

SAFELINE PHARMACEUTICALS
REGISTRATION NO. 1997/05185/07

COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE
PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013

1. INTRODUCTION

1.1 The Protection of Personal Information Act (“POPI”) is intended to balance two competing interests. These are:

1.1.1 the constitutional right to privacy (which requires personal information to be protected);
and

1.1.2 the need for our society to have access to and to process (and work with) personal information for legitimate purposes including, *inter alia*, conducting business.

1.2 This Compliance Manual sets out the framework for Safeline Pharmaceuticals’ Company’s compliance with POPI.

1.3 Where reference is made to the “processing” of personal information, this will include any activity in which the information is worked with, from the time that the information is

collected, up to the time that the information is destroyed, regardless of whether the information is worked with manually or by automatic means.

2. OUR OBLIGATIONS TO OUR CLIENTS

- 2.1 We undertake to adhere to the provisions of POPI at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of our clients.
- 2.2 We undertake to process information only for the purpose for which it is intended and to enable us to provide the services agreed with our clients.
- 2.3 Whenever necessary, we shall obtain consent to process personal information of our clients.
- 2.4 Where we do not seek consent, the processing of our client's personal information will be in terms of a legal obligation placed upon us, the conclusion or performance of our agreement with our client or to protect a legitimate interest of our client that requires protection.
- 2.5 We shall stop processing personal information if the required consent of our client is withdrawn, or if a legitimate and reasonable objection by our client is raised.
- 2.6 We shall collect personal information directly from the client whose information we require, unless:
 - 2.6.1 the information is derived from a public record or has been made public by the client; or

- 2.6.2 the client has consented to the collection of his/her/its personal information from another source; or
 - 2.6.3 the collection of the information from another source does not prejudice the client; or
 - 2.6.4 the information to be collected is necessary for the maintenance of law and order and/or national security; or
 - 2.6.5 the information is being collected to comply with a legal or statutory obligation, including an obligation to the South African Revenue Service; or
 - 2.6.6 the information collected is required for the conduct of proceedings in any court or tribunal, where these proceedings have commenced or are reasonably contemplated; or
 - 2.6.7 the information is required to maintain our legitimate interests or the legitimate interests of a third party to whom the information is supplied; or
 - 2.6.8 where requesting consent from the client would prejudice the purpose of the collection of the information; or
 - 2.6.9 where requesting consent is not reasonably practical in the prevailing circumstances.
- 2.7 We shall advise our clients of the purpose of the collection of their personal information.
- 2.8 We shall retain records of the personal information we have collected for the minimum period as required by law unless the client has furnished his/her/its consent or instructed us to retain the records for a longer period.

- 2.9 We shall destroy or delete records of the personal information (so as to de-identify the client) as soon as reasonably possible after the time period for which we were entitled to hold the records has expired.
- 2.10 We shall restrict the processing of personal information:
- 2.10.1 where the accuracy of the information is contested by the client, for a period sufficient to enable us to verify the accuracy of the information; or
 - 2.10.2 where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for the purposes of proof; or
 - 2.10.3 where the processing of personal information was unlawful and the client requests that the personal information is not destroyed or deleted, but rather retained; or
 - 2.10.4 where the client requests that the personal information be transmitted to another automated data processing system.
- 2.11 The further processing of personal information shall only be undertaken:
- 2.11.1 if the requirements of paragraphs 2.3; 2.6.1; 2.6.4; 2.6.5 or 2.6.6 above have been met;
 - 2.11.2 where the further processing is necessary because of a threat to public health or public safety or to the life or health of the client, or a third party;
 - 2.11.3 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or

2.11.4 where there has been an exemption from the Information Regulator appointed in terms of POPI.

2.12 We undertake to ensure that the personal information which we collect and process is complete, accurate, not misleading and up to date (where necessary).

2.13 We undertake to maintain records (whether physical or electronic) of all processing operations relating to the personal information.

2.14 When we accept a new mandate, instruction or conclude an agreement of any sort with a client, that client will be advised of the existence of this manual and our duties and obligations in terms of POPI.

3. OUR CLIENT'S RIGHTS

3.1 In cases where our client's consent is required to process their personal information, this consent may be withdrawn.

3.2 In cases where we process personal information without a client's consent in terms of a legal obligation placed upon us, the conclusion or performance of our mandate by or agreement with our client or to protect a legitimate interest of our client that requires protection, the client has the right to object to such processing.

3.3 All clients are entitled to lodge a complaint regarding our compliance with POPI with the Information Regulator.

3.4 We will obtain our client's prior written consent prior to us processing their personal information while we do our work for them, unless this consent has been obtained previously from the client or is contained in another document signed by the client.

4. SECURITY SAFEGUARDS

4.1 In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, we have the and/or will implement (where appropriate and within a reasonable time) the following security safeguards:

4.1.1 Our business premises where records are kept are protected by access control, burglar alarms and armed response.

4.1.2 Our archived files are stored in a secure storage facility protected by access control, burglar alarms and armed response.

4.1.3 All the user terminals on our internal computer network and our servers are protected by passwords which are changed on a regular basis.

4.1.4 Our email infrastructure complies with industry standard security safeguards and meets the General Data Protection Regulation (GDPR) which is standard in the European Union.

4.1.5 Vulnerability assessments are carried out on our digital infrastructure at least on an annual basis to identify weaknesses in our systems and to ensure we have adequate security measures in place.

4.1.6 We use an internationally recognised Firewall to protect the data on our local servers.

- 4.1.7 Our staff will be trained to carry out their duties in compliance with POPI, and this training will be ongoing.
- 4.1.8 It will be a term of the contract with every staff member that they must maintain full confidentiality in respect of all of our clients' affairs, including our clients' personal information.
- 4.1.9 Employment contracts for staff whose duty it is to process a client's personal information will be amended to include an obligation on the staff member (1) to maintain our security measures, and (2) to notify our information officer immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person.
- 4.1.10 The processing of the personal information of our employees will take place in accordance with the rules contained in the relevant labour legislation.
- 4.1.11 The digital work profiles and privileges of employees who have left our employ have and will continue to be properly terminated.
- 4.1.12 The personal information of clients and staff will be destroyed timeously in a manner that de-identifies the person.
- 4.2 These security safeguards will be verified on a regular basis to ensure effective implementation, and these safeguards will be continually updated in response to new risks and/or any identified deficiencies.

5. SECURITY BREACHES

- 5.1 Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, we will notify the Information Regulator and the relevant client, unless we are no longer able to identify the client. This notification will take place as soon as reasonably possible.
- 5.2 Such notification will be given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the client to be delayed.
- 5.3 Our notification to the client will be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the client:
- 5.3.1 by mail to the client's last known physical or postal address; or
 - 5.3.2 by email to the client's last known email address; or
 - 5.3.3 by publication on our website; or
 - 5.3.4 in any other manner as directed by the Information Regulator.
- 5.4 Our notification to the client will provide the client with sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and will include:
- 5.4.1 a description of the possible consequences of the security breach;
 - 5.4.2 details of the measures that we intend to take or have taken to address the security breach;

5.4.3 any recommendation as to what we believe the client could do to mitigate the adverse effects of the security breach; and

5.4.4 if known, the identity of the person who may have accessed, or acquired the personal information.

6. PROCEDURE IN RELATION TO A REQUEST FOR RECORDS

6.1 On production of proof of identity, any person is entitled to request that we confirm, free of charge, whether or not we hold any personal information about that person in our records.

6.2 If we hold such personal information, on request, and upon payment of a fee of R1,500.00 (one thousand five hundred Rand) plus VAT, we shall provide the person with the record, or a description of the personal information, including information about the identity of all third parties or categories of third parties who have or have had access to the information. We shall do this within a reasonable period of time, in a reasonable manner and in an understandable form.

6.3 A client requesting such personal information will also be advised of their right to request to have any errors in the personal information corrected, which request shall be made in writing and in a reasonable manner and in an understandable form.

6.4 In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have a discretion as to whether or not to do so.

6.5 In all cases where the disclosure of a record will entail the disclosure of information that is additional to the personal information of the person requesting the record, the written consent of our Information Officer (or his or her delegate) will be required, and that person shall make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.

6.6 If a request for personal information is made and part of the requested information may, or must, be refused, every other part not affected thereby will still be disclosed.

7. PROCEDURE IN RELATION TO THE CORRECTION OF PERSONAL INFORMATION

7.1 A client is entitled to require us to correct or delete personal information that we have which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

7.2 A client is also entitled to require us to destroy or delete records of personal information about the client that we are no longer authorised to retain.

7.3 Any such request must be made in writing and in a reasonable manner and in an understandable form.

7.4 Upon receipt of such a lawful request, we shall comply therewith as soon as reasonably practicable.

7.5 In the event that a dispute arises regarding the client's rights to have information corrected, and in the event that the client so requires, we shall attach to the information, in a way that it

will always be read with the information, an indication that the correction of the information has been requested but has not been made.

7.6 We shall notify the client who has made a request for their personal information to be corrected or deleted what action we have taken as a result of such a request.

8. SPECIAL PERSONAL INFORMATION

8.1 Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.

8.2 We shall not process any of this special personal information without the client's consent, except where this is necessary for the establishment, exercise or defense of a right or an obligation in law.

9. PROCEDURE IN RELATION TO THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

We will only process the personal information of a child if we have the consent of the child's parent or legal guardian.

10. OUR INFORMATION OFFICER

10.1 Our Information Officer is _____. Our Information Officer's responsibilities include:

10.1.1 Ensuring compliance with POPI.

10.1.2 Dealing with requests which we receive in terms of POPI.

- 10.1.3 Working with the Information Regulator in relation to any investigations in terms of POPI.
- 10.2 Our Information Officer will designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in paragraph 10.1 above. Currently the Deputy Information Officer of Safeline Pharmaceuticals is _____.
- 10.3 Our Information Officer and our Deputy Information Officer are registered with the Information Regulator.
- 10.4 In carrying out our duties, our Information Officer shall ensure that:
- 10.4.1 this Compliance Manual is implemented;
 - 10.4.2 an assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
 - 10.4.3 that this Compliance Manual is developed, monitored, maintained and made available;
 - 10.4.4 that internal measures are developed together with adequate systems to process requests for information or access to information;
 - 10.4.5 that internal awareness sessions are conducted regarding the provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator;
- and

10.4.6 that copies of this compliance manual are provided to persons at their request, hard copies to be provided upon payment of a fee (to be determined by the Information Regulator).

10.5 Guidance notes on Information Officers have been published by the Information Regulator (on 1 April 2021) and our Information Officer and deputy Information Officer shall familiarize themselves with the content of these guidance notes.

11. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

11.1 In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:

11.1.1 in the event that we intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;

11.1.2 if we are processing information on criminal behaviour or unlawful or objectionable conduct;

11.1.3 if we are processing information for the purposes of credit reporting,

11.1.4 if we are transferring special personal information or the personal information of children to a third party in a foreign country that does not provide adequate protection of that personal information.

11.2 The Information Regulator shall be notified of our intention to process any personal information as set out in paragraph 11.1 above prior to any processing taking place and we may not commence with such processing until the Information Regulator has confirmed that we may do so. The Information Regulator has 4 weeks to make a decision but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator, which must not exceed 13 weeks. If the Information Regulator does not make a decision within the stipulated time periods, we shall be entitled to assume that the decision is in our favour and commence processing the information.

12. DIRECT MARKETING

12.1 We shall only carry out direct marketing (using any form of electronic communication) to clients if:

12.1.1 The client was given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected; and

12.1.2 The client did not object then or at any time after receiving any such direct marketing communications from us.

13. We shall only approach clients using their personal information if we have obtained their personal information in the context of providing services associated with our company to them, and we may then only market related services to them.

14. We may only carry out direct marketing (using any form of electronic communication) to other people if we have received their consent to do so.

15. We may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent.
16. A request for consent to receive direct marketing must be made in the prescribed manner and form.
17. All direct marketing communications must disclose our identity and contain an address or other contact details to which the client may send a request that the communications cease.

18. **TRANSBORDER INFORMATION FLOWS**

- 18.1 We may not transfer a client's personal information to a third party in a foreign country, unless:
 - 18.1.1 the client consents to this, or requests it; or
 - 18.1.2 such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country; or
 - 18.1.3 the transfer of the personal information is required for the performance of the contract between us and the client; or
 - 18.1.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between us and the third party; or

18.1.5 the transfer of the personal information is for the benefit of the client and it is not reasonably possible to obtain their consent and that if it were possible the client would be likely to give such consent.

19. OFFENCES AND PENALTIES

19.1 POPI makes provision for serious penalties for the contravention of its terms. For minor offences a guilty party can receive a fine or be imprisoned for up to 12 months. For serious offences the period of imprisonment rises to a maximum of 10 years. Administrative fines for the company can reach a maximum of R10 million.

19.2 Breaches of this Compliance Manual will also be viewed as a serious disciplinary offence.

19.3 It is therefore imperative that we comply strictly with the terms of this Compliance Manual and protect our client's personal information in the same way as if it was our own.

SAFELINE PHARMACEUTICALS (PTY) LTD