POPIA MANUAL

This manual was prepared in accordance with section 51 of the Protection of Personal Information Act of 2013.

This manual applies to

Dr
Graham
N
Stapleton

1. BACKGROUND TO THE PROMOTION OF ACCESS TO INFORMATION ACT

This MANUAL on data protection explains what information Dr Graham N Stapleton collects while you are visiting the website and how this information is used.

We place great importance on the security of all personal data associated with our users. We have security measures in place to protect against the loss, misuse and alteration of personal information under our control. For example, every piece of data that you provide via our website will be encrypted using Secure Sockets Layer (SSL) technology to prevent unauthorized access to a collection of such data. Our security and privacy policies are periodically reviewed and adjusted as necessary and only authorized personnelhas access to personal information.

Parliament assented to POPIA on 19 November 2013. The commencement date of section 1, Part A of Chapter 5, section 112 and section 113 is 11 April 2014. The commencement date of the other sections is 1 July 2020 (with the exception of section 110 and 114(4). The President of South Africa has proclaimed the POPI commencement date to be 1 July 2020.

POPIA or POPI was promulgated on 26 November 2013. The Protection of Personal Information Act (POPIA) is intended to promote the right to privacy in the Constitution, while at the same time protecting the flow of information and advancing the right of access to and protection of information.

2. Dr Graham N Stapleton.

Dr Graham Stapleton is a registered surgeon who specialises in the treatment of hepato-pancreato-biliary diseases and gastrointestinal surgical oncology. This involves treating diseases of the gallbladder, bile ducts, liver, pancreas, stomach and intestines, with particular emphasis on oncological (cancer) surgery.

3. DEFINITIONS

The Protection of Personal Information Act (POPIA) involves three parties (who can be natural or juristic persons):

- **The data subject**: the person to whom the information relates.
- **The responsible party:** the person who determines why and how to process. For example, profit companies, non-profit companies, governments, state agencies and people. Called controllers in other jurisdictions
- **The operator:** a person who processes personal information on behalf of the responsible party. For example, an IT vendor. Called processors in other jurisdictions.

The Protection of Personal Information Act places various obligations on the responsible party, which is the body ultimately responsible for the lawful processing of personal information. Responsible parties

should only use operators that can meet the requirements of lawful personal information processing prescribed by the Protection of Personal Information Act.

As set out above, responsible parties determine the purpose for processing information, what information is processed, for how long and how it is processed. Where an operator is involved, the responsible party will still determine the purpose for processing etc, but will outsource the processing of the information to the operator. The responsible party therefore still makes all decisions in relation to the information andthe operator acts in accordance with these decisions and on the instructions from the responsible party.

The responsible party remains ultimately accountable for ensuring that POPIA is complied with by both itself and all operators providing services to the responsible party. The outsourcing or sub-contracting of any processing activities to operators does not absolve the responsible party from liability. If the operator contravenes POPIA, the responsible party will still be held liable by the Information Regulator.

As with many other relationships, a contractual agreement between a responsible party and operator will prove very useful and high highly recommended in order to definitively address and govern the roles of each party and the boundaries of the relationship.

An agreement between the responsible party and operator should address, at the least, the following points:

- That the operator only acts within the ambit of the agreement/mandate with the responsible party;
- The purpose for processing of the information;
- What information may be processed by the operator;
- What the operator may or may not do with the information outside of the processing mandate;
- A duty to protect the information received, not share it with third parties without consent, to keep the information received confidential and to otherwise act within the ambit of POPIA;
- Limit the operator from appointing further operators without the responsible party's knowledge or consent; and
- Liability for the operator*.

As mentioned above, the responsible party will be held ultimately liable by the Information Regulator for a breach of POPIA by the operator. The Information Regulator will impose this liability on the responsible party where the breach occurred within the scope of the mandate agreement between the responsible party and the operator and will not be diverted to the operator where the breach is as a result of the operator's failure to uphold the principles of POPIA.

Therefore, the agreement between the responsible party and the operator is extremely important for the responsible party as this agreement can result in the responsible party holding the operator liable for any claims that the Information Regulator and/or data subjects (the people whose personal information is

being processed) bring against the responsible party as a result of a breach of POPIA by the operator. A liability clause will allow the responsible party to bring a claim for any loss suffered by the responsible party as a result of the operator's negligence or breach of POPIA.

Some relief for a responsible party in this regard is where an operator breaches POPIA where the operator has exceeded its mandate. In these circumstances, the operator is seen to be acting as a responsible party in regard to the personal information as the operator is determining the purposes and means of processing.

4. PURPOSE OF THE POPIA MANUAL

POPIA establishes the rights and duties that are designed to safeguard personal data. In terms of POPIA, the legitimate needs of organisations to collect and use personal data for business and other purposes are balanced against the right of individuals to have their right of privacy, in the form of their personal details, respected.

POPIA applies to a particular activity, i.e. the processing of personal data, rather than a particular person or organisation. Therefore, if you process personal data then you must comply with POPIA and, in particular, you must handle personal data in accordance with POPIA's data protection principles.

Therefore, if you collect or hold information about an identifiable individual or if you use, disclose, retain or destroy that information, you are likely to be processing personal data. The scope of POPIA is very wide and it applies to almost everything you might do with an individual's personal details including details of your employees.

5. CONTACT DETAILS OF THE MANAGING DIRECTOR

Managing Director:	Dr Graham N Stapleton
Registered Address:	1406 Netcare Christian Barnard Memorial Hospital Cnr DF Malan Street & Rua Bartholemeu Dias Plain Foreshore Cape Town 8001 SOUTH AFRICA
Postal Address:	1406 Netcare Christian Barnard Memorial Hospital Cnr DF Malan Street & Rua Bartholemeu Dias Plain Foreshore Cape Town 8001 SOUTH AFRICA
Telephone Number:	+27 21 671 6181
Website:	https://www.hpbsurgery.co.za/

6. THE INFORMATION OFFICER

POPI designates the head of the business as the Information Officer. Depending on the type of business, the Information Officer will therefore be the sole trader, a partner in a partnership or CEO (or equivalent) in a company or CC.

The head of the business can delegate his or her responsibilities as Information Officer to any other duly authorised person. However, it is important to note that whoever "determines the purpose of and means for processing personal information" remains ultimately responsible for ensuring that the processing of personal information is done in a lawful manner and "retains the accountability and responsibility for any power or the functions authorised to that person"

The Guidance Note specifies that "Each subsidiary of a group of companies must register its Information Officer".

The Information Officer must appoint as many Deputy Information Officers as necessary. For example, the appointment of Deputy Information Officers may become necessary to make the organisations records as accessible as reasonably possible for requesters. This must be done in writing, specifically using Template "B" in the Guidance Note which also stipulates that the DIO "should report to the highest management office within a Body" and therefore must be an employee.

7. DUTIES AND RESPONSIBILITIES

Duties and responsibilities of the Information Officer? The specific duties are spelled out for us in the Guidance Note.

The Act stipulates the following general responsibilities:

1. to encourage compliance with POPI;
2. dealing with requests made to the organisation in relation to POPI (for instance, requests from Data Subjects to update or view their personal information);
3. working with the Regulator in relation to investigations;
4. otherwise ensuring compliance with POPI;
5. as may be prescribed (i.e. keep an eye on the Regulator's website!).

Information Officers need to be registered with the Regulator before taking up their duties.

Regulation 4 lists the following prescribed responsibilities in addition to those listed above:

- **Compliance framework:**
    - Develop and implement a compliance framework;
    - ensure it is monitored and maintained over time;

- (this could be captured in a privacy charter or framework document that outlines who is responsible for what and which policies apply).

- **Personal information impact assessment ("PIIA")**
  - conduct a PIIA to ensure that adequate measures and standards exist in order to comply the conditions for the lawful processing of personal information (as defined in Chapter 3of POPIA);

- **POPIA Manual**: ensure that your organisation has a POPIA manual;
  - ensure it is monitored, maintained and made available as prescribed by PAIA;
  - provide copies of the manual to anyone who asks for it (the Regulator may determine in future that a fee must be paid for this).

- Enable **Data Subject Participation**
  - develop measures and adequate systems to process requests for information or access to information;

- **Awareness Training**: conduct internal awareness sessions regarding:
  - the provisions of the POPI Act;
  - the regulations made in terms of the Act;
  - codes of conduct, or
  - information obtained from the Regulator;
  - (this will need to be ongoing as the Regulator provides updates, guidelines, new regulations, or as new codes of conduct become enforceable).

On a day to day basis the Information Officer may find themselves:

- making recommendations and raising concerns where appropriate;
- documenting information processing procedures;
- evaluating and further developing data protection and security policies;
- suggesting, selecting and implementing technical security measures;
- drafting forms and contracts appropriate for data protection;
- selecting employees, service providers and others to be involved in the processing of personal information;

- monitoring data privacy and security measures as well as the proper use of data processing programs;
- handling complaints relating to personal information;
- employee training; and
- preparing, submitting and maintaining notifications to [the Regulator].

8. CONTACT DETAILS OF THE INFORMATION OFFICER

Information Officer:
Zasskia van der Merwe

Physical Address: 1406 CHRISTIAAN BARNARD MEMORIAL HOSPITAL, DF MALAN STREET, FORESHORE, 8001

Telephone Number: +27 21 671 6181

Email: office@hpbsurgery.co.za

9, WHAT INFORMATION DO WE COLLECT?

Collection of Personal Information

We collect and process your Personal Information mainly to provide you with access to our services and products, to help us improve our offerings to you, to support our contractual relationship with you and for certain other purposes explained below. The type of information we collect will depend on the purpose for which it is collected and used. We will only collect information that we need for that purpose.

We collect information directly from you where you provide us with your personal details, for example when you purchase or supply a product or services to or from us or when you submit enquiries to us or contact us. Where possible, we will inform you what information you are required to provide to us and what information is optional.

Examples of information we collect from you are:

- name
- address
- email address
- telephone/cell number
- user-generated content, posts and other content you submit to our web site

We collect and process your Personal Information mainly to provide you with access to our services and products, to help us improve our offerings to you, to support our contractual relationship with you and for certain other purposes explained below. The type of information we collect will depend on the purpose for which it is collected and used. We will only collect information that we need for that purpose.

Collection of Non-Personal Information

We may automatically collect non-Personal Information about you such as the type of internet browsers you use or the website from which you linked to our website. We may also aggregate details which you have submitted to the site (for example, the products or services you are interested in). You cannot be identified from this information and it is only used to assist us in providing an effective service on this web site. We may from time to time supply third parties with this non-personal or aggregated data for uses in connection with this website.

Cookies policy

The Internet pages of Dr Graham N Stapleton use cookies. Cookies are text files that are stored in a computer system via an Internet browser. Many Internet sites and servers use cookies. Many cookies contain a so-called cookie ID. A cookie ID is a unique identifier of the cookie. It consists of a character string through which Internet pages and servers can be assigned to the specific Internet browser in which the cookie was stored. This allows visited Internet sites and servers to differentiate the individual browser of the data subject from other Internet browsers that contain other cookies. A specific Internet browser can be recognized and identified using the unique cookie ID.

Through the use of cookies, we can provide the users of this website with more user-friendly services that would not be possible without the cookie setting. By means of a cookie, the information and offers on our website can be optimized with the user in mind. Cookies allow us, as previously mentioned, to recognize our website users. The purpose of this recognition is to make it easier for users to utilize our website. The website user that uses cookies, e.g. does not have to enter access data each time the website is accessed, because this is taken over by the website, and the cookie is thus stored on the user's computer system. Another example is the cookie of a shopping cart in an online shop. The online store remembers the articles that a customer has placed in the virtual shopping cart via a cookie.

The data subject may, at any time, prevent the setting of cookies through our website by means of a corresponding setting of the Internet browser used, and may thus permanently deny the setting of cookies. Furthermore, already set cookies may be deleted at any time via an Internet browser or other software programs. This is possible in all popular Internet browsers. If the data subject deactivates the setting of cookies in the Internet browser used, not all functions of our website may be entirely usable.

Registration on our website

The data subject has the possibility to register on the website of the Responsible Party with the indication of personal data. Which personal data are transmitted to the Responsible Party is determined by the respective input mask used for the registration. The personal data entered by the data subject are collected and stored exclusively for internal use by the Responsible Party, and for his own purposes. The Responsible Party may request transfer to one or more operators (e.g. a parcel service) that also uses

personal data for an internal purpose which is attributable to the Responsible Party.

By registering on the website of the Responsible Party, the IP address - assigned by the Internet service provider (ISP) and used by the data subject - date, and time of the registration are also stored. The storage of this data takes place against the background that this is the only way to prevent the misuse of our services, and, if necessary, to make it possible to investigate committed offenses. Insofar, the storage of this data is necessary to secure the Responsible Party. This data is not passed on to third parties unless there is a statutory obligation to pass on the data, or if the transfer serves the aim of criminal prosecution.

The registration of the data subject, with the voluntary indication of implied consent that the personal data, is intended to enable the Responsible Party to offer the data subject contents or services that may only be offered to registered users due to the nature of the matter in question. Registered persons are free to change or withdraw their consent specified during the registration at any time, or to have them completely deleted from the data stock of the Responsible Party.

The data Responsible Party shall, at any time, provide information upon request to each data subject as to what personal data are stored about the data subject. In addition, the data Responsible Party shall correct or erase personal data at the request or indication of the data subject, insofar as there are no statutory storage obligations to keep the data. The entirety of the Responsible Party's employees is available to the data subject in this respect as contact persons.

9. HOW WE USE YOUR INFORMATION

- We will use your Personal and Non-Personal Information only for the purposes for which it was collected or agreed with you, for example:
    - Analyse the effectiveness of our advertisements, competitions and promotions;
    - Collect information about the device you are using to view the site, such as your IP address or the type of Internet browser or operating system you are using, and link this to your Personal Information so as to ensure that the site presents the best web experience for you;
    - Evaluate the use of the site, products and services;
    - For audit and record keeping purposes;
    - For market research purposes;
    - For monitoring and auditing site usage;
    - Help speed up your future activities and experience on the site. For example, a site can recognise that you have provided your Personal Information and will not request the same information a second time;
    - In connection with legal proceedings;
    - Make the site easier to use and to better tailor the site and our products to your interests and needs;
    - Offer you the opportunity to take part in competitions or promotions;
    - Personalise your website experience, as well as to evaluate (anonymously and in the aggregate) statistics on website activity, such as what time you visited it,
    - whether you've visited it before and what site referred you to it;

- Suggest products or services (including those of relevant third parties) which we think may be of interest to you;
- To assist with business development;
- To carry out our obligations arising from any contracts entered into between you and us
- To conduct market or customer satisfaction research or for statistical analysis;
- To confirm and verify your identity or to verify that you are an authorised customer for security purposes;
- To contact you regarding products and services which may be of interest to you, provided you have given us consent to do so or you have previously requested a product or service from us and the communication is relevant or related to that prior request and made within any timeframes established by applicable laws;
- To notify you about changes to our service;
- To respond to your queries or comments.

We will also use your Personal Information to comply with legal and regulatory requirements or industry codes to which we subscribe or which apply to us, or when it is otherwise allowed by law;

- Where we collect Personal Information for a specific purpose, we will not keep it for longer than is necessary to fulfil that purpose, unless we have to keep it for legitimate business or legal reasons. In order to protect information from accidental or malicious destruction, when we delete information from our services we may not immediately delete residual copies from our servers or remove information from our backup systems;
- You can opt out of receiving communications from us at any time. Any direct marketing communications that we send to you will provide you with the information and means necessary to opt out.

10. SUBSCRIPTION TO OUR NEWSLETTERS

On the website of our practice, users are given the opportunity to subscribe to our enterprise's newsletter. The input mask used for this purpose determines what personal data are transmitted, as well as when the newsletter is ordered from the Responsible Party.
the practice informs its customers and business partners regularly by means of a newsletter about enterprise developments and offers. The enterprise's newsletter may only be received by the data subject if (1) the data subject has a valid e-mail address and (2) the data subject registers for the newsletter shipping.

A confirmation e-mail will be sent to the e-mail address registered by a data subject for the first time for newsletter shipping, for legal reasons, in the double **opt-in procedure**. This confirmation e-mail is used to prove whether the owner of the e-mail address as the data subject is authorized to receive the newsletter.

During the registration for the newsletter, we also store the IP address of the computer system assigned by the Internet service provider (ISP) and used by the data subject at the time of the registration, as well

as the date and time of the registration. The collection of this data is necessary in order to understand the (possible) misuse of the e-mail address of a data subject at a later date, and it therefore serves the aim of the legal protection of the Responsible Party.

The personal data collected as part of a registration for the newsletter will only be used to send our newsletter. In addition, subscribers to the newsletter may be informed by e-mail, as long as this isnecessary for the operation of the newsletter service or a registration in question, as this could be the casein the event of modifications to the newsletter offer, or in the event of a change in technical circumstances. **There will be no transfer of personal data collected by the newsletter service to third parties.** The subscription to our newsletter may be **terminated by the data subject at any time**. The consent to the storage of personal data, which the data subject has given for shipping the newsletter, may be **revoked** at any time. For the purpose of revocation of consent, a corresponding link is found in each newsletter. It is also possible to unsubscribe from the newsletter at any time directly on the website ofthe Responsible Party, or to communicate this to the Responsible Party in a different way.

11. DISCLOSURE OF PERSONAL INFORMATION

We may disclose your Personal Information to our business partners who are involved in the delivery of products or services to you. We have agreements in place to ensure that they comply with these privacy terms.

You consent to us disclosing your personal information obtained from you with:

- third parties for the purposes listed above;
- other companies in our industry when we believe it will enhance the services and products we can offer to you, but only where you have not objected to such sharing;
- other third parties from whom you have chosen to receive marketing information.
- where we have a duty or a right to disclose in terms of law or industry codes;
- where we believe it is necessary to protect our rights;
- we are legally obliged to provide adequate protection for the personal information we hold and to stop unauthorised access and use of personal information. we will, on an on-going basis, continue to review our security controls and related processes to ensure that your personal information is secure;
- acceptable usage of personal information;
- access to personal information;
- computer and network security;
- governance and regulatory issues;
- investigating and reacting to security incidents;
- monitoring access and usage of personal information;
- physical security;
- retention and disposal of information;
- secure communications;
- security in contracting out activities or functions;

When we contract third parties, we impose appropriate security, privacy and confidentiality obligations on them to ensure that Personal Information that we remain responsible for, is kept secure.
We will ensure that anyone to whom we pass your Personal Information agrees to treat your information with the same level of protection as we are obliged to.

ACCESS TO YOUR PERSONAL INFORMATION

You have the right to request a copy of the Personal Information we hold about you. To do this, simply contact us at the numbers/addresses listed on our home page and specify what information you would like. We will take all reasonable steps to confirm your identity before providing details of your personal information.

Please note that any such access request may be subject to a payment of a legally allowable fee, as laid down in our PAIA Policy.

CORRECTION OF YOUR PERSONAL INFORMATION

You have the right to ask us to update, correct or delete your personal information. We will take all reasonable steps to confirm your identity before making changes to Personal Information we may hold about you. We would appreciate it if you would take the necessary steps to keep your Personal Information accurate and up-to-date by notifying us of any changes we need to be aware of.

RETENTION OF PERSONAL DATA

We will retain your data in compliance with the POPIA and in compliance with other applicable legislation.

Routine Erasure And Blocking Of Personal Data

The data Responsible Party shall process and store the personal data of the data subject only for the period necessary to achieve the purpose of storage, or as far as this is granted by the POPIA or other legislators in laws or regulations to which the Responsible Party is subject to.
If the storage purpose is not applicable, or if a storage period prescribed by the POPIA or anothercompetent legislator expires, the personal data will be destroyed.

RGHTS OF THE DATA SUBJECT

A) RIGHT OF CONFIRMATION

Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party the confirmation as to whether or not personal data concerning him or her are being processed. If a data subject wishes to avail himself of this right of confirmation, he or she may, at any time, contact our employee of the Responsible Party.

B) RIGHT OF ACCESS

Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party free of charge information about his or her personal data stored at any time and a copy of this information. Furthermore, the PAIA grants the data subject access to the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the Responsible Party rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;
- the existence of the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and

(4) of the PAIA and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether personal data are transferred to a third country or to an international organization. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

If a data subject wishes to avail himself of this right of access, he or she may at any time contact our employee of the Responsible Party.

C) RIGHT TO RECTIFICATION

Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact our Information Officer or another employee of the Responsible Party.

D) RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party the erasure of personal data concerning him or her without undue delay, and the Responsible Party shall have the obligation to erase personal data without undue delay where one of the following grounds applies, as long as the processing is not necessary:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent to which the processing is based according to point POPIA and where there is no other legal ground for the processing.

- The data subject objects to the processing pursuant to POPIA and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to POPIA.
- The personal data have been unlawfully processed.
- The personal data must be erased for compliance with a legal obligation in South Africa which the Responsible Party is subject.
- If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by Dr Graham N Stapleton, he or she may at any time contact an employee of Dr Graham N Stapleton of the Responsible Party. An employee of Dr Graham N Stapleton shall promptly ensure that the erasure request is complied with immediately. Where the Responsible Party has made personal data public and is obliged pursuant to POPIA to erase the personal data, the Responsible Party, taking account of available technology and thecost of implementation, shall take reasonable steps, including technical measures, to inform other Responsible Party's processing the personal data that the data subject has requested erasure by such Responsible Party's of any links to, or copy or replication of, those personal data, as far as processing is not required. An employee of the practice will arrange the necessary measures in individual cases.

E) RIGHT OF RESTRICTION OF PROCESSING

Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the data subject, for a period enabling the Responsible Party to verify the accuracy of the personal data.
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests instead the restriction of their use instead.
- The Responsible Party no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.
- The data subject has objected to processing pursuant to POPIA pending the verification whether the legitimate grounds of the Responsible Party override those of the data subject.

If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by the practice, he or she may at any time contact an employee of the practice of the Responsible Party. An employee of the practice will arrange the restriction of the processing.

G) RIGHT TO OBJECT

Each data subject shall have the right granted by the South African Regulator to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her, which is based on POPIA. This also applies to profiling based on these provisions

- the practice shall no longer process the personal data in the event of the objection unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or for the establishment, exercise or defense of legal claims.

- If the practice processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing.
- This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to the practice to the processing for direct marketing purposes, the practice will no longer process the personal data for these purposes.
- In addition, the data subject has the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her by the practice for scientific or historical research purposes, or for statistical purposes pursuant POPIA, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

In order to exercise the right to object, the data subject may directly contact an employee of the practice

H) AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING

Each data subject shall have the right granted by the South African Regulator not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her, as long as the decision

(1) is not is necessary for entering into, or the performance of, a contract between the data subject and a data Responsible Party, or

(2) is not authorised by the national law to which the Responsible Party is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or

(3) is not based on the data subject's explicit consent.

If the decision

(1) is necessary for entering into, or the performance of, a contract between the data subject and a data Responsible Party, or

(2) it is based on the data subject's explicit consent, the practice shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Responsible Party, to express his or her point of viewand contest the decision.

(3) If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may at any time directly contact our Information Regulator of the practice another employee of the Responsible Party.

I. RIGHT TO WITHDRAW DATA PROTECTION CONSENT

Each data subject shall have the right granted by the South African Regulator the right to withdraw his or her consent to processing of his or her personal data at any time.

If the data subject wishes to exercise the right to withdraw the consent, he or she may at any time directly contact an employee of the Responsible Party.

LEGAL BASIS FOR THE PROCESSING

POPIA serves as the legal basis for processing operations for which we obtain consent for a specific processing purpose. If the processing of personal data is necessary for the performance of a contract to which the data subject is party, as is the case, for example, when processing operations are necessary for the supply of goods or to provide any other service, the processing is based on POPIA. The same applies to such processing operations which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. Is our company subject to a legal obligation by which processing of personal data is required, such as for the fulfilment of tax obligations, the processing is based on POPIA. In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person.

PERIOD FOR WHICH THE PERSONAL DATA WILL BE STORED

The criteria used to determine the period of storage of personal data is the respective statutory retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfilment of the contract or the initiation of a contract.
We clarify that the provision of personal data is partly required by law (e.g. tax regulations) or can also result from contractual provisions (e.g. information on the contractual partner). Sometimes it may be necessary to conclude a contract that the data subject provides us with personal data, which must subsequently be processed by us. The data subject is, for example, obliged to provideus with personal data when our company signs a contract with him or her. The non-provision ofthe personal data would have the consequence that the contract with the data subject could not be concluded. Before personal data is provided by the data subject, the data subject must contact our Data Protection Officer. An employee of the practice clarifies to the data subject whether the provision of the personal data is required by law or contract or is necessary for the conclusion of the contract, whether there is an obligation to provide the personal data and the consequences of non-provision of the personal data.

Retention schedule of respective legislation are indicated below

HARD COPIES

Documents are stored in a archive different location.

Companies Act, No 71 of 2008

With regard to the Companies Act, No 71 of 2008 and the Companies Amendment Act No 3 of 2011, hardcopies of the documents mentioned below **must be retained for 7 years**:

- Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act;
- Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities;
- Copies of reports presented at the annual general meeting of the company;
- Copies of annual financial statements required by the Act;

- Copies of accounting records as required by the Act;
- Record of directors and past directors, after the director has retired from the company;
- Written communication to holders of securities and
- Minutes and resolutions of directors' meetings, audit committee and directors' committees
- Copies of the documents mentioned below must be retained indefinitely:
- Registration certificate ;
- Memorandum of Incorporation and alterations and amendments;
- Rules;
- Securities register and uncertified securities register;
- Register of company secretary and auditors and
- Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.

Consumer Protection Act, No 68 of 2008

The Consumer Protection Act seeks to promote a fair, accessible and sustainable marketplace and therefore requires a **retention period of 3 years** for information provided to a consumer by an intermediary such as:

- Full names, physical address, postal address and contact details;
- ID number and registration number;
- Contact details of public officer in case of a juristic person;
- Service redered;
- Intermediary fee;
- Cost to be recovered from the consumer;
- Frequency of accounting to the consumer;
- Amounts, sums, values, charges, fees, remuneration specified in monetary terms;
- Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided;
- Record of advice furnished to the consumer reflecting the basis on which the advice was given;
- Written instruction sent by the intermediary to the consumer ;
- Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions;
- Documents Section 45 and Regulation 31 for Auctions.

National Credit Act, No 34 of 2005

The National Credit Act aims to promote a fair and transparent credit industry which requires the retention of certain documents for a specified period.

Retention for 3 years from the earliest of the dates of which the registrant created, signed or received the document or from the date of termination of the agreement or in the case of an application for credit that is refused or not granted for any reason, from the date of receipt of the application which applies to the documents mentioned below:

Regulation 55(1)(b):

- Records of registered activities such as an application for credit declined;
- Reason for the decline of the application for credit;

- Pre-agreement statements and quotes;
- Documentation in support of steps taken in terms of section 81(2) of the Act;
- Record of payments made;
- Documentation in support of steps taken after default by consumer.

Regulation 55(1)(c) in respect of operations:

- Record of income, expenses and cash flow;
- Credit transaction flows;
- Management accounts and financial statements.

Regulation 55(1)(d) with regard to the Credit Bureau:

- All documents relating to disputes, inclusive of but not limited to, documents from the consumer;
- Documents from the entity responsible for disputed information;
- Documents pertaining to the investigation of the dispute;
- Correspondence addressed to and received from sources of information as set out in section 70(2) of the Act and Regulation 18(7) pertaining to the issues of the disputed information.

Regulation 55(1)(a) with regard to Debt Counsellors:

- Application for debt review;
- Copies of all documents submitted by the consumer;
- Copy of rejection letter;
- Debt restructuring proposal;
- Copy of any order made by the tribunal and/or the court and a copy of the clearance certificate.

Regulation 56 with regard to section 170 of the Act:

- Application for credit;
- Credit agreement entered into with the consumer.

Regulation 17(1) with regard to Credit Bureau information:

Documents with a required retention period of the earlier of 10 years or a rehabilitation order being granted:

- Sequestrations
- Administration orders.

Documents with a required retention period of 5 years:

- Rehabilitation orders
- Payment profile.

Documents with a required **retention period of the earlier of 5 years** or until judgment is rescinded by a court or abandoned by the credit provider in terms of section 86 of theMagistrate's Court Act No 32 of 1944:

- Civil Court Judgments
- Enquiries.

Documents with a required retention period of 1.5 years:

- Details and results of disputes lodged by the consumers.

Documents with a required retention period of 1 year:

- Adverse information.

Documents with an unlimited required retention period:

- Liquidation.

Documents required to be retained until a clearance certificate is issued:

- Debt restructuring.

Financial Advisory and Intermediary Services Act, No 37 of 2002:

Section 18 of the Act requires a retention period of 5 years, except to the extent that it is exempted by the registrar for the below mentioned documents:

- Known premature cancellations of transactions or financial products of the provider by clients;
- Complaints received together with an indication whether or not any such complaint has been resolved;
- The continued compliance with this Act and the reasons for such non-compliance;
- And the continued compliance by representatives with the requirements referred to in section 13(1) and (2).

The General Code of Conduct for Authorized Financial Services Provider and Representatives requires a retention period of 5 years for the below mentioned documents:

Proper procedures to record verbal and written communications relating to a financial service rendered to a client as are contemplated in the Act, this Code or any other Code drafted in terms of section 15 of the Act;

Store and retrieve such records and any other material documentation relating to the client or financial services rendered to the client;

And keep such client records and documentation safe from destruction;

All such records must be kept for a period after termination to the knowledge of the provider of the product concerned or in any other case after the rendering of the financial service concerned.

Financial Intelligence Centre Act, No 38 of 2001:

Section 22 and 23 of the Act require a retention period of 5 years for the documents and records of the activities mentioned below:

- Whenever an accountable transaction is concluded with a client, the institution must keep record of the identity of the client;
- If the client is acting on behalf of another person, the identity of the person on whose behalf the client is acting and the clients authority to act on behalf of that other person;
- If another person is acting on behalf of the client, the identity of that person and that other person's authority to act on behalf of the client;
- The manner in which the identity of the persons referred to above was established;
- The nature of that business relationship or transaction;
- In the case of a transaction, the amount involved and the parties to that transaction;

- All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction;
- The name of the person who obtained the identity of the person transacting on behalf of the accountable institution;
- Any document or copy of a document obtained by the accountable institution. These documents may also be kept in electronic format.

Compensation for Occupational Injuries and Diseases Act, No 130 of 1993:

Section 81(1) and (2) of the Compensation for Occupational Injuries and Diseases Act requires a retention period of 4 years for the documents mentioned below:

- Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.

Section 20(2) documents with a required retention period of 3 years:

- Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation;
- Records of incidents reported at work.

Asbestos Regulations, 2001, regulation 16(1) requires a retention period of minimum 40 years for the documents mentioned below:

- Records of assessment and air monitoring, and the asbestos inventory;
- Medical surveillance records;

Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2):

- Records of risk assessments and air monitoring;
- Medical surveillance records.

Lead Regulations, 2001, Regulation 10:

- Records of assessments and air monitoring;
- Medical surveillance records.

Noise - induced Hearing Loss Regulations, 2003, Regulation 11:

- All records of assessment and noise monitoring;
- All medical surveillance records, including the baseline audiogram of every employee.

Hazardous Chemical Substance Regulations, 1995, Regulation 9 requires a retention period of 30 years for the documents mentioned below:

- Records of assessments and air monitoring;
- Medical surveillance records.

Basic Conditions of Employment Act, No 75 of 1997:

The Basic Conditions of Employment Act requires a retention period of 3 years for the documents mentioned below:

Section 29(4):
Written particulars of an employee after termination of employment;
Section 31:

- Employee's name and occupation;
- Time worked by each employee;
- Remuneration paid to each employee;
- Date of birth of any employee under the age of 18 years.

Employment Equity Act, No 55 of 1998:

Section 26 and the General Administrative Regulations, 2009, Regulation 3(2) requires a retention period of 3 years for the documents mentioned below:

Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act;

Section 21 and Regulations 4(10) and (11) require a retention period of 3 years for the report which is sent to the Director General as indicated in the Act.

Labour Relations Act, No 66 of 1995:

Sections 53(4), 98(4) and 99 require a retention period of 3 years for the documents mentioned below:

- The Bargaining Council must retain books of account, supporting vouchers, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings;
- Registered Trade Unions and registered employer's organizations must retain books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings;
- Registered Trade Unions and employer's organizations must retain the ballot papers;
- Records to be retained by the employer are the collective agreements and arbitration awards.

Sections 99, 205(3), Schedule 8 of Section 5 and Schedule 3 of Section 8(a) require an indefinite retention period for the documents mentioned below:

- Registered Trade Unions and registered employer's organizations must retain a list of its members;
- An employer must retain prescribed details of any strike, lock-out or protest action involving its employees;
- Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions;
- The Commission must retain books of accounts, records of income and expenditure, assets and liabilities.

Unemployment Insurance Act, No 63 of 2002:

The Unemployment Insurance Act, applies to all employees and employers except:

- Workers working less than 24 hours per month;
- Learners;
- Public servants;
- Foreigners working on a contract basis;
- Workers who get a monthly State (old age) pension;
- Workers who only earn commission.

Section 56(2)(c) requires a retention period of 5 years, from the date of submission, for the documents mentioned below:

Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.

Tax Administration Act, No 28 of 2011:

Section 29 of the Tax Administration Act, states that records of documents must be retained to:

- Enable a person to observe the requirements of the Act;
- Are specifically required under a Tax Act by the Commissioner by the public notice;
- Will enable SARS to be satisfied that the person has observed these requirements.

Section 29(3)(a) requires a retention period of 5 years, from the date of submission for taxpayers that have submitted a return and an indefinite retention period, until thereturn
is submitted, then a 5 year period applies for taxpayers who were meant to submit a
return, but have not Section 29(3)(b) requires a retention period of 5 years from the end of the relevant tax period for taxpayers who were not required to submit a return, but had capital gains/losses or engaged in any other activity that is subject to tax or would be subject to tax but for the application of a threshold or exemption.

Section 32(a) and (b) require a retention period of 5 years but records must be retained until the audit is concluded or the assessment or decision becomes final, for documents indicating that a person has been notified or is aware that the records are subject to an audit or investigation and the person who has lodged an objection or appeal against an assessment or decision under the TAA.

Income Tax Act, No 58 of 1962:

Schedule 4, paragraph 14(1)(a)-(d) of the Income Tax Act requires a retention period of 5 years from the date of submission for documents pertaining to each employee that the employer shall keep:

- Amount of remuneration paid or due by him to the employee;
- The amount of employees tax deducted or withheld from the remuneration paid or due;
- The income tax reference number of that employee;
- Any further prescribed information;
- Employer Reconciliation return.

Schedule 6, paragraph 14(a)-(d) requires a retention period of 5 years from the date of submission or 5 years from the end of the relevant tax year, depending on the type of transaction for documents pertaining to:

- Amounts received by that registered micro business during a year of assessment;
- Dividends declared by that registered micro business during a year of assessment;
- Each asset as at the end of a year of assessment with cost price of more than R 10 000;
- Each liability as at the end of a year of assessment that exceeded R 10 000.

Value Added Tax Act, No 89 of 1991:

- Section 15(9), 16(2) and 55(1)(a) of the Value Added Tax Act and Interpretation Note 31, 30 March requires a retention period of 5 years from the date of submission of the return for the documents mentioned below:

- Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period;
- Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS;
- Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques;
- Documentary proof substantiating the zero rating of supplies;
- Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.

ELECTRONIC STORAGE

- The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.
- Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.
- Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used.

It is also required that all personal information which has become obsolete must be destroyed.

DESTRUCTION OF DOCUMENTS

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

After completion of the process the General Manager of the department shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will beretained by Registration.

The documents are then made available for collection by the removers of the Company's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.

Documents may also be stored off-site, in storage facilities approved by the Company.

21. POLICY CHAMPION

Contact details of the administrator responsible for this policy:

Name: Dr Graham N Stapleton

Position: Managing Director

Tel: +27 21 671 6181

E-mail: office@hpbsurgery.co.za

INFORMATION OFFICER DETAILS

NAME: Zasskia van der Merwe

Tel: +27 21 671 6181

E-mail: office@hpbsurgery.co.za

DEPUTY INFORMATION OFFICER DETAILS

NAME: MELINDA STAPLETON

TELEPHONE NUMBER: +27 21 6716181

FAX NUMBER N/A

E-MAIL ADDRESS: office@hpbsurgery.co.za

HEAD OFFICE DETAILS

TELEPHONE NUMBER: +27 21 6716181

FAX NUMBER N/A

E-MAIL ADDRESS: office@hpbsurgery.co.za

PHYSICAL ADDRESS: 1406 CHRISTIAAN BARNARD MEMORIAL HOSPITAL, DF MALAN STREET, FORESHORE, 8001

POSTAL ADDRESS: 1406 CHRISTIAAN BARNARD MEMORIAL HOSPITAL, DF MALAN STREET, FORESHORE, 8001

WEBSITE: www.hpbsurgery.co,za

22. REVISION HISTORY

REVIEWERS			
NAME SURNAME SIGNATURE	DATE	POSITION	SUBJECT AND RAISED QUESTIONS

CHANGES MADE			
DATE	AUTHOR	VERSION	CHANGES MADE

SOURCES

- SAICA Guidelines-Updated October 2013 (also refers to the Banks Act and Insolvency Act);
- Companies Act, 61/1973;
- Income Tax Act, 58/1962;
- Financial Intelligence Centre Act, 38/2001;
- ECTA, 25/2002;
- RICA, 70/2002;

- Second Hand Goods Act, 23/1955;
- Firearms Control Act, 60/2000;
- Basic Conditions of Employment Act, 75/1997;
- Unemployment Insurance Act, 63/2001;
- Unemployment Insurance Contributions Act, 4/2002;
- National Credit Act, 34/2005;
- Compensation for Occupational Injuries & Diseases Act, 130/1993;
- Skills Development Levies Act, 9/1999;
- Employment Equity Act, 55/1998;
- Labour Relations Act, 66/1995;
- Securities Services Act, 36/2004;
- Value-Added Tax Act, 89/1991;
- POPI, 4/2013;
- PRECCA, 12/2004;
- PROCDATRA, 33/2004;
- FAIS, 37/2002;
- Prescription Act, 68/1969;
- Safex Rules;
- Legal advice (Juta);
- Companies Amendment Act 3/2011;
- Companies Regulations 2011;
- Tax Administration Act, 28/2011.