

ProfNet Medical (Pty) Ltd

PAIA Manual

Table of Contents

1. INTRODUCTION TO PROFNET	3
2. CONTACT DETAILS OF PROFNET	3
3. GUIDE OF THE SA HUMAN RIGHTS COMMISSION / INFORMATION REGULATOR.....	3
4. RECORDS HELD BY PROFNET	4
5. INFORMATION AVAILABLE IN TERMS OF LEGISLATION	5
6. RECORDS AUTOMATICALLY AVAILABLE.....	6
7. PURPOSE OF PROCESSING PERSONAL INFORMATION	6
8. DATA SUBJECTS, THEIR PERSONAL INFORMATION AND POTENTIAL RECIPIENTS OF INFORMATION.....	7
9. PERSONAL INFORMATION SENT ACROSS THE BORDERS OF THE RSA.....	12
10. SECURITY MEASURES TO PROTECT PERSONAL INFORMATION	12
11. PROCEDURE TO OBTAIN ACCESS TO RECORDS OR INFORMATION	13
12. FEES PAYABLE TO OBTAIN THE REQUESTED RECORDS OR INFORMATION	13
13. AVAILABILITY OF THIS MANUAL	13

1. INTRODUCTION TO PROFNET

ProfNet Medical (Pty) Ltd (“ProfNet”), a private company registered under the laws of South Africa with registration number 2013/226782/07, provides leading-edge healthcare solutions for healthcare providers, medical insurers, administrators and managed care organisations using a combination of technology solutions, healthcare and artificial intelligence. ProfNet forms part of the Spesnet Global Group of Companies, which has offices in South Africa, Singapore, Indonesia, the Philippines and the United States of America (“the USA”).

2. CONTACT DETAILS OF PROFNET

Managing Director:	Mr. R. Olver
Information Officer:	Mr. R. Olver
Deputy Information Officer:	Theo Potgieter
Physical Address:	Block 2, Crossway Office Park, 240 Lenchen Ave, Centurion, Pretoria, 0157
Postal Address:	PO Box 8630, Centurion, 0046
Telephone Number:	+27 (0)12 683 0360
E-mail address:	informationofficer@spesnet.co.za
Website address:	https://www.profnetmedical.co.za

3. GUIDE OF THE SA HUMAN RIGHTS COMMISSION / INFORMATION REGULATOR

The South African Human Rights Commission (“SAHRC”) / Information Regulator compiled a Guide, in terms of Section 10 of the Promotion of Access to Information Act 2 of 2000 (“PAIA”), to assist persons wishing to exercise their rights in terms of this Act. This Guide contains, amongst others, the following information:

- The purpose of PAIA;
- The manner, form and costs of a request for access to information held by a body;
- Legal remedies when access to information is denied;
- When access to information may be denied; and
- The contact details of Information Officers in the national, provincial and local government.

The Guide is available in all the official languages on the website of the SAHRC at

<https://www.sahrc.org.za/home/21/files/Section%2010%20guide%202014.pdf> or can be obtained from the Information Regulator at:

Physical address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

Postal address: PO Box 31533, Braamfontein, Johannesburg, 2017

Telephone: +27 (0) 10 023 5207 / +27 (0) 82 746 4173

E-mail address: infoereg@justice.gov.za

Website: <https://www.justice.gov.za/infoereg/>

The publication of the Guide will become the responsibility of the Information Regulator with effect from 30 June 2021.

4. RECORDS HELD BY PROFNET

ProfNet holds the following categories of records:

(a) **Records relating to the Company and its Operations:**

Documents related to the establishment of the company, its incorporation, its directors and shareholders as required in terms of the Companies Act 71 of 2008; a shareholders' agreement; other statutory records; telephone recordings of external calls; CCTV footage of visitors to the ProfNet; recording of virtual meetings; member and client registries; governance documents and other related documents.

(b) **Membership records:**

Application forms; supporting documentation and agreements, including records of members' patients, required to perform these agreements.

(c) **Client records:**

Agreements and related information, including records of clients' patients and policy holders, required to perform the client agreements; standard operating procedures ("SOPs"); policies; financial records; governance-related documents and records relating to the performance of client services.

(d) **Employment records:**

Recruitment records; employment contracts; employee details; conditions of employment; workplace policies; skills development plans (where applicable) and

training records; salary register; relevant tax records; leave records; disciplinary records; medical scheme application forms; group life beneficiary nominations and related documentation.

(e) **Health and safety records:**

Evacuation plan; health and safety committee records; health and safety incident reports.

(f) **Financial records:**

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

(g) **Records related to assets:**

Asset register; stock records; sale and purchase agreements and related records.

(h) **Agreements:**

Agreements and related documentation with associations / societies, contractors, consultants, suppliers, vendors and other relevant persons and entities.

(i) **Public and private body records:**

Business engagements; official documents published and correspondence.

(j) **Legal records:**

Records related to legal matters.

(k) **Insurance records:**

Policies and related records; claims and payment records.

5. INFORMATION AVAILABLE IN TERMS OF LEGISLATION

ProfNet holds records as may be required in terms of the following legislation subject to the specific protection offered by these laws:

- (a) Basic Conditions of Employment Act 75 of 1997;
- (b) Broad-Based Black Economic Empowerment Act 53 of 2003;

- (c) Compensation for Occupational Injuries and Diseases Act 130 of 1993;
- (d) Disaster Management Act 57 of 2002;
- (e) Electronic Communications and Transactions Act 25 of 2002;
- (f) Employment Equity Act 55 of 1998;
- (g) Income Tax Act 58 of 1962;
- (h) Labour Relations Act 66 of 1995;
- (i) Medical Schemes Act 131 of 1998;
- (j) Occupational Health and Safety Act 85 of 1993;
- (k) Promotion of Access to Information Act 2 of 2000;
- (l) Protection of Personal Information Act 4 of 2013;
- (m) Skills Development Levies Act 9 of 1999;
- (n) Skills Development Act 97 of 1998;
- (o) Unemployment Contributions Act 4 of 2002;
- (p) Unemployment Insurance Act 63 of 2001; and
- (q) Value Added Tax Act 89 of 1991.

6. RECORDS AUTOMATICALLY AVAILABLE

No notice has been submitted by ProfNet to the Minister of Justice and Correctional Services regarding the categories of records, which are available without a person having to request access in terms of Section 52(2) of PAIA. However, the information on the website of ProfNet is automatically available. Access and usage of the information on the website are subject to the Website Terms and Conditions as well as the Privacy Policy of ProfNet.

7. PURPOSE OF PROCESSING PERSONAL INFORMATION

ProfNet processes personal information of data subjects for the following purposes:

- to conduct its business and meet its objectives.
- to perform agreements;
- to procure and enrol members, administer membership, collect fees and provide membership services;
- to procure and enrol clients, manage and execute contracts, collect fees and provide client services;
- for recruitment, employment, human resource and labour-related matters;

- for training, up-skilling and career growth purposes;
- for industrial relations and disciplinary purposes;
- for governance purposes;
- for communication purposes;
- to engage with public and private bodies (including regulators) on behalf of clients;
- to engage with clients and potential clients nationally and internationally;
- for marketing purposes;
- for training purposes;
- to procurement purposes;
- for historical, statistical and research purposes;
- for enforcement of its rights;
- to discharge statutory duties;
- for the provision of employment benefits;
- to detect criminal behaviour;
- for protection of our offices, business, assets and employees; and
- for any other lawful purpose related to its business.

8. DATA SUBJECTS, THEIR PERSONAL INFORMATION AND POTENTIAL RECIPIENTS OF INFORMATION

ProfNet holds the personal information in respect of the categories of data subjects specified below as may be relevant in the circumstances. The potential recipients of this information are also specified. Information and records are only disclosed to recipients as may be necessary in the circumstances and authorised in terms of the law or otherwise with the consent of the relevant data subject.

(a) Directors

Categories of personal information:

Full names and surnames; titles; contact details; identity numbers; passport numbers; race; gender; nationality; biometric information; spouses' details (for travel and accommodation arrangements); remuneration; vehicle registration details; bank details; tax numbers and related tax information; information included on visa application forms; signatures of official bank signatories; proof of residence; and correspondence.

Potential Recipients:

Other directors; relevant employees; banks; embassies; South African Revenue Service (“SARS”); relevant statutory and other public bodies (e.g., Compensation Commissioner for Occupational Diseases and Injuries [“COIDA”], Company and Intellectual Property Commission [“CIPC”] and the Unemployment Insurance Fund [“UIF”]); relevant funders; clients and potential clients; relevant suppliers, vendors and service providers; travel agents; legal and professional advisers; insurers; law enforcement structures and auditors.

(b) Employees**Categories of personal information:**

Full names and surnames; calling names / nicknames; titles; contact details; addresses; identity / passport numbers; dates of birth; age; passport numbers; race; gender; nationality; qualifications; professions; positions; biometric information; vetting reports (qualifications, credit and criminal records); employment-related information; positions, job descriptions and job grades; marital status, photos (voluntarily); relevant health and disability information; references; other information included in curriculum vitae (“CVs”); all information and documentation obtained during the recruitment / selection process; past employment history; COVID-19 screening information; health and safety-related incidents; records created in the performance of their duties; leave records; remuneration; employment benefits and related information; absenteeism information; trade union membership; emolument attachment orders; biometric information; bank details; tax numbers and related tax information; information included on medical scheme and visa application forms; authorised expenses; relevant information on spouses and emergency contacts; dependants’ and beneficiaries’ details for purposes of medical scheme membership, group risk cover, funeral cover and retirement annuity benefits (as may be applicable); recording of telephonic conversations with external callers and video meeting; CCTV footage, and correspondence.

Potential Recipients:

Directors and relevant employees; clients; relevant statutory and other public bodies (e.g., SARS); employee benefit providers; vetting agencies; relevant funders; clients and potential clients; relevant suppliers, vendors and service providers; banks; credit providers; travel agents; persons involved in disciplinary processes; medical practitioners (verify sick notes and medical reports); legal and professional advisers; insurers; law enforcement structures and auditors.

(c) Job Applicants**Categories of personal information:**

Full names and surnames; titles; contact details; addresses; identity / passport numbers; date of birth; age; race; gender; nationality; qualifications; professions; employment history and related information; relevant health and disability information; COVID-19-related screening information; vetting reports (qualifications, credit and criminal records); information included on CVs; salary information; interview notes; references; employment benefits; recording of telephonic conversations including screenings and video interviews (where applicable); CCTV footage; and correspondence.

Potential Recipients:

Relevant directors and employees; relevant statutory and other public bodies (e.g., Department of Education); recruitment and vetting agencies; legal and professional advisers; auditors and law enforcement structures.

(d) Society and Association Clients**Categories of personal information:**

Organisations' name, addresses and contact details; names, surnames, titles and contact details of contact persons, executives and employees; invoices and payment information; all the information included in proposals and agreements; SOPs; policies; governance documents; and correspondence.

Potential Recipients:

Relevant directors and employees; relevant suppliers, vendors and service providers; legal and professional advisers; insurers; law enforcement structures and auditors.

(e) Members**Categories of personal information:**

Full names and surnames, titles, identity numbers, addresses, contact details, qualifications, statutory council registration numbers and practice numbers; bank details; invoices and payment information; and correspondence.

Potential Recipients:

Relevant directors and employees; relevant SpesNet group companies; relevant statutory and other public bodies; relevant funders and employers of patients; switching houses; relevant suppliers, vendors and service providers; banks; legal and professional advisers; insurers; law enforcement structures and auditors.

- (f) Patients of Members (when rendering services to Members in terms of Written Agreements):

Categories of personal information:

Full names and surnames; titles; identity numbers; dates of birth; age; gender; addresses; contact details; marital status; funders (e.g., medical scheme / Compensation Commissioner for Occupational Diseases and Injuries); payment-related information, including invoices, remittances and statements; ICD-10 and procedure codes and correspondence.

Additional information for injury-on-duty patients: Claim numbers, funder types, treating and referring providers, treatment locations, personnel numbers, occupations, file numbers at treating providers, dates of accidents, causes of injuries, provinces, employer names, VAT numbers of employer, registration number of employers, all treatment-related information [e.g., admission and discharge dates from hospitals, clinical, billing and product codes]; medical reports and supporting documents, information related to submissions of claims.

Potential Recipients:

Relevant directors and employees; relevant SpesNet group companies; relevant statutory and other public bodies; relevant funders; switching houses; employers; relevant suppliers, vendors and service providers; legal and professional advisers; insurers; law enforcement structures and auditors.

- (g) Funder and Administrator Clients, including Switches and Managed Care Organisations

Categories of personal information:

Entity names, addresses and contact details; names, surnames, titles and contact details of contact persons, employees and executives; all the information included in proposals and agreements; and correspondence.

Potential Recipients:

Relevant directors and employees; relevant SpesNet group companies; relevant healthcare

providers; relevant statutory and other public bodies; relevant suppliers, vendors and service providers; legal and professional advisers; insurers; law enforcement structures and auditors.

- (h) Beneficiaries / Policy Holders of Funder and Administrator Clients (when rendering services for Clients in terms of Written Agreements):

Categories of personal information:

Full names and surnames, identity numbers, dates of birth, age, addresses, contact details, medical scheme numbers and incident numbers; policy holders' full names and surnames, policy numbers, addresses, contact details and incident numbers; ICD-10 codes and relevant descriptions of diseases, injuries and medical conditions; healthcare providers names and surnames, titles, addresses, practice numbers and VAT numbers.

Potential Recipients:

Relevant directors and employees; relevant SpesNet group companies; relevant statutory and other public bodies; relevant funders / insurers; relevant suppliers, vendors and service providers; legal and professional advisers; insurers; law enforcement structures and auditors.

- (i) Suppliers, Vendors, Other Persons, Entities and Bodies

Categories of personal information:

Organisation's name, registration details and contact details; names, surnames, titles and contact details of contact persons, employees and executives; all the information included in proposals and agreements; bank details and payment-related information; VAT Numbers; official documentation; BBBEE certificates; COVID-19 screening information of visitors to ProfNet; names, surnames and contact details of emergency contacts and beneficiaries of employees; names, surnames, contact details, identity and passport numbers, and other relevant information of spouses of directors and employees for travelling and accommodation arrangements; and correspondence.

Potential Recipients:

Relevant directors and employees; relevant SpesNet group companies; relevant suppliers, vendors and service providers; embassies; travel agents; travel and accommodation providers; legal and professional advisers; insurers; law enforcement structures and auditors.

- (j) Insurers

Categories of personal information:

Names and contact details; premiums; benefits and correspondence.

Potential Recipients:

Relevant directors and employees; relevant suppliers, vendors and service providers; legal and professional advisers; insurers; law enforcement structures and auditors.

9. PERSONAL INFORMATION SENT ACROSS THE BORDERS OF THE RSA

ProfNet sends personal information of relevant employees, directors and their spouses across the borders of the Republic of South Africa (“RSA”) for purposes of international tenders, visa applications, compliance with financial institution requirements and travel arrangements with their consent. These countries currently include Brazil, Germany, Australia, the USA, the Philippines, Indonesia, Botswana, Singapore, Ireland, Dubai and Swaziland. No other personal information of data subjects is sent to any third party in another country. If that will be necessary, ProfNet will obtain prior consent of the relevant data subject unless such information may be lawfully provided to that third party.

10. SECURITY MEASURES TO PROTECT PERSONAL INFORMATION

ProfNet is committed to ensuring the security of personal information in its possession and under its control in order to protect it from unauthorised processing and access as well as loss, damage or unauthorised destruction. It has implemented and continually review and update the information protection measures to ensure the security, integrity, and confidentiality of personal information in accordance with industry best practices. These measures include secure storage of records; access control to records; multiple levels of electronic security; workplace policies and off-site data back-ups. In addition, only those officers, employees and service providers or suppliers that require access to the information to discharge their functions and to render services to ProfNet are granted access to such information and only if they have concluded agreements with ProfNet or provided undertakings regarding the implementation of appropriate security measures, maintaining confidentiality and processing the information only for the agreed purposes. ProfNet will inform data subjects and the Information Regulator, if any person has unlawfully obtained access to their personal information, subject to the provisions of the law.

11. PROCEDURE TO OBTAIN ACCESS TO RECORDS OR INFORMATION

The fact that information and records are held by ProfNet as listed in this Manual should not be construed as conferring upon any requester any right to that information or record. PAIA grants a requester access to records of a private body, if the record is required for the exercise or protection of any right. If a public body lodges a request, the public body must be acting in the public interest. Access to records and information (other than that listed on ProfNet's website) is not automatic. Any person, who would like to request access to any of the above records or information, is required to complete a request form, which is available from the Information Officer of ProfNet or the Information Regulator at the contact details stipulated above.

The requester must provide sufficient detail on the request form to enable the Information Officer to identify the record and the requester. The requester must identify the right he/she is seeking to exercise or protect and explain why the record requested is required for the exercise or protection of that right. If a request is made on behalf of another person, the requester must submit proof of the capacity in which the request is made to the satisfaction of the Information Officer. Access to the requested records or information or parts of the records or information may be refused in terms of the law. Requesters will be advised of the outcome of their requests.

12. FEES PAYABLE TO OBTAIN THE REQUESTED RECORDS OR INFORMATION

Fees may be charged for requesting and accessing information and records held by ProfNet. These fees are prescribed in terms of PAIA. Details of the fees payable may be obtained from the Information Officer. The fees are also available from the Information Regulator.

13. AVAILABILITY OF THIS MANUAL

A copy of this Manual is available for inspection, free of charge, at ProfNet's offices and on its website. A copy of the Manual may also be requested from the Information Officer against payment of a fee as may be applicable.