CHIROPRACTOR

DR. BRUCE GRANT

M. TECH. CHIROPRACTIC
D.U.T.

DATA PROTECTION AND INFORMATION SHARING POLICY STATEMENT AND MANUAL OF

Dr. Bruce Grant (Sole Proprietorship)

CHIROPRACTOR

DR. BRUCE GRANT

M. TECH. CHIROPRACTIC
D.U.T.

POLICY STATEMENT

- This policy forms part of the policy owner's internal business processes and procedures.
- Any reference to the "Dr. Bruce Grant" shall be interpreted to include the "policy owner".
- Dr. Bruce Grant's governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of Dr. Bruce Grant are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
- Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

1. INTRODUCTION

This Data Protection and Information Sharing Policy ("Policy) describes the way that Dr. Bruce Grant, ("Dr. Bruce Grant"), will meet his legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Protection of Personal Information Act, No 4 of 2013 (POPI), as that is the key piece of legislation covering security and confidentiality of personal information. POPI requires Dr. Bruce Grant to inform their customers/clients/contractors/visitors as to the manner in which their personal information is used, disclosed and destroyed. Dr. Bruce Grant guarantees his commitment to protecting his customers/clients/contractors/visitors 's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

2. DEFINITIONS

2.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person;
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual customers/clients/contractors/visitors or a company that supplies Dr. Bruce Grant with products or other goods.

2.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, Dr. Bruce Grant is the responsible party.

2.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with Dr. Bruce Grant to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.5 Information Officer

The Information Officer is responsible for ensuring Dr. Bruce Grants' compliance with POPIA.

Where no Information Officer is appointed, the head of Dr. Bruce Grants' practice will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- the collection, receipt, recording, organising, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
- Whatsapp Groups.

2.8 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier
Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 De-Identify
This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Re-Identify
In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent
Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Communication sharing
Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting the sharing of information in the ordinary course of business

2.14 Biometrics
Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. PURPOSE OF THE POLICY

This purpose of this policy is to protect Dr. Bruce Grant from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, Dr. Bruce Grant could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose Dr. Bruce Grant uses information relating to them.
- Reputational damage. For instance, Dr. Bruce Grant could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by Dr. Bruce Grant.

This policy demonstrates Dr. Bruce Grants' commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating a culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of Dr. Bruce Grant.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of Dr. Bruce Grant and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. SCOPE OF THE POLICY

The Policy applies to all employees, directors, sub-contractors, agents, and appointees. The provisions of the Policy are applicable to both on and off-site processing of personal information.

INFORMATION OFFICER(S)

The Information Officer appointed to Dr. Bruce Grant Chiropractor is Dr. Bruce Grant.
He/she may be contacted at:

E-mail: bruce@compasshc.co.za

Telephone number: +27 31 563 1314

SPECIFIC DUTIES AND RESPONSIBILITIES

4.1 Governing Body

Dr. Bruce Grants' governing body cannot delegate their accountability and is ultimately answerable for ensuring that Dr. Bruce Grant meets his legal obligations in terms of POPIA.
The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

- Dr. Bruce Grant appoints an Information Officer, and where necessary, a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of Dr. Bruce Grant:
- are appropriately trained and supervised to do so,
- understand that they are contractually obligated to protect the personal information they come into contact with, and
- are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Review in order to accurately assess and review the ways in which Dr. Bruce Grant collects, holds, uses, shares, discloses, destroys and processes personal information.

4.2 Information Officer

Dr. Bruce Grants' Information Officer is responsible for:

- Taking steps to ensure Dr. Bruce Grant's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about Dr. Bruce Grant's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with Dr. Bruce Grant's personal information processing procedures. This will include reviewing Dr. Bruce Grant's information protection procedures and related policies.
- Ensuring that POPI Reviews are scheduled and conducted on a regular basis.
- Ensuring that Dr. Bruce Grant makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to Dr. Bruce Grant. For instance, maintaining a "contact us" facility on Dr. Bruce Grant's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by Dr. Bruce Grant. This will include overseeing the amendment of Dr. Bruce Grant's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of Dr. Bruce Grant are fully aware of the risks associated with the processing of personal information and that they remain informed about Dr. Bruce Grant's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of Dr. Bruce Grant.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by Dr. Bruce Grant's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer will assist the Information Officer in performing his or her duties.

4.3 IT Manager

Dr. Bruce Grant's IT Manager is responsible for:

- Ensuring that Dr. Bruce Grant's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious shacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.

- Performing regular IT Reviews to ensure that the security of Dr. Bruce Grant's hardware and software systems are functioning properly.
- Performing regular IT Reviews to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on Dr. Bruce Grant's behalf. For instance, cloud computing services.

4.4 Marketing & Communication Manager

Dr. Bruce Grant's Marketing & Communication Manager is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on Dr. Bruce Grant's website, including those attached to communications such as emails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of Dr. Bruce Grant to ensure that any outsourced marketing initiatives comply with POPIA.

4.5 Employees and other Persons acting on behalf of Dr. Bruce Grant

Employees and other persons acting on behalf of Dr. Bruce Grant will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain customers/clients/contractors/visitors, suppliers and other employees.

Employees and other persons acting on behalf of Dr. Bruce Grant are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of Dr. Bruce Grant may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within Dr. Bruce Grant or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of Dr. Bruce Grant must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of Dr. Bruce Grant will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of Dr. Bruce Grant or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted Dr. Bruce Grant with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of Dr. Bruce Grant will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, Dr. Bruce Grant will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of Dr. Bruce Grant will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from Dr. Bruce Grant's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of Dr. Bruce Grant are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of Dr. Bruce Grant, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.

- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the customers/clients/ contractors /visitors or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of Dr. Bruce Grant, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

5. POLICY STATEMENT

Dr. Bruce Grant collects and uses Personal Information of the individuals and corporate entities with whom he works in order to operate and carry out his business effectively. Dr. Bruce Grant regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between Dr. Bruce Grant and those individuals and entities who deal it. Dr. Bruce Grant therefore fully endorses and adheres to the principles of the Protection of Personal Information Act ("POPI").

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of Dr. Bruce Grant will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

Failing to comply with POPIA could potentially damage Dr. Bruce Grant's reputation or expose Dr. Bruce Grant to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

Dr. Bruce Grant will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, Dr. Bruce Grant will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing Limitation

Dr. Bruce Grant will ensure that personal information under his control is processed:

- in a fair, lawful and non-excessive manner, and
- only for a specifically defined purpose.

Dr. Bruce Grant will under no circumstances distribute or share personal information between separate legal entities, associated Company s (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

An example of a “POPI Notice and Consent Form” can be found under Annexure C.

6.3 Purpose Specification

All of Dr. Bruce Grant’s business units and operations must be informed by the principle of transparency.

Dr. Bruce Grant will process personal information only for specific, explicitly defined and legitimate reasons.

6.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where Dr. Bruce Grant seeks to process personal information he holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, Dr. Bruce Grant will first obtain additional consent from the data subject.

6.5 Information Quality

Dr. Bruce Grant will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate (for example, the beneficiary details of bank account number is of the utmost importance), the greater the effort Dr. Bruce Grant will put into ensuring its accuracy.

6.6 Open Communication

Dr. Bruce Grant will take reasonable steps to notify data subjects that their personal information is being collected including the purpose for which it is being collected and processed.

Dr. Bruce Grant will ensure that she establishes and maintains a “contact us” facility, for instance via his website or through an electronic helpdesk, for data subjects who want to:

- Enquire whether Dr. Bruce Grant holds related personal information, or
- Request access to related personal information, or
- Request Dr. Bruce Grant to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

Dr. Bruce Grant will manage the security of his filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

Dr. Bruce Grant will continuously review his security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on Dr. Bruce Grant’s IT network.

Dr. Bruce Grant will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.
All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which Dr. Bruce Grant is responsible.
All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

Dr. Bruce Grant’s operators and third-party service providers will be required to enter into service level agreements with Dr. Bruce Grant where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by Dr. Bruce Grant.

Dr. Bruce Grant will ensure that he provides a facility for data subjects who want to request the correction of deletion of their personal information.

Where applicable, Dr. Bruce Grant will include a link to unsubscribe from any of his electronic newsletters or related marketing activities.

7. PROCESSING OF PERSONAL INFORMATION

7.1 Purpose of Processing

Dr. Bruce Grant uses the Personal Information under his care in the following ways:

- Conducting credit reference checks and assessments
- Identifying and managing his customers/clients/contractors/visitors
- Identifying customers/clients/contractors/visitors medical and other related health needs
- Administration of agreements
- Providing products and services to customers/clients/contractors/visitors
- Detecting and prevention of fraud, crime, money laundering and other malpractice
- Conducting market or customer satisfaction research
- Marketing and sales
- In connection with legal proceedings
- Staff administration
- Keeping of accounts and records
- Complying with legal and regulatory requirements
- Profiling data subjects for the purposes of direct communication sharing

7.2 Personal information Collected

Section 9 of POPI states that *"Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive*."

Dr. Bruce Grant collects and processes customers/clients/ contractors /visitors 's personal information pertaining to the needs of the business. The type of information of information will depend on the needs for which it is collected and will be processed for that purpose only. Whenever possible, Dr. Bruce Grant will inform the customers/clients/contractors/visitors as to the information required and the information deemed optional. Dr. Bruce Grant aims to have agreements in place with all product suppliers, insurers and third-party service providers to ensure a mutual understanding with regard to protection of the customer's personal information. With the customer's consent, Dr. Bruce Grant may also supplement the information provided with the information that he receives from other providers in order to offer a more consistent and personalized experience for his customers/clients/contractors /visitors.

7.3 Categories of Data Subjects and their Personal Information

Dr. Bruce Grant may possess records relating to suppliers, shareholders, contractors service providers, staff, customers/clients/ contractors /visitors:

Entity Type	**Personal Information Processed**
Customers/clients/contractors /visitors: Natural Persons	Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence; medical information; banking information.
Customer – Juristic Persons/ Entities	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information, banking information
Contracted Service Providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information; banking information
Employees / Directors	Gender; pregnancy; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being, banking details

7.4 Categories of Recipients for Processing the Personal Information

Dr. Bruce Grant may share the Personal Information with his agents, affiliates, and associated companies who may use this information to send the Data Subject information on products and services. Dr. Bruce Grant may supply the Personal Information to any party to whom Dr. Bruce Grant may have assigned or transferred any of his rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organising of data;
- Storing of data;
- Sending of emails and other correspondence to customers/clients/ contractors /visitors;
- Conducting due diligence checks;
- Administration of the Medical Insurance and Provident Fund.

7.5 Retention of Personal Information Records

Dr. Bruce Grant may retain Personal Information records indefinitely, unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information Dr. Bruce Grant shall retain the Personal Information records to the extent permitted or required by law.

7.6 General Description of Information Security Measures

Dr. Bruce Grant employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under his care. Measures include:

- Firewalls
- Virus protection software and update protocols
- Logical and physical access control;
- Secure setup of hardware and software making up the IT infrastructure;
- Outsourced Service Providers who process Personal Information on behalf of Dr. Bruce Grant are contracted to implement security controls;
- Personal information shall be stored on site and access shall be limited to authorized personal only.
- All electronic files or data shall be backed up on to cloud based services by an external provider and hardcopy information is therefore shredded after three (3) years.

8. ACCESS TO PERSONAL INFORMATION

All individuals and entities may request access, amendment, or deletion of their own Personal Information held by Dr. Bruce Grant. Any requests should be directed, on the prescribed form, to the Information Officer.

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against Dr. Bruce Grant's PAIA Policy.

The Information Officer will process all requests within a reasonable time. *(Refer to PAIA Policy)*

8.1 RIGHTS OF DATA SUBJECTS

Where appropriate, Dr. Bruce Grant will ensure that his clients and customers /contractors/visitors are made aware of the rights conferred upon them as data subjects.

Dr. Bruce Grant will ensure that he gives effect to the following rights of data subjects:

8.1.1 The Right to Access Personal Information

Dr. Bruce Grant recognises that a data subject has the right to establish whether Dr. Bruce Grant holds personal information related to him, her or it including the right to request access to that personal information. An example of a "Personal Information Request Form" can be found under Annexure A.

8.1.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where Dr. Bruce Grant is no longer authorised to retain the personal information.

8.1.3 The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information. In such circumstances, Dr. Bruce Grant will give due consideration to the request and the requirements of POPIA. Dr. Bruce Grant may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

8.1.4 The Right to Object to Direct Information Sharing

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct information sharing by means of unsolicited electronic communications.

8.1.5 The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information. An example of a "POPI Complaint Form" can be found under Annexure B.

8.1.6 The Right to be Informed

The data subject has the right to be notified that his, her or its personal information is being collected by Dr. Bruce Grant. The data subject also has the right to be notified in any situation where Dr. Bruce Grant has reasonable grounds to believe that the personal information of the data subject has been accessed or a

8.2 REMEDIES AVAILABLE IF REQUEST FOR ACCESS TO PERSONAL INFORMATION IS REFUSED

8.2.1 Internal Remedies

Dr. Bruce Grant does not have internal appeal procedures. As such, the decision made by the Information Officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the information officer.

8.2.2 External Remedies

A requestor that is dissatisfied with the information officer's refusal to disclose information, may within 30 days of notification of the decision, apply to a court for relief. Likewise, a third party dissatisfied with the information officer's decision to grant a request for information, may within 180 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status.

8.3 GROUNDS FOR REFUSAL

Dr. Bruce Grant may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which Dr. Bruce Grant may refuse access include:

- Protecting personal information that Dr. Bruce Grant holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
- Protecting commercial information that Dr. Bruce Grant holds about a third party or Dr. Bruce Grant (for example trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of Dr. Bruce Grant or the third party);
- If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
- If disclosure of the record would endanger the life or physical safety of an individual;
- If disclosure of the record would prejudice or impair the security of property or means of transport;
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- If disclosure of the record would prejudice or impair the protection of the safety of the public;
- The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
- Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of Dr. Bruce Grant;
- Disclosure of the record would put Dr. Bruce Grant at a disadvantage in contractual or other negotiations or prejudice him in commercial competition;
- The record is a computer programme; and
- The record contains information about research being carried out or about to be carried out on behalf of a third party or Dr. Bruce Grant.

8.3.1 Records that cannot be found or do not exist

If Dr. Bruce Grant has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

8.4 COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. Dr. Bruce Grant takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to Dr. Bruce Grant in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form".
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on Dr. Bruce Grant's data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with Dr. Bruce Grant's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to Dr. Bruce Grant's governing body within 7 working days of receipt of the complaint. In all instances, Dr. Bruce Grant will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- The Information Officer's response to the data subject may comprise any of the following:
- A suggested remedy for the complaint,
- A dismissal of the complaint and the reasons as to why it was dismissed,
- An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

9. IMPLEMENTATION GUIDELINES

9.1 TRAINING & DISSEMINATION OF INFORMATION

This Policy has been put in place throughout Dr. Bruce Grant, training on the Policy and POPI will take place with all affected employees.

All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPI.

Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

9.2 EMPLOYEE CONTRACTS

Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

Each employee currently employed within Dr. Bruce Grant will sign an addendum to their Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

10. EIGHT PROCESSING CONDITIONS

POPI is implemented by abiding by **eight processing conditions**. Dr. Bruce Grant shall abide by these principles in all his processing activities.

10.1 ACCOUNTABILITY

Dr. Bruce Grant shall ensure that all processing conditions, as set out in POPI, are complied with when determining the purpose and means of processing Personal Information and during the processing itself. Dr. Bruce Grant shall remain liable for compliance with these conditions, even if he has outsourced his processing activities.

10.2 PROCESSING LIMITATION

10.2.1 Lawful grounds

The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.

Dr. Bruce Grant may only process Personal Information if one of the following grounds of lawful processing exists:

- The Data Subject consents to the processing;
- Processing is necessary for the conclusion or performance of a contract with the Data Subject;
- Processing complies with a legal responsibility imposed on Dr. Bruce Grant;
- Processing protects a legitimate interest of the Data Subject;
- Processing is necessary for pursuance of a legitimate interest of Dr. Bruce Grant, or a third party to whom the information is supplied;

Special Personal Information includes:

- Religious, philosophical, or political beliefs;
- Race or ethnic origin;
- Trade union membership;
- Health or sex life;
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal behaviour;
- Information concerning a child.

Dr. Bruce Grant may only process Special Personal Information under the following circumstances:

- The Data Subject has consented to such processing;
- The Special Personal Information was deliberately made public by the Data Subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical, or research reasons
- If processing of race or ethnic origin is in order to comply with affirmative action laws

All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object, at any time, to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data subject withdraws consent or objects to processing then Dr. Bruce Grant shall forthwith refrain from processing the Personal Information.

10.2.2 Collection directly from the Data Subject

Personal Information must be collected directly from the Data Subject, unless:

- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Personal Information is collected from another source with the Data Subject's consent;
- Collection of Personal Information from another source would not prejudice the Data Subject;
- Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the Data Subject would prejudice the lawful purpose of collection;
- Collection from the Data Subject is not reasonably practicable.

10.3 PURPOSE SPECIFICATION

Dr. Bruce Grant shall only process Personal Information for the specific purposes as set out and defined above herein. Dr. Bruce Grant is permitted to collect only the minimum required personal information for their purpose. In addition, the consent of the data subject is required as it ensures that he/she is aware that personal information is being processed, the purpose as well as the type of information being processed. The need for consent also ensures that personal information is collected directly from the source, further ensuring accuracy.

10.4 FURTHER PROCESSING LIMITATION

New processing activity must be compatible with original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

- Data Subject has consented to the further processing;
- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Further processing is necessary to maintain, comply with or exercise any law or legal right;
- Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party

10.5 INFORMATION QUALITY

Dr. Bruce Grant shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. Dr. Bruce Grant shall periodically review Data Subject records to ensure that the Personal Information is still valid and correct.

Employees should as far as reasonably practicable follow the following guidance when collecting Personal Information:

- Personal Information should be dated when received;
- A record should be kept of where the Personal Information was obtained;
- Changed to information records should be dated;
- Irrelevant or unneeded Personal Information should be deleted or destroyed;
- Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

10.6 OPENNESS

Dr. Bruce Grant shall take reasonable steps to ensure that the Data Subject is made aware of:

- What Personal Information is collected, and the source of the information;
- The purpose of collection and processing;
- Where the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;
- Whether collection is in terms of any law requiring such collection;
- Whether the Personal Information shall be shared with any third party.

10.7 DATA SUBJECT PARTICIPATION

Data Subject have the right to request access to, amendment, or deletion of their Personal Information.
All such requests must be submitted in writing to the Information Officer. Unless there are grounds for refusal as set out in paragraph 7.2, above, Dr. Bruce Grant shall disclose the requested Personal Information:

- On receipt of adequate proof of identity from the Data Subject, or requester;
- Within a reasonable time;
- On receipt of the prescribed fee, if any;
- In a reasonable format

Dr. Bruce Grant shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

10.8 SECURITY SAFEGUARDS

Dr. Bruce Grant shall ensure the integrity and confidentiality of all Personal Information in his possession, by taking reasonable steps to:

- Identify all reasonably foreseeable risks to information security;
- Establish and maintain appropriate safeguards against such risks;

10.8.1 Written records

- Personal Information records should be kept in locked cabinets, or safes;
- When in use Personal Information records should not be left unattended in areas where non-staff members may access them;
- Dr. Bruce Grant shall implement and maintain a “Clean Desk Policy” where all employees shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day;
- Personal Information which is no longer required should be disposed of by shredding.

Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer.

10.8.2 Electronic Records

- All electronically held Personal Information must be saved in a secure database;
- As far as reasonably practicable, no Personal Information should be saved on individual computers, laptops or hand-held devices;
- All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently;
- Dr. Bruce Grant shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day;
- Electronical Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.

Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

11. DIRECT COMMUNICATION SHARING

All Direct communications shall contain Dr. Bruce Grant's details, and an address or method for the customer to opt-out of receiving further marketing communication.

11.1.1 Existing Customers/clients/ contractors/visitors

Direct Communication by electronic means to existing customers/clients/ contractors /visitors is only permitted:

- If the customer's details were obtained in the context of a sale or service; and
- For the purpose of sharing information;

The customer must be given the opportunity to opt-out of receiving direct communication on each occasion of direct communication sharing.

11.1.2 Consent

Dr. Bruce Grant may send electronic Direct Communication Sharing to Data Subjects who have consented to receiving it. Dr. Bruce Grant may approach a Data Subject for consent only once.

11.1.3 Record Keeping

Dr. Bruce Grant shall keep record of:

- Date of consent;
- Wording of the consent;
- Who obtained the consent;
- Proof of opportunity to opt-out on each marketing contact;
- Record of opt-outs.

12. DESTRUCTION OF DOCUMENTS

12.1 Documents may be destroyed after the termination of the retention period specified herein, or as determined by Dr. Bruce Grant from time to time.

12.2 Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by Dr. Bruce Grant pending such return.

12.3 The documents must made available for collection by the shredding company, or other approved document disposal Company.

12.4 Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

13. POPI REVIEW

Dr. Bruce Grant's Information Officer will schedule periodic POPI Reviews.

13.1 The purpose of a POPI Review is to:

- 13.1.1 Identify the processes used to collect, record, store, disseminate and destroy personal information.
- 13.1.2 Determine the flow of personal information throughout Dr. Bruce Grants' practice. For instance, Dr. Bruce Grant's various business units, divisions, branches and other associated Companies.
- 13.1.3 Redefine the purpose for gathering and processing personal information.
- 13.1.4 Ensure that the processing parameters are still adequately limited.
- 13.1.5 Ensure that new data subjects are made aware of the processing of their personal information.
- 13.1.6 Re-establish the rationale for any further processing where information is received via a third party.
- 13.1.7 Verify the quality and security of personal information.
- 13.1.8 Monitor the extend of compliance with POPIA and this policy.
- 13.1.9 Monitor the effectiveness of internal controls established to manage Dr. Bruce Grant's POPI related compliance risk.

13.2 In performing the POPI Review, Information Officers will liaise with line managers in order to identify areas within Dr. Bruce Grant's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

Information Officers will be permitted direct access to and have demonstrable support from line managers and Dr. Bruce Grant's governing body in performing their duties.

14. STATUTORY RETENTION PERIODS

Legislation	Document Type	Period
Consumer Protection Act	Full names, physical address, postal address and contact details; ID number and registration number; Contact details of public officer in case of a juristic person; Service rendered; Cost to be recovered from the consumer; Frequency of accounting to the consumer; Amounts, sums, values, charges, fees, remuneration specified in monetary terms; Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions;	3 years

Financial Intelligence Centre Act	Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer; If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person; If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer; The manner in which the identity of the persons referred to above was established; The nature of that business relationship or transaction; In the case of a transaction, the amount involved and the parties to that transaction; All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; The name of the person who obtained the identity of the person transacting on behalf of the accountable institution; Any document or copy of a document obtained by the accountable institution	5 years

Compensation for Occupational Injuries and Diseases Act	Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.	4 years
	Section 20(2) documents : -Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; -Records of incidents reported at work.	3 years
	Asbestos Regulations, 2001, regulation 16(1): -Records of assessment and air monitoring, and the asbestos inventory; -Medical surveillance records; Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): -Records of risk assessments and air monitoring; -Medical surveillance records. Lead Regulations, 2001, Regulation 10: -Records of assessments and air monitoring; -Medical surveillance records Noise - induced Hearing Loss Regulations, 2003, Regulation 11: -All records of assessment and noise monitoring; -All medical surveillance records, including the baseline audiogram of every employee.	40 years
	Hazardous Chemical Substance Regulations, 1995, Regulation 9: -Records of assessments and air monitoring; -Medical surveillance records	30 years

Basic Conditions of Employment Act	Section 29(4): -Written particulars of an employee after termination of employment; Section 31: -Employee's name and occupation; -Time worked by each employee; -Remuneration paid to each employee; -Date of birth of any employee under the age of 18 years.	3 years
Employment Equity Act	Records in respect of the Company's workforce, employment equity plan and other records relevant to compliance with the Act; Section 21 report which is sent to the Director General	3 years
Labour Relations Act	Records to be retained by the employer are the collective agreements and arbitration awards.	3 years
	An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions	Indefinite
Unemployment Insurance Act	Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed	5 years
Tax Administration Act	Section 29 documents which: -Enable a person to observe the requirements of the Act; -Are specifically required under a Tax Act by the Commissioner by the public notice; -Will enable SARS to be satisfied that the person has observed these requirements	5 years

Income Tax Act	Amount of remuneration paid or due by him to the employee; The amount of employees tax deducted or withheld from the remuneration paid or due; The income tax reference number of that employee; Any further prescribed information; Employer Reconciliation return.	5 years
Value Added Tax Act	Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period; Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; Documentary proof substantiating the zero rating of supplies; Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	5 years