and the Information Regulator if any person has unlawfully obtained access to your personal information, subject to the provisions of the law.

16. Record-Keeping

We maintain records of your personal information for as long as it is necessary for lawful purposes related to the conducting of our business, including providing treatment and care to patients, complying with legal obligations, resolving complaints, attending to litigation (if applicable), enforcing agreements and for historical, statistical and research purposes subject to the provisions of the law.

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

We process and store your personal information predominantly within South Africa. If we must disclose your personal information to a third party in another country, we will obtain your prior consent, unless such disclosure is permitted by law.

18. Right to Access Personal Information

You have the right to request access to your personal information in our possession or under our control, as well as information of third parties to whom we have supplied that information. Your right is not unlimited. The law imposes certain restrictions on this right. If you wish to exercise this right, please complete the prescribed form, available at the reception of the relevant company and from the Information Officer and submit it to the receptionist or Information Officer. Costs may apply to such a request, which can be obtained from the receptionist or the Information Officer. Please refer to our PAIA Manual for additional information.

19. Accuracy of Personal Information

We must always have accurate information about you on record, as it could impact communication with you and your health, if applicable. You must therefore inform us as soon as any of your information has changed. You may also request us to correct or delete any information or destroy or delete a record of personal information. Such a request must be made in writing on the prescribed form, available at the reception of the relevant company and from the Information Officer, and submitted to the receptionist or the Information Officer. You can discuss options to submit a request electronically with the Information Officer. You must provide sufficient detail to identify the information and the correction or deletion required. Information will only be corrected or deleted if we agree that it is incorrect or should be deleted. It may not be possible to delete all the information if we may lawfully retain it. Please enquire at reception or contact the Information Officer to discuss how we can assist you with your request. If we correct any information and the corrected information will impact any decision made or to be made about you, we will send the corrected information to the persons to whom the information has been disclosed in the past, if they should be aware of the changed information.

20. Changes to this Policy

We reserve the right in our sole and absolute discretion to revise or supplement this Privacy Policy from time to time to reflect, amongst others, any changes in our business or the law. We will publish the updated Privacy Policy on our website. It will also be available at the reception of all the Icon Group Companies and treatment facilities, subject to this Policy. Any revised version of the Policy will take effect as of the date it is posted on the website. You should always make sure that you have read the latest version of the Policy. **It is your responsibility to make sure you are satisfied with any changes before continuing to use our services.** If you have any questions concerning this Policy, please contact our Information Officer.

21. Enquiries and Concerns

All enquiries, requests or concerns regarding this Policy or relating to the processing of your personal information should be addressed to the Information Officer. You may also complain to the Information Regulator at POPIAcomplaints.IR@inforegulator.org.za (violation of personal information) or PAIAcomplaints.IR@inforegulator.org.za (access to record requests). We would appreciate it if you would allow us to consider your request or complaint before you approach the Information Regulator.

22. Law Applicable to this Privacy Policy

This Privacy Policy is governed by the laws of the Republic of South Africa and is subject to the jurisdiction of the South African courts.