Clinix Health Management (Pty) Ltd Privacy Policy and Statement

Terms of engagement between Us and You / the Data Subject in relation to the Processing of Personal Information

Introduction

This document describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service and tells You about Your privacy rights and how the law protects You and these are the terms of engagement that You consent to in and through and with your interaction with Us with Your personal information.

We use Your Personal data to provide and improve the Service and for the advancement of Your healthcare and the health of our other patients and our community.

As part of the above purpose, we also use Personal Information:

to be able to communicate with you,

to be able to keep your information accurate and up to date,

to improve on our relationship with you,

to maintain and improve our Operational and IT services, including this website,

to comply with our legislative duties.

Agreement and consent

By using the Service and engaging with us and sharing your personal information with us, You agree to the collection and use of information in accordance with this Privacy Policy.

Mission statement:

The purpose of this Policy is to:

give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—

balancing the right to privacy against other rights, particularly the right of access to information; and

protecting important interests, including the free flow of information within the Republic and across international borders;

adhere to the regulated manner in which personal information may be processed, by established conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

safeguard the rights of persons with rights and remedies to protect their personal information from processing that is not in accordance with the relevant legislation; and

adhere to established voluntary and compulsory measures, including the Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by the relevant legislation;

for us to remain mindful of Our duties to Our patients relating to their privacy, as provided for in relevant legislation, including, but not limited to:

The Constitution;

14. Privacy

Everyone has the right to privacy, which includes the right not to have—

(d) the privacy of their communications infringed.

The National Health Act, 2003 (Act No. 61 of 2003):

Chapter 2 : Rights and Duties of Users and Health Care Personnel

Section 14. Confidentiality

(1) All information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment, is confidential.

(2) Subject to section 15, no person may disclose any information contemplated in unless—

(a) the user consents to that disclosure in writing;

(b) a court order or any law requires that disclosure; or

(c) non-disclosure of the information represents a serious threat to public health.

Mental Health Care Act, 2002 (Act No. 17 of 2002)

Chapter III : Rights and Duties relating to Mental Health Care Users

8. Respect, human dignity and privacy

1) The person, human dignity and privacy of every mental health care user must be respected.

Other legislation that is of relevance and which is incorporated herein, that are set out infra herein;

and in terms of Our Ethical Values and Codes of Conduct as Medical Service Providers.

Application:

This Policy applies to the processing of personal information—

entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and

where the responsible party is—

domiciled in the Republic; or

not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

This policy applies, subject to paragraph (b), to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object, or a specific provision, of this Act.

If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Chapter 3 of POPIA, the extensive conditions prevail.

This Policy must be interpreted in a manner that—

gives effect to the purpose of POPIA set out in section 2 thereof; and

does not prevent any public or private body from exercising or performing its powers, duties and functions in terms of the law as far as such powers, duties and functions relate to the processing of personal information and such processing is in accordance with this Act or any other legislation, as referred to in subsection (2), that regulates the processing of personal information.

This Policy does not apply to information:

in the course of a purely personal or household activity;

That has been de-identified to the extent that it cannot be re-identified again;

By or on behalf of a public body—

Which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or

The purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;

By the Cabinet and its committees or the Executive Council of a province; or

Relating to the judicial functions of a court referred to in section 166 of the Constitution.

‘‘Terrorist and related activities’’, for purposes of subsection (1)(c), means those activities referred to in section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004).

Interpretation and Definitions

Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions

For the purposes of this Privacy Policy:

Account means a unique account created for You to access our Service or parts of our Service;

Associated Company means any Company in the Clinix Health Group, including but not limited to the companies representing the individual hospitals in the Group and Clinix Health Academy (Pty) Ltd and Clinix Health Group (Pty) Ltd., all of which are deemed to have accepted the benefits of this Policy;

Application means the software program provided by Us, downloaded by You on any electronic device, named Clinix Health Group App;

‘‘Automated” means any equipment capable of operating automatically in response to instructions given for the purpose of processing information;

“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;

‘‘child’’ means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;

‘‘code of conduct’’ means a code of conduct issued in terms of Chapter 7;

Company (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to Clinix Health Management (Pty) Ltd, Head Office: 50 Sixth road, Block C, Hyde Park, Johannesburg, and its associated companies;

‘‘competent person’’ means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;

‘‘consent’’ means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

‘‘Constitution’’ means the Constitution of the Republic of South Africa, 1996;

Cookies are small files that are placed on Your computer, mobile device or any other device by a website, containing the details of Your browsing history on that website among its many uses;

Country refers to South Africa;

‘‘data subject’’ means You, and / or the person to whom personal information relates;

Device means any device that can access the Service such as a computer, a cellphone or a digital tablet;

‘‘de-identify’’, in relation to personal information of a data subject, means to delete any information that—

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and ‘‘de-identified’’ has a corresponding meaning;

‘‘direct marketing’’ means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

(a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

(b) requesting the data subject to make a donation of any kind for any reason;

‘‘electronic communication’’ means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;

‘‘enforcement notice’’ means a notice issued in terms of section 95;

‘‘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;

‘‘information matching programme’’ means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;

‘‘information officer’’ of, or in relation to, a—

(a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or

(b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

‘‘Minister’’ means the Cabinet member responsible for the administration of justice;

‘‘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;

‘‘person’’ means a natural person or a juristic person;

Personal Data is any information that relates to an identified or identifiable individual;

‘‘personal information’’ means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) 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;

(g) the views or opinions of another individual about the person; and

(h) 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;

‘‘prescribed’’ means prescribed by regulation or by a code of conduct;

‘‘private body’’ means—

(a) a natural person who carries or has carried on any trade, business or

profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person, but excludes a public body;

‘‘processing’’ means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

‘‘professional legal adviser’’ means any legally qualified person, whether in private practice or not, who lawfully provides a client, at his or her or its request, with independent, confidential legal advice;

‘‘Promotion of Access to Information Act / POPIA’’ means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

‘‘public body’’ means—

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(b) any other functionary or institution when—

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a public power or performing a public function in terms of any

legislation;

‘‘public record’’ means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

‘‘record’’ means any recorded information—

(a) regardless of form or medium, including any of the following:

(i) Writing on any material;

(ii) 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;

(iii) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) 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;

(b) in the possession or under the control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence;

‘‘Regulator’’ means the Information Regulator established in terms of section 39;

‘‘re-identify’’, in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and ‘‘re-identified’’ has a corresponding meaning;

‘‘Republic’’ means the Republic of South Africa;

‘‘responsible party’’ means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

‘‘restriction’’ means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

Service refers to the Application or the Website or both;

Service Provider means any natural or legal person who processes the data on behalf of Us. It refers to third-party companies or individuals employed by Us to facilitate the Service, to provide the Service on behalf of Us, to perform services related to the Service or to assist Us in analyzing how the Service is used;

‘‘special personal information’’ means personal information relating to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject;

‘‘this Act’’ includes any regulation or code of conduct made under this Act; and

Third-party Social Media Service refers to any website or any social network website through which a User can log in or create an account to use the Service.

‘‘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;

Usage Data refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).

Website refers to Clinix Health Group website, accessible from "www.clinix.co.za"

You means the individual accessing or using the Service, or Us, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.

Collection and Usage of Your Personal Data

Types of Data Collected

Personal Data

While using Our Service, We may ask You to provide Us with certain personally identifiable information that can be used to contact or identify You. Personally identifiable information may include, but is not limited to:

Names and Surname

ID Number and Passport number or asylum seeker number

Health Status, including but not limited to your actual or possible exposure to COVID-19

Location data

Employment status, for instance whether you are an employee or associated medical specialist of Clinix

If a staff member:

Area of work

Staff type

Employee number

Whether you are a representative of a service provider or product supplier

Email address

Phone numbers

Address, State, Province, Postal code, City

Professional Registration details, i.e. HPCSA

Feedback and survey responses;

Communication preferences.

Usage Data

Usage Data is collected automatically when using the Service.

Usage Data may include information such as Your Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When You access the Service by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device You use, Your mobile device unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data.

We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

Information from Third-Party Social Media Services

We allow You to create an account and log in to use the Service through the following Third-party Social Media Services:

Google

Facebook

Twitter

If You decide to register through or otherwise grant us access to a Third-Party Social Media Service, We may collect Personal data that is already associated with Your Third-Party Social

Media Service's account, such as Your name, Your email address, Your activities or Your contact list associated with that account.

You may also have the option of sharing additional information with Us through Your Third-Party Social Media Service's account. If You choose to provide such information and Personal Data, during registration or otherwise, You are giving Us permission to use, share, and store it in a manner consistent with this Privacy Policy.

Information Collected while Using the Application.

While using Our Application, in order to provide features of Our Application, We may collect, with Your prior permission:

Information regarding your location;

Information from your Device's phone book (contacts list);

Pictures and other information from your Device's camera and photo library;

CCTV footage: There is CCTV coverage in certain areas on Clinix premises for purposes of Your and Our Security and to make it possible for us to manage our operations effectively in Your and Our best interest.

We use this information to provide features of Our Service, to improve and customize Our Service. The information may be uploaded to Our servers and/or a Service Provider's server or it may be simply stored on Your device;

You can enable or disable access to this information at any time, through Your Device settings.

Tracking Technologies and Cookies

We use Cookies and similar tracking technologies to track the activity on Our Service and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyze Our Service. The technologies We use may include:

Cookies or Browser Cookies. A cookie is a small file placed on Your Device. You can instruct Your browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if You do not accept Cookies, You may not be able to use some parts of our Service. Unless you have adjusted Your browser setting so that it will refuse Cookies, our Service may use Cookies.

Flash Cookies. Certain features of our Service may use local stored objects (or Flash Cookies) to collect and store information about Your preferences or Your activity on our Service. Flash Cookies are not managed by the same browser settings as those used for Browser Cookies.

Web Beacons. Certain sections of our Service and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit Us, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on Your personal computer or mobile device when You go offline, while Session Cookies are deleted as soon as You close Your web browser. Learn more about cookies:

We use both Session and Persistent Cookies for the purposes set out below:

Necessary / Essential Cookies

Type: Session Cookies

Purpose: These Cookies are essential to provide You with services available through the Website and to enable You to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that You have asked for cannot be provided, and We only use these Cookies to provide You with those services.

Cookies Policy / Notice Acceptance Cookies

Type: Persistent Cookies

Administered by: Us

Purpose: These Cookies identify if users have accepted the use of cookies on the Website.

Functionality Cookies

Type: Persistent Cookies

Administered by: Us

Purpose: These Cookies allow us to remember choices You make when You use the Website, such as remembering your login details or language preference. The purpose of these Cookies

is to provide You with a more personal experience and to avoid You having to re-enter your preferences every time You use the Website.

For more information about the cookies we use and your choices regarding cookies, please visit our Cookies Policy or the Cookies section of our Privacy Policy.

Accountability:

We will abide by the following conditions for the lawful processing of personal information:

As Responsible Party we will ensure that the conditions for the lawful processing of personal information are complied with at the time of the determination of the purpose and means of the processing and during the processing itself, and We will abide by the following conditions for the lawful processing of personal information:

Processing limitation:

We will ensure that Personal information will be processed

lawfully; and

in a reasonable manner that does not infringe the privacy of the data subject.

Purpose specification:

We will only process personal information if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

Further processing limitation:

We will ensure that the further processing of personal information will be in accordance or compatible with the purpose for which it was collected.

To assess whether further processing is compatible with the purpose of collection, we as responsible party will take account of:

the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

the nature of the information concerned;

the consequences of the intended further processing for the data subject;

the manner in which the information has been collected; and

any contractual rights and obligations between Us and You.

It should be noted that the further processing of personal information will not incompatible with the purpose of collection if—

the data subject or a competent person where the data subject is a child has consented to the further processing of the information;

the information is available in or derived from a public record or has deliberately been made public by the data subject;

further processing will be necessary—

to avoid prejudice to the upholding of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;

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, 1997 (Act No. 34 of 1997);

for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

in the interests of national security;

the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to—

public health or public safety; or

the life or health of the data subject or another individual;

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

the further processing of the information is in accordance with an exemption granted under section 37 of POPIA.

The prohibition on processing personal information concerning a data subject's religious or philosophical beliefs, as referred to in section 26, does not apply if the processing is carried out by:

spiritual or religious organisations, or independent sections of those organisations if—

the information concerns data subjects belonging to those organisations;

or

it is necessary to achieve their aims and principles;

institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or

other institutions: Provided that the processing is necessary to protect the spiritual welfare of the data subjects, unless they have indicated that they object to the processing.

In the cases referred to in subsection (1)(a), the prohibition does not apply to processing of personal information concerning the religion or philosophy of life of family members of the data subjects, if:

the association concerned maintains regular contact with those family members in connection with its aims; and

the family members have not objected in writing to the processing.

In the cases referred to in subsections (1) and (2), personal information concerning a data subject's religious or philosophical beliefs may not be supplied to third parties without the consent of the data subject.

Authorisation concerning data subject's race or ethnic origin

The prohibition on processing personal information concerning a data subject's race or ethnic origin, as referred to in section 26, does not apply if the processing is carried out to—

identify data subjects and only when this is essential for that purpose; and

comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

Authorisation concerning data subject's trade union membership

The prohibition on processing personal information concerning a data subject's trade union membership, as referred to in section 26, does not apply to the processing by the trade union to which the data subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union or trade union federation.

In the cases referred to under subsection (1), no personal information may be supplied to third parties without the consent of the data subject.

Authorisation concerning data subject's political persuasion

The prohibition on processing personal information concerning a data subject's political persuasion, as referred to in section 26, does not apply to processing by or for an institution, founded on political principles, of the personal information of—

its members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution; or

a data subject if such processing is necessary for the purposes of—

forming a political party;

participating in the activities of, or engaging in the recruitment of members for or canvassing supporters or voters for, a political party with the view to—

an election of the National Assembly or the provincial legislature as regulated in terms of the Electoral Act, 1998 (Act No. 73 of 1998);

municipal elections as regulated in terms of the Local Government: Municipal Electoral Act, 2000 (Act No. 27 of 2000); or

a referendum as regulated in terms of the Referendums Act, 1983 (Act No. 108 of 1983); or

campaigning for a political party or cause.

In the cases referred to under subsection (1), no personal information may be supplied to third parties without the consent of the data subject.

Authorisation concerning data subject's health or sex life

The prohibition on processing personal information concerning a data subject's health or sex life, as referred to in section 26, does not apply to the processing by—

medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;

insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for—

assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing;

the performance of an insurance or medical scheme agreement; or

the enforcement of any contractual rights and obligations;

schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;

any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;

any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or

administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for—

the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or

the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

In the cases referred to under subsection (1), the information may only be processed by responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject.

A responsible party that is permitted to process information concerning a data subject's health or sex life in terms of this section and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, must treat the information as confidential, unless the responsible party is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information in accordance with subsection (1).

The prohibition on processing any of the categories of personal information referred to in section 26, does not apply if it is necessary to supplement the processing of personal information concerning a data subject's health, as referred to under subsection (1)(a), with a view to the proper treatment or care of the data subject.

Personal information concerning inherited characteristics may not be processed in respect of a data subject from whom the information concerned has been obtained, unless—

a serious medical interest prevails; or

the processing is necessary for historical, statistical or research activity.

More detailed rules may be prescribed concerning the application of subsection (1)(b) and (f).

Authorisation concerning data subject's criminal behaviour or biometric information

The prohibition on processing personal information concerning a data subject's criminal behaviour or biometric information, as referred to in section 26, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law.

The processing of information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

The prohibition on processing any of the categories of personal information referred to in section 26 does not apply if such processing is necessary to supplement the processing of information on criminal behaviour or biometric information permitted by this section.

Information quality:

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

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

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

On receipt of a request in terms of subsection (1) a responsible party must, as soon as reasonably practicable—

correct the information;

destroy or delete the information;

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

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 under subsection (2) 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 in terms of subsection (1), of the action taken as a result of the request.

We will strive to update your personal information at every possible opportunity, including at each visit to our facilities, in order to achieve the best possible quality of information, in Your and Our best interests.

You are required to inform us of any changes to your personal information in order for us to achieve the necessary accuracy thereof.

Openness:

Notification to data subject when collecting personal information:

If personal information is collected, We as the responsible party must take reasonably practicable steps to ensure that the data subject is aware of—

the information being collected and where the information is not collected from the data subject, the source from which it is collected;

the name and address of the responsible party;

the purpose for which the information is being collected;

whether or not the supply of the information by that data subject is voluntary or mandatory;

the consequences of failure to provide the information;

any particular law authorising or requiring the collection of the information;

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;

any further information such as the—

recipient or category of recipients of the information;

nature or category of the information;

existence of the right of access to and the right to rectify the information collected;

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

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 steps referred to in subsection (1) must be taken—

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 in that subsection; or

in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

A responsible party that has previously taken the steps referred to in subsection (1) complies with subsection (1) in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information remains the same.

It is not necessary for a responsible party to comply with subsection (1) if—

the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;

non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;

non-compliance is necessary—

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

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, 1997 (Act No. 34 of 1997);

for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

in the interests of national security;

compliance would prejudice a lawful purpose of the collection;

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

the information will—

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

be used for historical, statistical or research purposes.

Security safeguards:

We will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information.

This will include maintaining systems and procedures and taking steps that safeguards these Security measures that are applicable to the integrity and confidentiality of personal information:

As responsible party we will secure the integrity and confidentiality of personal information in Our possession or under Our 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.

In order to give effect to this, we will take reasonable measures to—

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

establish and maintain appropriate safeguards against the risks identified;

regularly verify that the safeguards are effectively implemented; and

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

As 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;

Information processed by operator or person acting under authority:

We will take reasonable measures to ensure that:

An operator or anyone processing personal information on behalf of us as a responsible party or an operator, will—

process such information only with the knowledge or authorisation of us as the responsible party; and

treats the 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.

Security measures regarding information processed by Operator:

The security of Your Personal Data is important to Us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Data, We cannot guarantee its absolute security.

We will take reasonable measures to ensure that:

The operator which processes personal information for the Responsible party establishes and maintains the security measures referred to in section 19 in terms of a written contract with the Operator.

That the Operator must notify us as 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.

Notification of security compromises:

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, we as Responsible Party must notify—

the Regulator; and

subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

The notification will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

As Responsible party we will only delay notification to the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

The notification to a data subject will be in writing and communicated to the data subject in at least one of the following ways:

Mailed to the data subject's last known physical or postal address;

sent by e-mail to the data subject's last known e-mail address;

placed in a prominent position on our website;

published in the news media; or

as may be directed by the Regulator.

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

a description of the possible consequences of the security compromise;

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

a recommendation regarding the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

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 us as 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.

Data subject participation:

The conditions, as referred to in subsection (1), are not applicable to the processing of personal information to the extent that such processing is—

excluded, in terms of section 6 or 7, from the operation of POPIA; or

exempted in terms of section 37 or 38 thereof, from one or more of the conditions concerned in relation to such processing.

The processing of the special personal information of a data subject is prohibited in terms of section 26 of POPIA, unless the—

provisions of sections 27 to 33 are applicable; or

the Regulator has granted an authorisation in terms of section 27(2), in which case, subject to section 37 or 38, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

The processing of the personal information of a child is prohibited in terms of section 34, unless the—

provisions of section 35(1) are applicable; or

the Regulator has granted an authorisation in terms of section 35(2), in which case, subject to section 37, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

The processing of the special personal information of a child is prohibited in terms of sections 26 and 34 unless the provisions of sections 27 and 35 are applicable in which case, subject to section 37, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

The conditions for the lawful processing of personal information by or for a responsible party for the purpose of direct marketing by any means are reflected in Chapter 3, read with section 69 insofar as that section relates to direct marketing by means of unsolicited electronic communications.

Sections 60 to 68 provide for the development, in appropriate circumstances, of codes of conduct for purposes of clarifying how the conditions referred to in subsection (1), subject to any exemptions which may have been granted in terms of section 37, are to be applied, or are to be complied with within a particular sector. We will comply with such codes when they become effective.

The prohibition on processing personal information, as referred to in section 26, does not apply if the—

processing is carried out with the consent of a data subject referred to in section 26 of POPIA;

processing is necessary for the establishment, exercise or defense of a right or obligation in law;

processing is necessary to comply with an obligation of international public law;

processing is for historical, statistical or research purposes to the extent that—

the purpose serves a public interest and the processing is necessary for the purpose concerned; or

it appears to be impossible or would involve a disproportionate effort to ask for consent,

and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;

information has deliberately been made public by the data subject; or

provisions of sections 28 to 33 are, as the case may be, complied with.

The Regulator may, subject to subsection (3), upon application by a responsible party and by notice in the Gazette, authorise a responsible party to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject.

The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2).

<u>Rights of Data Subjects:</u>

You as data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3 of POPIA, including the right—

to be notified that—

personal information about him, her or it is being collected as provided for in terms of section 18; or

his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;

to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of section 23;

to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24;

to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)(a);

to object to the processing of his, her or its personal information—

at any time for purposes of direct marketing in terms of section 11(3)(b); or

in terms of section 69(3)(c);

not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1);

not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71;

to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74; and

to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99.

Rights of Data Subjects Regarding Direct Marketing by Means of Unsolicited Electronic Communications, Directories and Automated Decision Making:

Direct marketing by means of unsolicited electronic communications:

The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject—

has given his, her or its consent to the processing; or

is, subject to subsection (3), a customer of the responsible party.

A responsible party may approach a data subject—

whose consent is required in terms of subsection (1)(a); and

who has not previously withheld such consent,

only once in order to request the consent of that data subject.

The data subject's consent must be requested in the prescribed manner and form.

A responsible party may only process the personal information of a data subject who is a customer of the responsible party in terms of subsection (1)(b)—

if the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;

for the purpose of direct marketing of the responsible party's own similar products or services; and

if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details—

at the time when the information was collected; and

on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

Any communication for the purpose of direct marketing must contain—

details of the identity of the sender or the person on whose behalf the communication has been sent; and

an address or other contact details to which the recipient may send a request that such communications cease.

‘‘Automatic calling machine’’, for purposes of subsection (1), means a machine that is able to do automated calls without human intervention.

Directories

A data subject who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his, her or its personal information is included, must be informed, free of charge and before the information is included in the directory—

about the purpose of the directory; and

about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.

A data subject must be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use.

Subsections (1) and (2) do not apply to editions of directories that were produced in printed or off-line electronic form prior to the commencement of this section.

If the personal information of data subjects who are subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the conditions for the lawful processing of personal information prior to the commencement of this section, the personal information of such subscribers may remain included in this public directory in its printed or electronic versions, after having received the information required by subsection (1).

‘‘Subscriber’’, for purposes of this section, means any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services.

<u>Automated decision making:</u>

Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

The provisions of subsection (1) do not apply if the decision—

has been taken in connection with the conclusion or execution of a contract, and—

the request of the data subject in terms of the contract has been met; or

appropriate measures have been taken to protect the data subject's legitimate interests; or

is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

The appropriate measures, referred to in subsection (2)(a)(ii), must—

provide an opportunity for a data subject to make representations about a decision referred to in subsection (1); and

require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of paragraph (a).

Transfers of personal information outside Republic:

A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless—

the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that—

effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

the data subject consents to the transfer;

the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

the transfer is for the benefit of the data subject, and—

it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

For the purpose of this section—

''binding corporate rules'' means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and

''group of undertakings'' means a controlling undertaking and its controlled undertakings.

Interference with protection of personal information of data subject

For the purposes of this Chapter, interference with the protection of the personal information of a data subject consists, in relation to that data subject, of—

any breach of the conditions for the lawful processing of personal information as referred to in Chapter 3;

non-compliance with section 22, 54, 69, 70, 71 or 72; or

a breach of the provisions of a code of conduct issued in terms of section 60.

Use of Your Personal Data

We may use Personal Data for the following purposes:

To advance your health and the health of our other patients and the community.

To provide and maintain our Service, including to monitor the usage of our Service.

To manage Your Account: to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.

For the performance of a contract: the development, compliance and undertaking of the purchase contract for the products, items or services You have purchased or of any other contract with Us through the Service.

To contact You:

To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.

To provide You with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless You have opted not to receive such information.

To manage Your requests: To attend and manage Your requests to Us.

For business transfers: We may use Your information to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.

For other purposes: We may use Your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Service, products, services, marketing and your experience.

We may share Your personal information in the following situations:

With Your medical aid;

For purposes of Clinical research and trails as provided for in the relevant legislation;

With the Regulatory authorities in terms of their statutory mandates;

In accordance with our duties in terms of the Legislation relating to the notification of communicable diseases that inter alia provides as follows:

National Health Act, 2003 (Act No. 61 of 2003)

Regulations

Regulations relating to the Surveillance and the Control of Notifiable Medical Conditions, 2017

Chapter 1 : Implementation Principles and Responsibilities in relation to Notifiable Medical Conditions

8. Responsibilities of health care providers

(1) A health care provider must—

(a) notify the focal person at the health sub-district level of any diagnosed case of a notifiable medical condition through the use of—

(i) standard case definitions for notifiable medical conditions according to the WHO international Classification of Diseases as adapted by the national department;

(ii) national department forms and tools for reporting notifiable medical conditions;

(iii) notification procedures stipulated in these Regulations;

(b) ensure adherence to these Regulations;

(c) adhere to national department guidelines on the surveillance and control of notifiable medical conditions.

Regulations relating to the Surveillance and the Control of Notifiable Medical Conditions, 2017

Chapter 4 : General Matters

18. Confidentiality

(1) Information concerning a case, contact or a carrier of a notifiable medical condition, including information relating to his or her health status, treatment or stay in a health establishment, is confidential.

(2) No person may disclose information contemplated in subregulation 18(1) unless—

(a) the disclosure is for the purposes of public health surveillance, investigations and interventions; or

(b) a court order or any law requires that disclosure.

National Health Act, 2003 (Act No. 61 of 2003)

Regulations

Regulations relating to the Surveillance and the Control of Notifiable Medical Conditions, 2017

Chapter 4 : General Matters

19. Protection of health records

The health records of a case, contact or carrier of a notifiable medical condition must be protected as provided for in section 17(1) of the Act.

National Health Act, 2003 (Act No. 61 of 2003)

Chapter 2 : Rights and Duties of Users and Health Care Personnel

17. Protection of health records

(1) The person in charge of a health establishment in possession of a user's health records must set up control measures to prevent unauthorized access to those records and to the storage facility in which, or system by which, records are kept.

(2) Any person who—

(a) Fails to perform a duty imposed on them in terms of subsection (1);

(b) falsifies any record by adding to or deleting or changing any information contained in that record;

(c) creates, changes or destroys a record without authority to do so;

(d) fails to create or change a record when properly required to do so;

(e) provides false information with the intent that it be included in a record;

(f) without authority, copies any part of a record;

(g) without authority, connects the personal identification elements of a user's record with any element of that record that concerns the user's condition, treatment or history;

(h) gains unauthorised access to a record or record-keeping system, including intercepting information being transmitted from one person, or one part of a record-keeping system, to another;

(i) without authority, connects any part of a computer or other electronic system on which records are kept to—

(i) any other computer or other electronic system; or

(ii) any terminal or other installation connected to or forming part of any other computer or other electronic system; or

(j) without authority, modifies or impairs the operation of—

(i) any part of the operating system of a computer or other electronic system on which a user's records are kept; or

(ii) any part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a user's records are kept,

commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding one year or to both a fine and such imprisonment.

With Service Providers: We may share Your personal information with Service Providers to monitor and analyze the use of our Service, to contact You. Their services will be subject to a written agreement with us to uphold your privacy to none less of a degree than what we are required to do in terms of this Policy and the relevant Legislation.

For business transfers: We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of Our business to another company.

With Associated Companies: We may share Your information with Our Associated Companies, in which case we will require those Associated Companies to honour this Privacy Policy. Associated Companies include Our parent company and any other subsidiaries, joint venture partners or other companies that We control or that are under common control with Us.

With business partners: We may share Your information with Our business partners to offer You certain products, services or promotions with your consent.

With other users: when You share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside. If You interact with other users or register through a Third-Party Social Media Service, Your contacts on the Third-Party Social Media Service may see Your name, profile, pictures and description of Your activity. Similarly, other users will be able to view descriptions of Your activity, communicate with You and view Your profile.

With Your consent: We may disclose Your personal information for any other purpose with Your consent unless We are prohibited to do so in terms of legislation or an order of court.

To protect our legitimate legal interests. This may include the limited disclosure of your personal information in cases where the data subject spreads or publishes false information of Us, in order to protect our good name and reputation. In this regard the Data Subject acknowledges that the spread of false information can be extremely harmful to a business and that irreparable harm could be suffered if left immediately unanswered, that will impact on our ability to provide healthcare to our communities in terms of their Constitutional Right to Healthcare.

We will respect the provision of Section 7 of the Choice on Termination of Pregnancy Act, 1996 (Act No. 92 of 1996)

Notification and keeping of records

(1) Any medical practitioner, or a registered midwife or registered nurse who has completed the prescribed training course, who terminates a pregnancy in terms of section 2(1)(a) or (b), shall record the prescribed information in the prescribed manner and give notice thereof to the person referred to in subsection (2).

(2) The person in charge of a facility referred to in section 3 or a person designated for such purpose, shall be notified as prescribed of every termination of a pregnancy carried out in that facility.

(3) The person in charge of a facility referred to in section 3, shall, within one month of the termination of a pregnancy at such facility, collate the prescribed information and forward it by registered post confidentially to the relevant Head of Department: Provided that the name and address of a woman who has requested or obtained a termination of pregnancy, shall not be included in the prescribed information.

[Words preceding the proviso to subsection (3) substituted by section 3(a) of Act No. 1 of 2008]

(4) The Head of Department shall—

(a) keep record of the prescribed information which he or she receives in terms of subsection

(3); and

(b) submit to the Director-General the information contemplated in paragraph (a) every six months.

[Subsection (4) substituted by section 3(b) of Act No. 1 of 2008]

(5) The identity of a woman who has requested or obtained a termination of pregnancy shall remain confidential at all times unless she herself chooses to disclose that information.

Retention of Your Personal Data

We will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy and in relevant legislation and as is required in view of court judgments on the subject. In this regard specific reference is made to the retention of medical records for purposes of possible litigation. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

We will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

Transfer of Your Personal Data

Your information, including Personal Data, is processed at Our operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to — and maintained on — computers located outside of Your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from Your jurisdiction.

Your consent to this Privacy Policy followed by Your submission of such information represents Your agreement to that transfer.

Disclosure of Your Personal Data

Business Transactions

If We are involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

Law enforcement

Under certain circumstances, We may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Other legal requirements

We may disclose Your Personal Data in the good faith belief that such action is necessary to:

Comply with a legal obligation

Protect and defend Our rights or property

Prevent or investigate possible wrongdoing in connection with the Service

Protect the personal safety of Users of the Service or the public

Protect against legal liability

When disclosure is required by the regulatory authorities including the Health Professional's Council of South Africa, the Nursing Council of South Africa and the Office of Health Care Standards of South Africa, under their statutory mandates.

Children's Privacy

As a general rule we will not process the personal information of children, safe for when:

It forms an integral part of our operations as a health care provider, for instance when the child is Our patient and medical records are generated and processed in this regard, as we are obliged to do in terms of the relevant legislation;

It is carried out with the prior consent of a competent person

Necessary for the establishment, exercise or defence of a right or obligation in law

Necessary to comply with a legal obligation

For historical, statistical or research purposes to the extent that - the purpose serves a public interest and the processing is necessary for the purpose concerned; or

it appears to be impossible or would involve a disproportionate effort to ask for consent,

and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or

of personal information which has deliberately been made public by the child with the consent of a competent person.

We will be mindful of the provisions of Section 13 of the Children's Act that states that::

Every child has the right to—

a) have access to information on health promotion and the prevention and treatment of ill-health and disease, sexuality and reproduction;

b) have access to information regarding his or her health status;

c) have access to information regarding the causes and treatment of his or her health status;

and

d) confidentiality regarding his or her health status and the health status of a parent, care-giver or family member, except when maintaining such confidentiality is not in the best interests of the child.

2) Information provided to children in terms of this subsection must be relevant and must be in a format accessible to children, giving due consideration to the needs of disabled children.

We will also be mindful of the provisions of Section 28 of the Constitution, Act 108 of 1996, that states that:

28. Children

(1) Every child has the right—

(a) to a name and a nationality from birth;

(b) to family care or parental care, or to appropriate alternative care when removed from the family environment;

(c) to basic nutrition, shelter, basic health care services and social services;

(d) to be protected from maltreatment, neglect, abuse or degradation;

(e) to be protected from exploitative labour practices;

(f) not to be required or permitted to perform work or provide services that—

(i) are inappropriate for a person of that child's age; or

(ii) place at risk the child's well-being, education, physical or mental health or spiritual, moral or social development;

(g) not to be detained except as a measure of last resort, in which case, in addition to the rights a child enjoys under sections 12 and 35, the child may be detained only for the shortest appropriate period of time, and has the right to be—

(i) kept separately from detained persons over the age of 18 years; and

(ii) treated in a manner, and kept in conditions, that take account of the child's age;

(h) to have a legal practitioner assigned to the child by the state, and at state expense, in civil proceedings affecting the child, if substantial injustice would otherwise result; and

(i) not to be used directly in armed conflict, and to be protected in times of armed conflict.

(2) A child's best interests are of paramount importance in every matter concerning the child.

(3) In this section "child" means a person under the age of 18 years.

It should be noted that the Regulator may, notwithstanding the prohibition referred to in section 34, but subject to subsection (3), upon application by a responsible party and by notice in the Government Gazette, authorise a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child and that the Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2), including conditions with regard to how a responsible party must—

upon request of a competent person provide a reasonable means for that person to—

review the personal information processed; and

refuse to permit its further processing;

provide notice—

regarding the nature of the personal information of children that is processed;

how such information is processed; and

regarding any further processing practices;

refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and

establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

Regulator may exempt processing of personal information

The Regulator may, by notice in the Gazette, grant an exemption to a responsible party to process personal information, even if that processing is in breach of a condition for the processing of such information, or any measure that gives effect to such condition, if the Regulator is satisfied that, in the circumstances of the case—

the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or

the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.

The public interest referred to in subsection (1) includes—

the interests of national security;

the prevention, detection and prosecution of offences;

important economic and financial interests of a public body;

fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c);

historical, statistical or research activity; or

the special importance of the interest in freedom of expression.

The Regulator may impose reasonable conditions in respect of any exemption granted under subsection (1).

Links to Other Websites

Our Service may contain links to other websites that are not operated by Us. If You click on a third party link, You will be directed to that third party's site. We strongly advise You to review the Privacy Policy of every site You visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Changes to this Privacy Policy

We may update Our Privacy Policy from time to time. We will notify You of any changes by posting the new Privacy Policy on this page.

We will let You know via email and/or a prominent notice on Our Service, prior to the change becoming effective and update the "Last updated" date at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Access to Personal Information:

A data subject, having provided adequate proof of identity, has the right to—

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

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

within a reasonable time;

at a prescribed fee, if any;

in a reasonable manner and format; and

in a form that is generally understandable.

If, in response to a request in terms of subsection (1), 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 in terms of subsection (1)(b) to enable the responsible party to respond to a request, the responsible party—

must give the applicant 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.

The provisions of sections 30 and 61 of the Promotion of Access to Information Act ("PAIA") are applicable in respect of access to health or other records.

Kindly refer to the relevant section on Our website with further details on the process to be followed to access Information as provided for in PAIA.

If a request for access to personal information is made to a responsible party and part of that information may or must be refused in terms of subsection (4)(a), every other part must be disclosed.

Processing subject to prior authorisation

The responsible party must obtain prior authorisation from the Regulator, in terms of section 58, prior to any processing if that responsible party plans to—

process any unique identifiers of data subjects—

for a purpose other than the one for which the identifier was specifically intended at collection; and

with the aim of linking the information together with information processed by other responsible parties;

process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

process information for the purposes of credit reporting; or

transfer special personal information, as referred to in section 26, or the personal information of children as referred to in section 34, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72.

The provisions of subsection (1) may be applied by the Regulator to other types of information processing by law or regulation if such processing carries a particular risk for the legitimate interests of the data subject.

This section and section 58 are not applicable if a code of conduct has been issued and has come into force in terms of Chapter 7 in a specific sector or sectors of society.

A responsible party must obtain prior authorisation as referred to in subsection (1) only once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised in accordance with the provisions of subsection (1).

Responsible party to notify Regulator if processing is subject to prior authorization:

Information processing as contemplated in section 57(1) must be notified as such by the responsible party to the Regulator.

Responsible parties may not carry out information processing that has been notified to the Regulator in terms of subsection (1) until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

In the case of the notification of information processing to which section 57(1) is applicable, the Regulator must inform the responsible party in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation.

In the event that the Regulator decides to conduct a more detailed investigation, it must indicate the period within which it plans to conduct this investigation, which period must not exceed 13 weeks.

On conclusion of the more detailed investigation referred to in subsection (4) the Regulator must issue a statement concerning the lawfulness of the information processing.

A statement by the Regulator in terms of subsection (5), to the extent that the information processing is not lawful, is deemed to be an enforcement notice served in terms of section 95 of this Act.

A responsible party that has suspended its processing as required by subsection (2), and which has not received the Regulator's decision within the time limits specified in subsections (3) and (4), may presume a decision in its favour and continue with its processing.

Our Information Officer:

Company Secretary

Email: cosec@clinix.co.za

Duties and responsibilities of Information Officer

Our Information Officer's is responsible for the following:

The encouragement of compliance, us, with the conditions for the lawful processing of personal information;

dealing with requests made to Us pursuant to this Act;

working with the Regulator in relation to investigations conducted pursuant to Chapter 6 relating to Us;

otherwise ensuring compliance by Us with the provisions of POPIA; and

as may be prescribed by the Regulator or in terms of Legislation.

We will register the Information Officer with the Information Regulator by 1 July 2021. This is not currently possible. The information regulator plans to develop an electronic portal by 31 March 2021 to enable an organisation to register their information officer and people to access to the register of Information Officers (section 55(2)). The CEO and Executive: PAIA is responsible for developing the portal internally with the assistance of the DOJ & CD's Information Systems Management Branch.

Complaints

Complaints maybe submitted to Our Information Officer and a person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject.

A responsible party or data subject may, in terms of section 63(3), submit a complaint to the Regulator in the prescribed manner and form if he, she or it is aggrieved by the determination of an adjudicator.

Civil action recourse and Exclusion of Liability

You, as Data Subject, may under certain circumstances be entitled to institute a civil action against us for a breach of our statutory duties, during which case we will be entitled to *inter alia* and in addition towhatsoever other defences we may have, raise the following defenses as expressly provided for in Section 99(2) of POPIA:

vis major;

consent of the plaintiff;

fault on the part of the plaintiff;

that compliance was not reasonably practicable in the circumstances of the particular case; or

the Regulator has granted an exemption in terms of section 37.

General terms:

Contra Proferentem. In the interpretation of this agreement no rules of construction shall apply to the disadvantage of one party on the basis that that party put forward or drafted this agreement or any part thereof.

Jurisdiction:

The South African Courts will have sole jurisdiction to entertain any matter to be decided in relation to the subject matter of this Policy

Notices

Notices to the other party will be delivered by hand and send by email to the relevant addresses, in order to be effective.

Domicilium

We choose as Our domicilium ciandi et executandi the following addresses:

The Company Secretary and Information Officer

Clinix Health Management (Pty) Ltd

47 St Patrick's Road

Houghton

Johannesburg

And

Email to cosec@clinix.co.za

We may regard your last known physical address and / or email address as your chosen domicilium address unless you notified Us of the change of those details

Mode of complaints to Regulator

A complaint to the Regulator must be made in writing.

The Regulator must give such reasonable assistance as is necessary in the circumstances to enable a person, who wishes to make a complaint to the Regulator, to put the complaint in writing.

Contact Us

If you have any questions about this Privacy Policy or any related matter, You can contact us:

By email: cosec@clinix.co.za

Amendments to this policy:

This policy will be reviewed from time to time and any revision will be published on our website and will be effective immediately.