Protection of Personal Information Policy Version 1.1

1. Policy Purpose / Policy Statement

Healthchem Group (Pty) Ltd t/a Healthchem pharmacy and Midstream pharmacy ("Healthchem") as the Responsible Party, is committed to the lawful collection, use, management of, processing and storage of personal data in terms of the Protection of Personal Information Act, Act 4 of 2013 ("the POPI Act") and recognises that everyone in South Africa has the right to privacy, as provided for in Section 14 of our Constitution. It further acknowledges that the POPI Act amplifies the right to privacy with provisions intended to protect consumers against identity theft as well as the unauthorised use or sale of their personal information for any purpose, including the creation of databases for marketing and sales campaigns.

Although the POPI Act does not prevent or make it illegal for the Directors and therefore Healthchem to collect the personal information of patients, prescribers, clients or other persons allowed access to the account of a client, the Act speaks to the reason why and the manner in which such information is collected, stored, used, managed and processed.

The purpose of this Policy is thus to govern the legal processing, management and protection of the information so collected. Furthermore, it is to assure the persons from whom such personal information is collected that Healthchem only collects such information for the effective operation of the pharmacies and that no information is gathered for or will be disseminated to third parties for commercial or marketing purposes.

2. Application / Principles and Scope of Policy

This policy is applicable to all personal information collected by Healthchem and regulates the manner in which Personal Information must be collected, processed, stored and ensures protection to the Data Subjects and the prevention of misuse of personal information pertaining to individuals and entities. As such this Policy is applicable to all employees of Healthchem and should be strictly complied with by all employees.

In addition, this Policy is applicable to all Service Providers who provide information technology related services or security related services to Healthchem and as a result of such services have access to or assists in the collection, processing, storage or management of such personal information.

3. Terminology and definitions

(a) Personal Information is widely defined in the POPI Act and includes, but is not limited to, information relating to an identifiable living natural person or a juristic person ("Data Subjects"), such as:

- Race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, believe, culture, language, birth.
- History - education, medical, financial, criminal, employment
- Identifiers – number, symbols, e-mail address, physical address, telephone numbers, location, online ID or other assignment to a person such as a unique identifier (in example a student or patient number)
- Biometric information – physical or psychological behavioural characterization, blood type, fingerprints, DNA analysis, retinal scanning, voice recognition
- Personal opinion views or preferences
- Correspondence implicitly or explicitly of a private and confidential nature
- Views or opinions of another individual
- 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

(b) The processing of Personal Information includes but is not limited to any operation / activity or any set of operations, whether automated or not, concerning Personal Information. It includes:

- Collection / receipt / recording / organising / collation / storage / updating / modification / retrieval / alteration
- Dissemination by means of transmission, distribution or making available to others.
- Merging / linking / restricting / degradation / erasure / destruction

(c) Consent is defined as "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information". It appears that all three requirements must be complied with before consent was achieved.

4. Information collected by Healthchem

4.1 The personal information collected by Healthchem regarding patients, prescribers and clients are, of which some is incidental, as follows:

(a) Name, surname, physical and postal addresses, e-mail addresses, telephone numbers, identifying numbers or symbols, such as identity number, passport number, as well as medical aid scheme details relating to service providers of Healthchem and utilised by such persons

(b) Gender, marital status, nationality, age, language, date of birth and employment

(c) Correspondence from and to persons implicitly or explicitly of a private or confidential nature

(d) Personal opinions and views or preferences and views or opinions of other individuals

4.2 The personal information collected by Healthchem regarding third parties are as follows:

(a) Name, surname, nationality, telephone numbers, identifying numbers or symbols, such as identity number or passport number

(b) Correspondence from and to persons implicitly or explicitly of a private or confidential nature

4.3 The personal information collected by Healthchem regarding its employees and temporary workers are as follows:

(a) Name, surname, physical and postal addresses, e-mail addresses, telephone numbers, identifying numbers or symbols, such as identity number, passport number, banking account details and all other human resource related information including tax numbers

(b) Gender, marital status, nationality, age, language, date of birth and employment history

(c) Biometric information such as fingerprints, handprints, photo and facial data, which include video recordings of entry, regress and other security related recordings

(d) Correspondence from and to persons implicitly or explicitly of a private or confidential nature

(e) Personal opinions, views or preferences and views or opinions of other individuals

(f) Personal and Financial related information relating to next of kin or beneficiaries for provident funds, medical plans and funeral plans

5. Reason for collecting personal information.

Healthchem does not collect personal information for dissemination to third parties for marketing, sales or database purposes.

5.1 Healthchem collects information in the following ways:

(i) Through direct or active interactions with the patient, prescriber, client or other relevant persons;

(ii) Through interactions with the website or various social media platforms;

(iii) From third parties i.e. medical aid funds;

(iv) Employment applications; and

(v) CCTV.

5.2 Healthchem will primarily use the information collected only for the purpose for which it was originally collected. The information will be used for a secondary purpose only if such purpose constitutes a legitimate interest and is compatible with the primary purpose for which the information was collected.

6. Storage of personal information

All personal information is stored electronically and / or as paper-based documents. The electronic personal information collected for operational purposes is captured and stored on the Unisolv server and / or the Pastel accounting system utilised by Healthchem and the paper-based documents are stored in locked filing cabinets in the offices. Personal information from employees is captured and stored on VIP and kept in a locked office.

The personal information collected for security purposes from patients, prescribers, clients, visitors, employees, contractors, delivery persons and services providers are stored digitally / electronically on the CCTV database which is only accessible by specific employees of Healthchem and the service providers, being Midstream Electrical Supplies (“MES”) that provide, manage, service and maintain information technology equipment, systems and services.

Personal information of all clients of the pharmacy are stored in accordance with the relevant legislation. Any personal information that is no longer required for operation, security or record purposes shall be destroyed by deleting it from the electronic systems or by shredding paper-based documents.

Where applicable to Healthchem's operations, information is stored in accordance with the following legislation, including but not limited to:

- Companies Act 71 of 2008
- Income Tax Act 58 of 1962
- Value-Added Tax Act 89 of 1991
- Skills Development Levies Act 9 of 1999
- Medical Schemes Act 131 of 1998
- Insurance Act 18 of 2017
- Employment Equity Act 55 of 199
- Unemployment Insurance Contributions Act 4 of 2002
- Unemployment Insurance Act 63 of 2001
- Occupational Health and Safety Act 85 of 1993
- Compensation for Occupational Injuries and Diseases Act 130 of 1993
- Labour Relations Act 66 of 1995
- Basic Conditions of Employment Act 75 of 1997
- National Minimum Wage Act 9 of 2018
- Competition Act 89 of 1998
- National Payment System Act 78 of 1998
- Protection of Personal Information Act 4 of 2013
- Promotion of Access to Information Act 2 of 2000
- Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000
- National Credit Act 34 of 2005
- Consumer Protection Act 68 of 2008
- Identification Act 68 of 1997
- Corruption Act 94 of 1992
- Financial Intelligence Centre Act 38 of 2001
- Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
- Disaster Management Act 57 of 2002
- Financial Institutions (Protection of Funds) Act 28 of 2001

7. Safeguarding the information and the integrity of the information

The paper-based information is kept in locked cabinets and the keys of the cabinets are managed to allow only authorised personnel access to the information as and when required to perform their duties.

All electronic information is kept on servers, which is accessed from the respective computers of employees who has authorised access to the relevant data base. All computers of Healthchem are password protected and only accessible by the user of the specific computer.

None of the computers are remotely accessible from other locations.

All personal information is furthermore safeguarded as described in the agreements entered into with the service providers of Information Technology and Security services.

8. The process of collecting information

Although it is not required that the consent of clients be obtained before their information is collected, it is important that the clients are informed that their information is collected, what information is collected and the reasons and purpose for the collection and processing, as well as how the information will be protected. A notice to this effect is circulated to all relevant parties and will form part of the new clients' application / contract for service from Healthchem.

9. Rights of Data Subjects

The individual data subjects have the right to:

(a) access their own data

(b) change or update it to ensure that the responsible party is always holding the latest and correct information

(c) request that it be deleted if it is no longer required for the purpose for which it was collected

(d) object to direct marketing

(e) be notified if data is compromised; and

(f) lay a complaint with the Information Regulator if the responsible party is not compliant with the POPI Act

When Personal Information is collected, the Data Subject has the following right:

At a minimum, they should be told:

- what information will be collected
- the reasons or purpose for collection and processing
- who their information will be sent to, if any
- any laws or requirements authorising such collection

10. Compliance with the eight conditions for the lawful processing of personal information

Healthchem may lawfully process personal information if it complies with the eight conditions as required by the POPI Act. The provisions of the eight conditions are complied with and are as follows:

10.1 Condition 1: Accountability dealt with in section 8 of the POPI Act

The Responsible Party is tasked to ensure that the eight conditions set out in Chapter 3 of the POPI Act, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of processing and during the processing itself.

The Responsible Party means a private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information. In this instance the responsible party is Healthchem and its Board of Directors who determines the purpose and means for processing personal information.

The Directors are tasked with the responsibility of compliance in the company and has subsequently appointed the General Manager, Francois Deneys Zeederberg as the Information Officer. A Deputy Information Officer will be appointed to assist with the responsibility of complying with the legislation. The registration of the Information Officer and Deputy Information Officer will be submitted to the Information Regulator as soon as the portal is available.

To ensure compliance, this Framework was prepared and the continued implementation thereof will be the responsibility of the Information Officer and be overseen by the Directors.

10.2 Condition 2: Processing limitation dealt with in sections 9 to 12 of the POPI Act

Personal information must be collected directly from the data subject, except if the information is contained in, or derived from a public record or deliberately made public by the data subject or if the data subject gave consent to the collection of the information from another source and the collection of the information from the other source will not prejudice a legitimate interest of the data subject. The Responsible Party may collect personal information from another source than the data subject if the collection thereof from the data subject would prejudice a lawful purpose of the collection or if it is not reasonably practicable in the circumstances of the particular case.

Personal Information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject. Considering the purpose for which the personal information is processed, it may only be processed if it is adequate, relevant and not excessive.

Personal information may only be processed if one of the following was complied with:

(a) The data subject consents to the processing (The Responsible Party bears the burden of proof that the data subject consented to the processing as referred to in this subsection and the data subject may withdraw the consent at any time, provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1)(b) to (f) will not be affected.)

(b) Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party

(c) Processing complies with an obligation imposed by law on the responsible party

(d) Processing protects a legitimate interest of the data subject

(e) Processing is necessary for the proper performance of a public law by a public body

(f) Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied

A data subject may, at any time, object to the processing of personal information, but only:

(a) in terms of subsection 1(d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

(b) for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69

10.3 Condition 3: Purpose specification as dealt with in section 13 and 14 of the POPI Act

Personal Information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Responsible Party. The data subject must be made aware of the purpose of the collection of the information (see section18(1)) unless the provisions of section 18(4) are applicable.

Section 18(4) provides that it is not necessary for a responsible party to comply with notifying a data subject if:

(a) The data subject has provided consent for the non-compliance

(b) Non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of the Act

(c) Non-compliance is necessary –

  (i) To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences

  (ii) To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, Act 34 of 1997

  (iii) For the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

  (iv) In the interest of national security

(d) compliance would prejudice a lawful purpose of the collection

(e) compliance is not reasonably practicable in the circumstances of the particular case; or

(f) The information will –

  (i) not be used in a form in which the data subject may be identified; or

  (ii) be used for historical, statistical or research purposes

Records of Personal Information must not be retained any longer than is necessary for achieving the purposes for which the information was collected or subsequently processed, unless:

(a) retention of the record is required or authorised by law

(b) the responsible party reasonably requires the record for lawful purposes related to its functions and activities

(c) retention of the record is required by a contract between the parties thereto; or

(d) the data subject has consented to the retention of the record.

The responsible party may retain records of personal information for periods in excess of those indicated above for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.

If the responsible party used a record of personal information of a data subject to make a decision about the data subject, the responsible party must:

(a) retain the record for such a period as may be required or prescribed by law; or

(b) if there is no law prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record

After the responsible party is no longer authorised to retain the record in terms of this subsections, the responsible party must destroy, delete or de-identify the record of personal information as soon as reasonably practicable and such destruction or deletion of the record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

Processing of personal information must be restricted by the responsible party:

(a) for a period to enable the responsible party to verify the accuracy of the information, if its accuracy is contested by the data subject

(b) if the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof

(c) if the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

(d) if the data subject requests to transmit the personal data into another automated processing system

Personal Information so restricted may, with the exception of storage, only be processed for purposes of proof, or with the data subject’s consent, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

The responsible party must inform the data subject before the abovementioned restriction on processing is lifted.

10.4 Condition 4: Further processing limitation dealt with in section 15 of the POPI Act

Personal Information may not be processed for a secondary purpose unless the further processing is in accordance or compatible with the original purpose for which it was collected. To assess whether the further processing is compatible with the purpose of collection, the responsible party must take account of:

(a) The relationship between the purpose of the intended further processing and the purpose for which the information has been collected

(b) The nature of the information concerned

(c) The consequences of the intended further processing for the data subject

(d) The manner in which the information has been collected; and

(e) Any contractual rights and obligations between the parties

Further processing of personal information is not incompatible with the purpose of collection if:

(a) The data subject has consented to the further processing of the information

(b) The information is available in or derived from a public record or has deliberately been made public by the data subject

(c) Further processing in necessary:

    (i) To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences

    (ii) To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, Act 34 of 1997

    (iii) For the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

    (iv) In the interest of national security

(d) The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to:

(i) Public health or public safety; or

(ii) The life or health of the data subject or another individual

(e) The information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or

(f) The further processing of information is in accordance with an exemption granted under section 37 by the Regulator

10.5 Condition 5: Information quality as dealt with in section 16 of the POPI Act

The responsible party must take reasonable practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, while having regard to the purpose for which the personal information was collected or further processed.

The nature and purpose of the Personal Information will dictate as to how often such Personal Information must be updated.

Healthchem will obtain personal information directly from the data subject and will validate it while capturing such. Information will be audited twice annually, but the data subjects may approach the office at any time during office hours to update their contact or address details.

10.6 Condition 6: Openness as dealt with in sections 17 and 18 of the POPI Act

Healthchem complies with section 51 of the Promotion of Access to Information Act, and an Access to Information Manual was accordingly prepared and approved.

The responsible party must take reasonable practicable steps to ensure that the data subject is aware of:

(i) the information being collected and where the information is not collected from the data subject, the source from which it is collected

(ii) the name and address of the responsible party

(iii) the purpose for which the information is being collected

(iv) whether or not the supply of the information by the data subject is voluntary and or mandatory

(v) the consequences of failure to provide the information

(vi) the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation

(vii) any further information such as the:

(i) recipient or category of recipients of the information

(ii) nature or category of the information

(iii) existence of the right of access to and the right to rectify the information collected

(iv) existence of the right to object to the processing of personal information as referred to in section 11(3); and

(v) right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator

which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

The abovementioned steps must be taken:

(a) If the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to; or

(b) In any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

If these steps were previously taken by the responsible party, the responsible party complies with these provisions in relation to subsequent collection from the data subject of the same information or information of the same kind if the purpose of the collection of the information remains the same.

10.7 Condition 7: Security safeguards as dealt with in sections 19 to 22 of the POPI Act

The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information.

To give effect to this, the responsible party must take reasonable measures to:

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control

(b) establish and maintain appropriate safeguards against the risks identified

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

An operator or anyone processing personal information on behalf of a responsible party or an operator, must process such information only with the knowledge or authorisation of the responsible party and treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.

The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person. In such a case, the responsible party must notify the Regulator and the data subject (except if the Regulator or a relevant public body delay notification), unless the identity of such data subject cannot be established.

Notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

(a) mailed to the data subject’s last known physical or postal address

(b) sent by e-mail to the data subject’s last known e-mail address

(c) placed in a prominent position on the website of the responsible party

(d) published in the news media; or

(e) as may be directed by the Regulator

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:

(a) a description of the possible consequences of the security compromise

(b) a description of the measures that the responsible party intends to take or has taken to address the security compromise

(c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise

(d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information

The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

10.8 Condition 8: Data subject participation as dealt with in section 23 to 25 of the POPI Act

A data subject, after provided adequate proof of identity, has the right to:

(a) request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and

(b) request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have had, access to the information-

(i) within a reasonable time

(ii) at a prescribed fee, if any

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable

If in response to a request, personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 24 to request the correction of information.

If a data subject is required by a responsible party to pay a fee for services provided to the data subject to enable the responsible party to respond to a request, the responsible party must give the data subject a written estimate of the fee before providing the services and may require the applicant to pay a deposit for all or part of the fee.

A responsible party may or must refuse, as the case may be, to disclose any information requested in terms of subsection (1) to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act apply. Similarly, the provisions of sections 30 and 61 of the Promotion of Access to Information Act are applicable in respect of access to health or other records. If a request for access to personal information is made to a responsible party and part of that information may or must be refused, every other part must be disclosed.

A data subject may, in the prescribed manner, request a responsible party to:

(a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(b) destroy or delete a record of personal information about a data subject that the responsible party is no longer authorised to retain in terms of section 14

The responsible party must, as soon as reasonably practicable, on receipt of such a request:

(a) correct the information

(b) destroy or delete the information

(c) provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or

(d) where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

If the responsible party has taken steps that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.

The responsible party must notify a data subject, who has made a request of the action taken as a result of the request.

The provisions of sections 18 and 53 of the Promotion of Access to Information Act apply to requests made in terms of section 23 of the POPI Act.