

Impact Therapy Centre Inc.
Procedures for Protection of Personal Information
Annexe A

1. Introduction

Impact Therapy Centre Inc., herein referred to as “the Centre”, is a health care provider company providing assessment and treatment to clients and patients in the health care sector. To date the Centre’s practitioners comprise of clinical, counselling and educational psychologists, homeopaths, speech therapists and learning facilitators.

2. Purpose of Data Collection

Impact Therapy Centre Inc. collects personal information from clients and patients for the purposes of billing, medical aid claims, contacting clients/patients for booking administration, biographical details for assessment and treatment purposes, risk to self and others management, treatment feedback and consent purposes.

3. Personal Information Data Collected

Impact Therapy Centre Inc. collects the following personal information for the purposes outlined in point 2 above and specific purpose described next to the information below:

Data Collected	Reason for Collection
Name and Surname	Identifying data for billing, claims submission and contact purposes
Date of Birth and age	Identifying data for billing, claims submission and treatment/assessment purposes
Residential Address	Billing and debt collection purposes
Cellphone Number	Contact purposes
Occupation	Treatment/assessment purposes
Employer	Billing, debt collection and contact purposes
Medical Aid Provider, Plan, Number, Main Member, and Dependents (with corresponding Date of Births)	Billing and claims purposes
Name of Relative or Friend	Contact purposes and personal risk management
Referring Doctor (if applicable)	Referral and treatment information
In Case of Minors	
Mother’s Name and contact number	Contact, consent, billing, claim, risk management and feedback purposes.
Father’s Name and contact number	Contact, consent, billing, and claim purposes

4. Method of Data Collection

In line with COVID-19 regulations, all clients who enter the premises are screened using a digital thermometer. Temperatures are recorded on a log sheet with the date, therapist's name, appointment time, temperature and client/patient signature, in an effort to de-identify the client or patient and maintain confidentiality. Names can be re-identified by our Information Officer should COVID-19 related contact need to be made.

All new clients and patients are given a blank file form at their first appointment and asked to fill out the details outlined in point 3 above. They are furthermore required to sign a consent form in line with HPCSA and POPIA regulations. Data from the hardcopy file is then captured onto the Centre's electronic booking and invoicing system, SMEmetrics, by one of the administration staff, Privilege Ncube (appointed Information Officer) or Memory Ncube.

5. Data Sharing

Impact Therapy Centre Inc. shares personal data with the following third parties:

1. SMEmetrics
2. Medical Aids
3. Debt Collection Agencies when necessary
4. Other health care practitioners for the purposes of referral, treatment and/or assessment.

6. Measures to Protect Data

Impact Therapy Centre Inc. has taken the following measures to protect personal information:

- Protection of hardcopy data:
 1. Client and patient files are kept in a locked cupboard within the Centre. Employees, Privilege Ncube and Memory Ncube as well as practitioners working at the centre may have access to files by using their own key to the cupboard.
 2. Practitioner's place completed files in a holder within the cupboard in order for files to be processed and packed away.
 3. Personal information data captured in files is shredded in a shredding machine once the file has reached an expiration date as set out by HPCSA guidelines.
- Protection of electronic data:
 1. Personal information data is captured onto a practice management system called SMEmetrics licensed under PiMetix software. The following contractual clauses have been signed and accepted between SMEmetrics and Impact Therapy Centre Inc. to ensure protection of personal information on their system:
 - A. Clause 2.6

It is recorded that PiMetix does not host third-party content. Any technical and personal data is stored and retained in accordance with PiMetix' Privacy Policy.

B. Clause 8

8.1 "Confidential Information" means, without limitation: any technical, financial, marketing, product or business information; trade secrets; business activities, practices or processes; designs, trademarks or logos; the Software; patient, client, supplier or business associate information; and any information that is not freely available to the public, being information acquired by either party from the other party during the course of this Agreement, whether formally designated as confidential or not.

8.2 Both parties are restrained from, and undertake in favour of the other that it will not, without the prior written consent of such other party or otherwise in accordance with this Agreement:

8.2.1 disclose the other party's Confidential Information to any other person. Provided that it will be entitled to disclose Confidential Information to those of its staff who need to know the Confidential Information for the purpose of performing that party's obligations and who are under a similar confidentiality obligation; or

8.2.2 use or copy the other party's Confidential Information for any purpose other than to perform its obligations.

8.3 This clause will not apply to information that is: trivial or obvious; already in the possession of a party otherwise than as a result of disclosure by the disclosing party to such party; or in the public domain for reason other than a breach hereof.

C. Clause 10.2

PiMetix will take reasonable steps to secure the Software and all data thereon with anti-virus software and suitable encryption tools, and will make every effort to protect your personal identifiable information. All secure orders and confidential information are processed through Secure Sockets Layer (SSL) technology via secure server, and all login information including email address and password is guarded using the latest encryption methods. While Pimetix will use commercially reasonable efforts to comply with this clause, PiMetix does not warrant: that the Software is free from Fault, virus, hacking or is error-free; that your use thereof will be uninterrupted, timely or secure; that

the Software will meet your requirements; the results of Use; that the results obtained from the Use of the Software will be accurate or reliable; or that the products, services, information, or other material purchased or obtained by you through the Software will meet your expectations.

D. Clause 10.3

You understand that the technical processing and transmission of communications services, including your content and other data, may involve (a) transmissions over various networks; and (b) changes to conform and adapt to technical requirements of connecting networks or devices. While PiMetix will use commercially reasonable efforts to protect, and to use third party suppliers who endeavour to protect, your content, PiMetix does not guarantee that the content will be stored, displayed or transmitted exactly as you intended.

2. Each practitioner has a protected password which enables them access to the SMeMetric system. All practitioners use the same SMeMetric package and therefore have access to other practitioner's client/patient information, however each practitioner has signed an agreement to protect the personal information of their own and other practitioner's clients/patient information. These agreements can be found in the Centre's POPI file which is kept locked away in a safe cabinet.
 3. Each practitioner has a cybersecurity system installed on their electronic devices which they use to conduct their business at the Centre. This cybersecurity system is called Bitdefender and it uses advanced artificial intelligence and other technologies to anticipate, detect and instantly block and cyber threats.
 4. Each practitioner has signed an agreement to have all electronic devices which they use to conduct their Impact Therapy Inc. related work password protected.
 5. All personal information that is kept on the Centre's electronic devices for administrative purposes such as billing and data reconciliation among others, are stored in password protected files. In addition all electronic devices at the centre are password protected.
 6. Emailed PDF reports are are password protected in that the receiver of the report will need a password in order to open the attached report.
 7. All electronic data is permanently deleted once client/patient files reach termination dates which are in accordance with HPCSA guidelines.
- Protection of Employee information:
Employee information is stored electronically in a password protected file on the Centre's system. Hardcopy employee information is stored in a file which is locked away in a cabinet within the Centre.

- Protection of information by Third parties:

Third party service providers who have access to personal information are asked to sign a confidentiality agreement in order to protect the personal information of the clients/patients at the Centre. Medical Aids with whom Personal information is shared will be assumed to be responsible for protection of that personal information in accordance with their own POPI compliance procedures based on the Protection of Personal Information Act 4 of 2013.

- De-identification of personal information

Any client/patient information that is shared with other healthcare practitioners for the purposes of supervision or research will be de-identified. All practitioners have agreed to de-identify clients/patients when communicating for administrative purposes with other practitioners or employees at the Centre.

7. Information Officer

Impact Therapy Centre Inc. has appointed Privilege Ncube as the Centre's Information officer. She has signed and agreed to the appointment of Information Officer and has been registered as such. She has agreed to ensure implementation of all all measures as set out in this document, Annexe A. The agreement has been stored away in a locked cabinet within the Centre.

8. Breach Procedures

Any breach of the above measures or any other breach of personal information that is discovered will be managed in the following 2 ways:

1. The individual/s whose personal information was breached shall be informed as soon as is reasonably possible.
2. The Regulator shall be informed of such breach.

All practitioners and employees at the Centre have signed an agreement that they will inform the Information Officer as soon as they realise a breach has occurred.

9. Consent Forms

All new clients are asked to sign a consent form which contains POPI clauses relevant to the client/patient whereby they agree to the inherent risks of breach of personal information. Existing clients will be given a new consent form to sign which contains the aforementioned consent to risk. These forms are stored in their client/patient files as hardcopies.

10. POPI Documentation

All POPI related documentation, including this policy will be stored in a POPI file which is locked away in a safe cupboard within the centre. All electronic POPI related documentation will be stored in a password protected file on the Centre's system. Should a client/patient or Officer require access to the centre's POPI policies then upon this request the the Information Officer, or her proxy shall grant immediate access to these policies.