health
Department:
Health
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

Ground Floor, Health Office Park
Private Bag X 2068
MMABATHO
2735

INFORMATION AND RECORDS MANAGEMENT

Tel: (018) 391 4138
Email: DMakhubu@nwpg.gov.za
www.health.nwpg.gov.za

A long and healthy life for all communities of the North West Province

COMPLIANCE FRAMEWORK FOR PROTECTION OF PERSONAL INFORMATION IN THE NORTH WEST DEPARTMENT OF HEALTH

SEPTEMBER 2023

Author	INFORMATION AND RECORDS MANAGEMENT DIRECTORATE
Review Date	September 2026
Description	This document defines North West Department of Health' position on **protection of personal information**. It contains the compliance requirements, implementation and management.
Coverage	This document is applicable to all institutions and facilities of North West Department of Health.
Framework Number	***I&RM23/FR01/R26***

TABLE OF CONTENTS

1. PREAMBLE

1.1. The Protection of Personal Information Act 4 of 2013 (POPI Act) is a South African legislation dealing specifically and exclusively with protection of personal information. The Act came into effect on the 1st of July 2020. The purpose thereof 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.

1.2. The POPI Act regulates the manner in which personal information may be processed by establishing conditions, in harmony with international standards that prescribe the minimum threshold requirements for the lawful processing of personal information. The Act provides persons with rights and remedies to protect their personal information from processing that is not in accordance with it; and last but not least, it establishes voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by the Act.

1.3. Furthermore, all organisations were required to be compliant with the Act by the 1st of July 2021. In terms of section 1 of the POPI Act, the Department of Health is a public body, and therefore a responsible party as defined, that is subject to this Act due to the fact that it processes a substantial amount of personal information of various data subjects.

1.4. According to the POPI Act, It is a requirement that the Department should have an Information Officer who will then have Deputy Information Officer/s to provide assistance with duties bestowed upon them by the Act. As mentioned above that the POPI Act provides for justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information, it is therefore obvious that the Act acknowledges and works in conjunction with the Promotion of Access to information Act 2 of 2000 (PAIA), hence it provides

that the Information Officer of, or in relation to, public body means an Information Officer or Deputy Information Officer as contemplated in terms of Section 1 or 17 of PAIA. According to these sections of PAIA an Information Officer is the Head of the Department.

1.5. As mentioned above, the POPI Act provides for the establishment of an Information Regulator. This Information Regulator may, under section 112(2) thereof, make regulations in relation to, amongst others, responsibilities of Information Officers as referred to in section 55(1)(e) thereof. Therefore, in addition to responsibilities of Information Officers provided in section 55(1) of the Act, the Regulator, in ***Regulations Relating to the Protection of Personal Information No 1383***, dated 14 December 2018, provided additional responsibilities of Information Officers and such included, amongst others, to develop, implement, monitor and maintain a Compliance Framework.

1.6. This framework provides measures that the Department should put in place to ensure that the processing of personal information by its officials, operators and associates is in accordance with the conditions for lawful processing of personal information as envisaged in Chapter Three (3) of the POPI Act. In addition the Act also provides certain circumstances under which the Department may be exempted from such conditions, and section 38 specifically mentions those circumstances.

1.7. Furthermore, this framework provides measures that the Department should put in place to ensure that Special Personal Information is processed in accordance with the Act. According to section 26 of the Act processing of special personal information is prohibited and such information includes, amongst others, health information which the Department processes a substantial amount of on a regular basis. However, the Act also provides exceptions to such prohibitions and section 27 and 32 specifically exempt this Department from processing health information.

1.8. The framework will further provide measures that the Department should put in place to ensure that processing of personal information concerning children is also done in accordance with the Act as it is generally prohibited. However, the Act

provides exceptions to such prohibitions and section 35 specifically exempts the Department from processing personal information concerning children.

1.9. The Department shall have no liability to any official, operator, associates and/or any third party for any claim of any nature whatsoever which may arise out of the use of and/or reliance on the contents of this guide. Officials, operators, associates and/or any third party hereby waive any rights to any claim of any nature whatsoever which may arise out of the use of and/or reliance on this guide, and further indemnifies the Department against any claim of any nature whatsoever.

1.10. It is therefore advisable that officials of the Department, operators and associates should keep abreast of legislative developments, related guidelines issued by the Regulator and any case law relevant to the subject matter. If there is any conflict between the contents of this guide and the aforementioned legislative developments, related guidance issued by the Regulator and any relevant case law, members and associates must comply with the latter.

2. RATIONALE

2.1. This framework has been developed to serve as a guideline to officials, operators and associates of North West Department of Health regarding the processing of personal information.

2.2. The framework forms part of the overall risk management strategy. It is supported by policies, procedures and legislative framework that define and support sustainability and the protection of personal information of data subjects.

2.3. According to section 4(1) of the regulations, the Information Officer must, in addition to the responsibilities referred to in section 55(1) of the Act, ensure that a compliance framework is developed, implemented, monitored and maintained.

2.4. This compliance and regulatory framework has been prepared to provide a structured set of guidelines, standards and best practices to help the Department

to achieve compliance in terms of the POPI Act and its regulations. It will help the Department understand which compliance requirements are to be met and how to meet them.

2.5. This framework aims to guide the Department to accomplish the following tasks:

(a) Create a coherent picture of the current compliance status and implement the required steps to achieve that which it desires.

(b) Harmonise various regulatory mandate to understand its responsibilities.

(c) Manage and minimise risks.

(d) Utilise resources effectively to achieve and maintain compliance with minimal wastage of time and effort.

(e) Integrate new requirements into the existing compliance management.

2.6. In essence, the framework provides a standard in which the Regulator can judge the Department's compliance status by mapping its compliance program to the framework's requirements and demonstrate the improvements made to show the Department's compliance commitments.

3. DEFINITION OF TERMS

For the purpose of this framework, the following expressions bear the meanings assigned to them:

3.1. **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;

3.2. **Code of conduct** means a code of conduct issued in terms of Chapter 7;

3.3. **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;

3.4. **Consent** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

3.5. **Constitution** means the Constitution of the Republic of South Africa, 1996;

3.6. **Cyber security** means the practice of deploying people, policies, processes and technologies to protect organizations, their critical systems and sensitive information from digital attacks;

3.7. **Data subject** means the person to whom personal information relates;

3.8. **Department** means North West Department of Health;

3.9. **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;

3.10. **Encryption** means the process of converting information or data into a code, especially to prevent unauthorized access;

3.11. 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;

3.12. **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;

3.13. **Person** means a natural person or a juristic person;

3.14. **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;

3.15. **Prescribed"** means prescribed by regulation or by a code of conduct;

3.16 **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;

3.17. **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;

3.18. **Protection of Personal Information Act, POPIA or POPI Act"** means Protection of Personal Information Act 4 of 2013;

3.19. **Promotion of Access to Information Act"** means the Promotion of Access to Information Act (Act No. 2 of 2000);

3.20. **Pseudonymisation** is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

3.21. **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;

3.22. **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 anything 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;

3.23. **Regulator** means the Information Regulator established in terms of section 39;

3.24. Republic means the Republic of South Africa;

3.25. **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, a responsible party in this document will be the North West Department of Health;

3.26. **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; and

3.27. **Special personal information** means personal information.

4. SCOPE OF THE FRAMEWORK

4.1. This document is intended to govern and provide a framework which forms the structure that provides a holistic overview of how the Department creates, manages and processes personal information. This framework is applicable to all facilities in North West Department of Health, all employees regardless of whether they are permanent or on contract, interns, service providers or consultants doing business with the Department.

4.2. Every effort is made to ensure that the content of this framework is correct and aligned with legislation as at the date of its approval, however, the Department does not warrant that this framework deals with every aspect relating to the subject matter.

5. LEGISLATIVE FRAMEWORK

5.1. This Compliance framework should be read and applied in the context of the provisions of the following legislative framework:

(a) Constitution of the Republic of South Africa, Section 106 of 1996.
(b) National Archives and Records Service of South Africa Act (NARSSA), Act No 43 of 1996 as amended.
(c) Public Finance Management Act (PFMA), Act No 1 of 1999.
(d) Promotion of Access to information Act (PAIA), Act No 2 of 2000.

(e) Promotion of administrative Justice Act (PAJA), Act No. 3 of 2000.

(f) Electronic Communications and Transactions Act (ECTA), Act No. 25 of 2002.

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

(h) Protection of Personal Information Act (the POPI Act), Act No. 4 of 2013.

(i) Protection of Information, Act No. 84 of 1982.

6. ESTABLISHMENT OF THE GOVERNANCE FRAMEWORK

6.1. The Department should register the Information Officer with the office of the Information Regulator. As stipulated in the Promotion of Access to Information Act No. 2 of 2000, the Information Officer of the Department is the incumbent of the Head of Department position or the person who is acting as such. The Department should also designate a Deputy Information Officer.

6.2. The act allows organisations to designate more than one official as a Deputy Information Officer, if necessary. Given the size and complexity of North West Department of Health, it is advisable that more than one official should be designated as a Deputy Information Officer. These Deputy Information Officers should also be registered with the office of the Information Regulator.

6.3. The responsibilities of the Information Officer and/or Deputy Information Officers include:

6.3.1 The encouragement and ensuring compliance with the conditions for the lawful processing of personal information;

6.3.2 Dealing with the request made to the Department pursuant to the Act;

6.3.3 Working with the regulator in relation to investigations conducted pursuant to Chapter 10 of the POPI Act in relation to the Department;

6.3.4 **Further ensure that**:

a) The compliance framework is developed, implemented, monitored and maintained.

b) A personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

c) A PAIA manual is developed , monitored, maintained and made available as prescribed in section 14 and 51 of the Promotion of Access to Information Act (Act No. 2 of 200);
d) Internal measures are developed together with adequate systems to process requests for Information or access thereto;
e) Internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator;

6.3.5. The Information Officer shall upon request by any person, provide copies of the PAIA manual to that person upon the payment of a fee to be determined by the Regulator from time to time;

6.6.6. Ensure that an organisational structure clearly identifies operational roles;

6.3.7. Develop policies and procedures to give effect to the governance structure; and
6.3.8 Ensure that there is a review process of all policies and procedures.

6.3.9. In addition to the aforesaid responsibilities of the Information Officers and/or deputy Information Officers, it will be a good practice that a full record of reported incidents related to unauthorised access of personal information should be kept.

7. INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION

7.1. The Department must develop an internal policy on the protection of personal information. The policy must guide the organisation and/or its employees on how to process personal information and it should be aligned with the conditions for lawful processing and must incorporate the following:

(a) Develop a protection of personal information strategy;
(b) Integrate the protection of personal information with risk assessments and risk reporting;
(c) Develop a protection of personal information charter;
(d) Include protection of personal information in the mission, values and culture of the Department;
(e) Require employees to acknowledge and agree to adhere to the protection of personal information and/or privacy policies in writing;

(f) Conduct an annual review of the policy;

(g) Incorporate principles of ethical governance of personal information;

(h) Undertake an assessment of all processing activities undertaken per division;

(i) Each processing activity must be identified in terms of the relevant division, job function;

(j) Identify if there is compliance with the POPI Act in relation to each processing activity;

(k) Identify risks and identify mitigating measures linked to each processing activity;

(l) Assign individuals to implement the records management policy, tools and implementation plan;

(m) Categorise different types of information that is being processed (Personnel, Legal, Financial, Disaster Recovery, Commercial, and Operational);

(n) Develop an inventory of personal information;

(o) Record all processing activities and maintain a register of each processing activity;

(p) Develop a system to classify information and develop a retention and disposal policy in accordance with each data set, category of personal information;

(q) Conduct an audit of all current processes that collect, store, share, correct and delete personal information;

(r) Identify special personal information;

(s) Identify all personal information that is processed;

(t) Identify how personal information is collected;

(u) Identify where personal information is collected, stored and processed;

(v) Identify each person that processes personal information;

(w) Maintain a register of every activity conducted and its associated processing activity;

(x) Develop a procedure to enable the data subject to object to the processing of their personal information (Section 11);

(y) Develop a policy on record retention (Section 14);

(z) Develop a policy on information quality to ensure that information is updated and accurate;

(aa) Develop a procedure to deal with the correction and deletion of personal information (Section 24);

(bb) Develop a process to notify the data subject on the reason for processing, the type of information that is being processed, the details of the responsible party processing the personal information, if the necessary consent was secured, was the personal information collected directly from the data subject;

(cc) Conduct a process to map all personal information processing;

(dd) Ensure that the personal information mapping process is reviewed on a regular basis;

(ee) Establish a lawful basis for all processing of personal information;

(ff) Develop a framework to establish and assess legitimate interests;

(gg) Document the lawful basis for processing of personal information;

(hh) Establish a register of all consents that have been secured;

(ii) Review process to secure consents annually;

(jj) Develop a policy on internal and external sharing of personal information;

(kk) Develop an information asset register that keeps a record of systems, procedures and applications that are utilised for the processing and storage of personal information;

(ll) Ensure information is accurate by ensuring the integrity of all personal information;

(mm) Ensure employees who process personal information should compile a monthly report on personal information that is processed. The report must be escalated on a monthly basis or when necessary the Information Officer to ensure that they are fully aware of the current status of all processing activities; and

(nn) Develop a policy on the use of personal information for a specific purpose and its usage beyond the primary purpose of collection.

8. INFORMATION SECURITY

8.1. Information security has to do with maintenance of confidentiality, by ensuring that all types of information regardless of their form or medium are protected from unauthorized access and/or disclosure. Measures to ensure confidentiality include:

a) Appropriate security measures should be put in place to protect information on electronic, microfilm, microfiche or paper based format from possible breaches.

b) The Department should ensure that the integrity of its information is safeguarded so that it should remain authentic, accurate, reliable and complete.

c) Its processing methods should also be handled in the same manner. In addition, the Department must ensure that the right information is made available to the right people whenever required.

8.2. WHY INFORMATION SECURITY?

a) The Department and its information systems, both electronic and paper based face security threats from a variety of sources such as computer assisted fraud, sabotage, vandalism, theft, fire, floods.

b) Computer viruses and hacking are very common and become increasingly sophisticated, as a result, the Department should ensure that security is strengthened in this regard.

c) Since the Department is often exposed and vulnerable to security threats and litigations, protection of personal information in particular should be one of the primary concerns in system design.

8.3. INFORMATION SECURITY AND RECORDS MANAGEMENT

a) Properly managed records should also be well secured. This implies that the Department should conduct an assessment that would determine the security level of records, based on their nature, content and importance.

b) As a general rule, if the loss of information, access to or deletion/destruction of the same could cause damage to the Department, then stronger information security measures should be put in place.

8.4. STORAGE OF RECORDS

Records that have a potential of causing damage to the Department, should there be any data breach, need stronger and/or stricter storage solutions. Paper based records should be kept in registries or designated filing rooms. In cases where officials work with records that contain personal information, stricter measures should be put in place to protect them. At least the following measures should be put in place:

(a) Paper based records should be put in lockable cabinets or drawers when not in use.
(b) A clean desk policy should be adopted
(c) Eliminate access of third parties to offices where personal records are being processed.
(d) Implement access control registers in registries and filing rooms
(e) Files and papers containing personal information should be locked away at the end of the business.
(f) Avoid putting sticky notes with personal information anywhere in the offices or work stations.
(g) Electronic documents should be protected with strong passwords.
(h) Keep antivirus software up to date on all computers.
(i) Mobile devices should also be password protected.
(j) Do not leave documents out in the open, including in the printer output tray.
(k) Computers should not be left on overnight, during extended meetings and lunch breaks.

8.5. DISPOSAL OF ELECTRONIC AND PAPER BASED FILES

a) When personal information or any other sensitive digital and/or paper documents are no longer needed they should be disposed in accordance with the Departmental records management policy.

b) Spoiled papers and copies containing personal and sensitive information should be shredded and destroyed immediately. Computers and hard drives should also be properly destroyed.

8.6. TRAINING AND AWARENESS

a) Training and awareness on proper information security protocols should be done for all employees.

b) Employees should be made aware about passwords protection, destruction of electronics and any information held inside, document disposal, phishing scams, clean desk policy and most importantly, the print security, since the print vulnerabilities are increasing.

8.7. INFORMATION SECURITY POLICY

8.7.1. The Department must develop an Information Security Policy on the protection of personal information. An Information Security Policy can be defined as a plan that outlines the directives, regulations, rules and practices that prescribe how an organization manages, protects, and distributes information. The policy should regulate how the Department must manage, protect and distribute personal information and lay the framework for securing information, regardless of its form or medium. The policy must be well-written, enforceable and practical.

8.7.2. Since an Information Security Policy should set forth rules and processes for staff members, it would create a standard around the acceptable use of the Department's paper based and electronic information, including networks and applications to protect data confidentiality, integrity, and availability. As a result, the Information Security Policy should be a major step towards a comprehensive, consistent and meaningful security conscious environment within the Department.

8.7.3. Information security entails the creation of a condition to protect information, regardless of its form or medium against threats and vulnerabilities, incidental and/or deliberate unauthorised changes, destruction, disposal, removal, and/or disclosure. It is also characterised as the preservation of:

(a) **Confidentiality**: ensuring that information and associated assets are accessible only to those authorised to have access;
(b) **Integrity**: safeguarding the accuracy and completeness of information and;
(c) **Availability**: ensuring that authorised users have access to information and associated assets when required.

8.7.4. A good information security policy should contain the following characteristics, (this list is not all-inclusive):

a) Access control
b) Data classification and control
c) Risk assessment
d) Password and user ID management
e) Encryption and digital signatures
f) Instant messaging, PDAs and smart phones
g) Security awareness and training
h) Data privacy management
i) Corporate governance
j) Electronic mail, viruses, malicious code protection, and social engineering
k) Identity theft
l) Network security
m) Firewall
n) Communication security
o) Website and e-commerce
p) Security in third party contract
q) Document destruction and retention
r) Print security
s) Incident response
t) Contingency planning
u) Telecommuting and mobile computing
v) Intrusion Detection Systems.

8.7.5. Furthermore, the Information Security Policy should lay a solid foundation for the development and implementation of secure practices within the Department. The policy should not be instructional or overly descriptive, but must represent the rules that would be adhered to by the Department. Such compliance will require an understanding by staff of not only the policy, but also of the circumstances in which such compliance is expected in their day-to-day activities. Knowing the policy is only one half of the equation,

since staff needs to know how they should comply, from a procedural perspective.

9. PERSONAL INFORMATION IMPACT ASSESSMENT (PIIA)

9.1. The Information Regulator has under Section 112(2) of POPI Act made regulations relating to the protection of personal information. Regulation 4(1)(b) of Regulations Relating to the Protection of Personal Information No. 1383, prescribes that Information Officers must ensure that a Personal Information Impact Assessment (hereinafter referred to PIIA) is undertaken. PIIA is a process that is utilized to perform the following tasks:

(a) Identify types of personal information processed by the Department and the manner of processing;
(b) Assess compliance with the eight conditions for lawful processing of personal information;
(c) Identify risks associated with processing; and
(d) Propose mitigation measures aimed at minimizing the identified or anticipated risks.

9.2. Overview

9.2.1 PIIA should speak to the Departmental records management policy. It must be conducted to ensure that adequate measures and standards exist to comply with the conditions for lawful processing of personal information.

9.2.2 A PIIA should be conducted under specific circumstances, which include:

(a) High privacy risk projects.
(b) New or changed ways of processing of personal information that have the potential to have a significant impact on the privacy of data subjects.
(c) Profiling;
(d) Automatic decisions which lead to legal consequences for those affected;
(e) Systematic monitoring;

9.3. Examples of High Risk information processing

9.3.1. Further examples of processing information which would attract high risk include the following:

(a) Processing of special personal information on a large scale;
(b) The merging or linking of personal information;
(c) Personal information on incapacitated persons or those with limited ability to act;
(d) Use of new technologies or biometric procedures;
(e) Trans-border transfer of personal information to other countries; and
(f) Processing which obstructs data subjects from exercising their rights.

9.3.2 The identification, assessment and management of privacy risks should be considered as a fundamental component of accountability. Understanding the risks of the way the Department processes personal information is central for this privacy framework.

9.4. Purpose

9.4.1. The purpose of this document is to enable the identification, recording and minimizing of risks to the protection of personal information. This includes:

(a) The nature, scope, context and purposes of the processing;
(b) Assessing necessity, proportionality and compliance measures;
(c) Identifying and assessing risks to data subjects; and
(d) Identifying any additional measures to mitigate those risks.

9.4.2. A PIIA should identify the flow of personal information between the Department, its operators, data subjects and systems. The PIIA must identify procedures that eliminate, mitigate or reduce high risks.

9.4.3. The PIIA process should be documented, with appropriate document controls and should be reviewed as and when new personal information has to be processed or there are changes in the way personal information is being processed.

9.4.4. The document drafted would describe the following, the list is not exhaustive:

(a) How personal information is processed and the source;
(b) Who is accountable, responsible within the Department for the processing of the information;
(c) Purpose for which personal information is processed;
(d) How personal information will be processed;
(e) Personal information retention and disposal policy;
(f) How personal information will be managed and modified;
(g) How will personal information processors and application developers protect personal information;
(h) Identify any personal information transferred to other jurisdictions.

9.4.5. In conclusion, the guidelines from the information regulator should be used to draft the PIIA document and then be globalized in the Department to be completed, outlining all the personal information processed by each directorate and the manner of processing.

10. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

10.1. There are certain conditions to be met when processing personal information, and these are the backbone of the PIIA and they should be further elaborated and assessed in the PIIA document.

10.2. Section 4(1) and section 55(1) of the POPI Act state that the Information Officer has the duty to ensure compliance and that the eight (8) conditions for lawful processing of personal information are met. As part of the POPI Act implementation, the Information Officer is required to ensure that a preliminary Risk Assessment is conducted and that the below conditions are met:

(a) Accountability – is responsible for processing and ensuring compliance with the conditions for lawful processing of personal information.
(b) Processing limitation – certain limitations the Department has when processing personal information.

(c) Purpose specification – the purpose for which the personal information was collected.

(d) Further processing limitation – limitations when the personal information is to be further processed and sent to a third party.

(e) Information quality – ensuring that there are measures in place to ensure that the information collected is complete and accurate.

(f) Openness – notification of the data subject when collecting or processing their personal information.

(g) Security Safeguards – security measures on the integrity and confidentiality of personal information.

(h) Data subject participation – access and correction of the personal information by data subjects.

10.3. There is certain information that requires thorough attention when processing, therefore protocols have to be developed when processing such information (i.e. Children's information and special information). Furthermore, the Information Officer has to develop safeguards to ensure the lawful processing of children's information according to section 34.

11. RECORDS MANAGEMENT

11.1. The Department receives and keeps substantial amounts of personal information from data subjects, and this is to aid the carrying out of its mandates, to support its daily administrative operations, and fulfilling legal and other obligations. The Department should create and maintain authentic, reliable and usable records when rendering health care services to the communities, in supporting continuing service delivery to the people and when providing the required accountability.

11.2. Records management is a process of proper creation/receipt, maintenance, use and disposal of records throughout their life cycle. According to Section 14(1) of the POPI Act, records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—

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

(b) the Department reasonably requires the record for lawful purposes related to its functions or activities;

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

(d) The data subject or a competent person where the data subject is a child has consented to the retention of the record.

11.3. The Department, after having used a record of personal information of a data subject to make a decision about the data subject, must—

a) Retain the record for such period as may be required or prescribed by law or a code of conduct; or

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

11.4. The Department must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the Department is no longer authorised to retain the record. The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

11.5. To achieve good governance, effective and efficient administration, the Department should see sound records management as a fundamental principle. The Department must ensure that the integrity of records is protected for as long as they are required as evidence of business operations, by managing the information resources in terms of the Records Management Policy which should incorporate, at least, the following:

(a) Identification of what a record is.

(b) Identification of records that require additional protection.

(c) Retention and disposal periods.

(d) Identification of where records will be stored.

(e) Individuals assigned to implement the Records Management Policy, tools and implementation plan.

(f) The development of an Electronic Documents And Records Management System (EDRMS), which should enable access for certain categories of information to select employees, segregate duties to enhance protection of personal information.

(g) The register that should be maintained of all employees and their corresponding access to information technology systems and records.

(h) An audit of all contracts, such as Service Level Agreements, Operator Agreements, as well as information systems and ensure that they are aligned with the POPI Act.

(i) An audit of all processes that collect, disseminate, record, store and destroy personal information.

(j) Assignment of protection of personal information responsibilities and obligations to each employee in terms of their individual job descriptions.

(k) Incorporate protection of personal information mechanisms into how risk assessments are conducted and reported.

(l) Incorporate protection of personal information mechanisms into the processing of health and safety protocols.

(m) Development of a retention and disposal policy.

(n) Ensuring that staff are trained on policies and procedures.

(o) Ensuring that paperwork is disposed of securely through shredding.

(p) Adoption of strict controls on who can access personal information. Limiting access to necessary employees and documenting who has access to certain types of information. Blanket access of personal information to all employees should be avoided.

(q) A disaster management and recovery plan and a business continuity policy.

(r) Identify personal information and records that need to be backed-up.

(s) Store back-ups of electronic and systems offsite.

(t) A secure storage where personal information must be stored securely to prevent unauthorised access.

12. PROCESSING OF PERSONAL INFORMATION CONCERNING A CHILD

12.1. As the Department renders health care services to people, it also processes a substantial amount of personal information concerning children. Since the POPI

Act provides for lawful processing of personal information concerning children, the Department should ensure that it processes such in accordance with the Act.

12.2. Section 34 and 35 of the POPI Act, specifically provide for processing of personal information concerning children. According to section 34, processing of personal information concerning children is generally prohibited. Section 35, however, creates an exception to that prohibition as it provides grounds or circumstances under which the Department may process such information. Section 35(1) provides, as follows;

12.3. The prohibition on processing personal information of children, as referred to in section 34, does not apply if the processing is:

(a) carried out with the prior consent of a competent person;
(b) necessary for the establishment, exercise or defence of a right or obligation in law;
(c) necessary to comply with an obligation of National public law;
(d) for historical, statistical or research purposes to the extent that:

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

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

12.4. According to Section 35 (1) (a), processing of personal information concerning a child is acceptable if it is carried out with the prior consent of a competent person.

a) Section 1 of POPI Act defines a competent person as any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

b) As a result, the Department should always provide health care services to children in the presence and with the permission of their parents and/or guardian.

12.5. When it comes to further processing of personal information concerning children, for any purpose other than rendering health services to them, the Department should create reasonable means to ensure that it does not do so without prior consent of a competent person or prior authorisation of the Information Regulator per section 35(2) and (3) of the POPI Act, which provides as follows:

12.5.1 "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 *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.

12.5.2. 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:

(a) upon request of a competent person provide reasonable means for that person to:

i) Review the personal information processed; and

ii) Refuse to permit its further processing;

(b) Provide notice:

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

ii) how such information is processed; and

iii) regarding any further processing practices;

(c) 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

(d) Establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children."

12.6. The Department has a legal obligation to render health services to individuals as a government institution, therefore it is covered by Sec 35 (1) (b). Moreover, South African government, in terms of international law, is also obliged to provide its citizens with health care services as they form part and parcel of socio economic rights granted to every person in the world by international human rights law.

13. INTERNAL MEASURES THAT PROTECT DATA SUBJECTS' RIGHTS

13.1. Data subjects have the right to have their personal information processed in a manner that is in line with the conditions for lawful processing of personal information as referred to in Chapter three of the POPI Act. This places a demand on the Department to develop internal measures that protect data subjects' rights when processing their personal information, such as (Names, Identity numbers, contact details and others).

13.2. The Department should acknowledge that the data subjects have the following rights:

a) To be notified that:

i) their personal information is collected as provided for in terms of section 18; or

ii) their personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;

b) to establish whether the Department holds personal information of that data subject and to request access to their personal information as provided for in terms of section 23;

c) to request, where necessary, the correction, destruction or deletion of their personal information as provided for in terms of section 24;

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

e) to object to the processing of their personal information—

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

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

f) not to have their personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1);

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

h) to submit a complaint to the Information 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

i) To institute civil proceedings regarding the alleged interference with the protection of their personal information as provided for in section 99.

13.3. The Department collects personal information from data subjects as patients in;

a) Health facilities, students in colleges and universities, from companies as service providers as well its employees.

b) The Department should therefore come up with measures that will ensure that their rights mentioned in Chapter Three of the Act are catered for.

13.4. Data subjects need to be notified that their personal information is being collected.

13.4.1. The Department is expected to do so by taking reasonable practical steps that will ensure that the data subjects are aware that their information is

being collected and for what purpose, i.e., the Department should have consent forms that will be used by different units that process personal information.

13.4.2. Contents of consent forms should be read and thoroughly explained to data subjects before they can be completed and signed. Furthermore, notices detailing data subjects' rights and the protection of their personal information should be developed in different languages.

13.4.3. Notices should be placed in areas where such information is usually collected and can easily be seen and read by data subjects.

13.5. The Department should come up with measures to notify data subject when their personal information has been accessed or acquired by an unauthorised person as provided for by the Act.

13.6. An official who is processing personal information and becomes aware that someone accessed it unlawfully must inform his or her superior within reasonable time who should then inform the Information Officer of that incident.

13.7. In the case of an Operator, the contract manager should be informed of the incident within reasonable time who should then inform the Information Officer of that incident.

13.8. The Information Officer will then inform a data subject as urgent as possible and take necessary steps in terms of section 22 of the POPI Act.

Data subject should be informed so that they can assist the Department take necessary steps to prevent any harm that might arise as a result of the unlawfully accessed personal information.

14. DEALING WITH INFORMATION ACCESS REQUESTS

14.1. One of the Information Officer's responsibilities include dealing with requests made to the Department pursuant to the POPI Act, Section 55(1)(b). Data subjects are authorised by the POPI Act to request that their personal information be amended or deleted in circumstances where such information has become outdated, inaccurate, incomplete, misleading, or excessive, has been unlawfully obtained, or if the Department is no longer entitled to retain the information.

14.2. Records held by the Department may be accessed on request only once the requirements for request for access have been met. In terms of PAIA, a requester may be any person making a request to access a record held by the Department, or a person acting on behalf of the person to whom the personal information belongs to.

14.3. The request for access to personal information must be made in the prescribed form to the Information Officer of the Department at their address or via e-mail. The provisions of sections 18 and 53 of PAIA apply to requests for information made in terms of the POPI Act. The request form must include an adequate amount of information to provide sufficient particulars to enable officials of the Department to ascertain what record or records are being requested, who the requester is, as well as a postal or email address of the requester within the Republic.

13.4. Where a request is made on behalf of someone else, the requester needs to submit proof of the capacity in which they are making the request. Where a requester is illiterate or has a disability that prevents them from completing a form, they may make the request for access to the record verbally or through other means. The Information Officer is then responsible for putting the request into writing and providing the requester with a copy.

14.5. Thereafter, the Department should provide data subjects with confirmation that they hold their personal information and this should not come at any cost. The Department should provide the data subject with a description of the personal information processed and confirm to whom the personal information has been/will be shared with. Such request from a data subject must be complied with –

(a) within a reasonable time;
(b) at a prescribed fee (may be levied before the actual record or description of the personal information is made available to the data subject);
(c) in a reasonable manner and format; and
(d) In a form that is generally understandable.

14.6. Should the Department not wish to provide personal information to a data subject such refusal must be based on the same grounds for refusal as allowed under PAIA, according to which, an Information Officer is obliged to refuse access to a record if disclosure thereof involves the unreasonable disclosure of personal information about

a third party, including "deceased individuals". The principle is that a third party should decide on the disclosure of such information themselves.

14.7. The POPI Act obliges the Department to provide access to personal information concerning a data subject only to that data subject upon their request, unless they have consented otherwise, and may require that sufficient proof of the identity of the data subject be provided before receiving access to their personal information. The Department should then comply with such a request within a reasonably practicable timeframe and tender proof that the request had been complied with.

15. PROCESSING OF SPECIAL PERSONAL INFORMATION

15.1. According to section 26 of the POPI Act, the Department is prohibited from processing special personal information of data subjects if it concerns the following:

a) Religious beliefs;
b) Philosophical beliefs;
c) Race;
d) Ethnic origin;
e) Trade union membership;
f) Political persuasion;
g) Health;
h) Sex life; or
i) Biometric information; or
j) The criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

15.2. Section 27 of the POPI Act further states instances wherein the prohibition for the Department to process the above stated special personal information would not apply, and that is if the:

a) Processing is carried out with the consent of the data subject in question;

b) Processing is necessary for the establishment, exercise or defence of a right or obligation in law;
c) The processing is necessary to comply with an obligation of international public law;
d) Processing is for historical, statistical or research purposes to the extent that the;
e) purpose serves a public interest and the processing is necessary for the purpose concerned; or
f) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;
g) Information has been deliberately made public by the data subject.

15.3. The Regulator may, upon an application by the Department and by notice in the *Gazette,* authorise the Department 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.

15.4. Processing personal information concerning religious or philosophical beliefs (section 28)

15.4.1. Processing of special personal information concerning the religious and philosophical beliefs of the data subjects may be done, provided that it is carried out by:

a) Spiritual or religious organizations, or independent sections of those organisations if-

i) the information concerns data subjects belonging to those organisations; or
ii) it is necessary to achieve their aims and principles;

(b) 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;

(c) 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.

15.4.2. In the cases referred to above, 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.

15.4.3. Even though the Department may process special personal information concerning a data subject's religious or philosophical beliefs, that information may not be supplied to third parties without the consent of the data subject.

15.4.4. Processing personal information concerning the race or ethnic origin (section 29)

15.4.4.1. Processing of special personal information concerning a data subject's race or ethnic origin may be done, provided that it is carried out to:

a) Identify data subjects and only when this is essential for that purpose; and

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

15.5. Processing personal information concerning trade union membership (section 30)

15.5.1. Processing special personal information concerning a data subject's trade union membership may only be done by the trade union to which the data subject belongs, or its federation. Personal information of the data subject may not be supplied to third parties without the consent of the data subject.

15.6. Processing personal information concerning political persuasion (section 31)

15.6.1. The prohibition on processing personal information concerning a data subject's political persuasion 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. Once again, personal information of the data subject may not be supplied to third parties without the consent of the data subject.

15.7. Processing personal information concerning health or sex life

15.7.1. Processing special personal information concerning a data subject's health or sex life is allowed, provided that it is processed by:

(a) 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

(b) Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary:

i) 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;

ii) For the performance of an insurance or medical scheme agreement; or

iii) For the enforcement of any contractual rights and obligations;

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

(d) any health facility, managing the care of a child if such processing is necessary for the performance of their lawful duties;

(e) Any health facility, if such processing is necessary in connection with the implementation of prison sentences or detention measures;

(f) Administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for:

i) 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;

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

15.8. In all these cases, the information may only be processed by the Department subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the Department and the data subject.

15.9. When processing a data subject's health or sex life, the Department must treat the information as confidential, unless it is required by law or

in connection with its duties to communicate the information to other parties that are authorized to process such information.

15.10. The prohibition on processing special personal information does not apply if it is necessary to supplement the processing of personal information concerning a data subject's health, with a view to the proper treatment or care of the data subject.

15.11. 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.

15.12. Processing personal information concerning criminal behaviour or biometric information (section 33)

15.12.1. Processing special personal information concerning a data subject's criminal behaviour or biometric information may be done, provided that the Department has obtained that information in accordance with the law.

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

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

16. TECHNICAL AND ORGANISATIONAL MEASURES TO MITIGATE CIVIL ACTIONS

16.1. The Department ought to actualize its intention of complying with the POPI Act. It would be in the best interest of the Department to comply

since generally, frequency and regularity of data breaches grow in number. In addition to that, data subjects are becoming more educated on their personal information rights in terms of the POPI Act. This calls for measures to be put in place to safeguard the Department against such actions. The measures developed will have both organisational and technical implications with regards to the Department's agenda of complying with the POPI Act. The following are some of the technical and organisational measures the Department should adopt:

16.2. Technical measures

16.2.1. Technical measures can be defined as the measures and controls afforded to systems and any technological aspect of an organisation, such as hardware, networks and software. Protecting such aspects is crucial for the security of personal Information and is the best line of defense against data breaches. Here are some of the most common technical measures the Department should implement:

(a) **Cyber security** – Firewalls, malware scans, anti-virus protection, patches and updating the software when required are the most common technical security measures the Department should implement in order to safeguard the personal information processed against cyber-attacks.

(b) **Encryption and pseudonymisation** – These two technical security measures should also be used by the Department to protect personal information.

(c) **Physical security** – Security lighting and alarms, access logs and CCTVs should be available and well-functioning to ensure effective protection of personal information processed within the Department. Visitors must be checked in accordance with a predetermined procedure and they should not be left alone while in the Department's premises.

(d) **Appropriate disposal** – Disposal of paperwork and devices that contain personal data must be done in a way that personal

information cannot be retrieved by an unauthorised person, whether intentionally or unintentionally. Shredding of documents that are no longer needed must also be done in every office. The Department should therefore provide employees with enough shredding machines. The secure disposal of digital databases and hardware devices must also be ensured.

(e) **Passwords** – The Department should ensure that devices such as computers, laptops, cell phones, are protected with strong passwords only known by the user thereof. There should be a policy in place for setting strong passwords. It should be ensured that documents and systems containing sensitive data are also password protected.

(f) **Access rights** – Access to databases containing personal information should be granted on a need-to-know basis and it must be ensured that there is no blanket access to all employees. Thus the Department should have Access of Personal Information Policy in place.

16.3. Organisational measures

16.3.1. Organisational measures consist of internal policies, organisational methods or standards, and controls and audits that controllers and processors can apply to ensure the security of personal information. They can include, but are not limited to:

(a) **Information security policies** – The Department should have information security polices, such as Records Management policy, and assign individuals to implement then policies in accordance with the developed implementation plan.

(b) **Business continuity plan** – The Department should have policies and measures in place to back-up personal information and ensure that it can be recovered and maintained in the event of an incident. Measures should be put in place to ensure that backup personal information is protected from any possible data breach.

(c) **Risk assessments** – The Department should ensure that the Risk Management Unit conducts risk assessments to identify activities that have a potential of having personal information being damaged, lost or accessed in an unauthorised manner in the midst of processing it. Subsequent to that, the Department should identify mitigating measures linked to each processing activity.

(d) **Other policies and procedures** – The Department should have robust and easy to follow policies and procedures that will help its employees to know what their obligations are and what to do if certain situations occur. Examples could include a clean desk policy, remote work policy, and data breach procedures.

(e) **Training programmes** – The Department should develop a comprehensive training plan for Information Officers, as well as employees in general to ensure that they are all empowered and have a knowledge of legal requirements and what is expected of them.

(f) **Awareness programmes** - The Department should develop internal and external awareness programmes on Protection of Personal Information to ensure that all employees are aware of the importance of protection of personal information.

(g) **Reviews and audits** – Having policies and procedures in place is not enough. The Department needs to make sure that they are effective. As a result, it is important to establish controls and audits to evaluate the effectiveness, correct what is not working and improve whatever could have been done better. Having said that, the Department should have regular audits and reviews to see if their policies and procedures are effective enough to produce a desired result.

(h) **Due diligence** – The Department may be held liable for using systems and procedures that cannot guarantee that personal information of data subjects is secured. It is therefore imperative to establish due diligence checks before the Department commits

to using new systems and procedures and to regularly conduct compliance checks.

16.4. Contracts and service level agreements

16.4.1. Ensuring that all contracts that are entered into between the Department and stakeholders are POPI Act compliant.

16.5. **Breach management**

16.5.1. Should security of personal information be compromised, the Department should implement the following procedures:

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

i) the Regulator; and

ii) Subject to 16.5.1.3, the data subject, unless the identity of such data subject cannot be established.

b) The notification referred to in 16.5.1.1 must 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 Department's information system.

c) The Department may only delay notification of 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.

d) The notification to a data subject referred to in 16.5.1.1 must be in writing and communicated to the data subject in at least one of the following ways:

i) Mailed to the data subject's last known physical or postal address;
ii) Sent by e-mail to the data subject's last known e-mail address;
iii) Placed in a prominent position on the website of the Department;
iv) Published in the news media; or
v) As may be directed by the Regulator.

e) The notification referred to in 16.5.1.1 must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

i) A description of the possible consequences of the security compromise;
ii) A description of the measures that the Department intends to take or has taken to address the security compromise;
iii) A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
iv) If known to the Department, the identity of the unauthorised person who may have accessed or acquired the personal information.

f) The Regulator may direct the Department to publicize, 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.

17. FRAMEWORK MANAGEMENT, IMPLEMENTATION AND MONITORING

17.1. Implementation and Monitoring

a) The Information Officer shall ensure the implementation of the framework as well as monitor and evaluate compliance to the same.

17.2. Framework audit, review and amendments

a) Regular compliance audits shall be performed in order to ensure compliance with this framework.

b) This framework shall be reviewed as and when necessary depending on amendment of the POPI Act.

17.3. Breach of framework

17.3.1. A breach of this framework essentially means a contravention of the POPI Act, as a result, the responsible party and/or the Department may be liable to severe penalties, in the case of a contravention of—

(a) Section 100, 103(1), 104(2), 105(1), 106(1), (3) or (4) to a fine or imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment; or Section 59, 101, 102, 103(2) or 104(1), to a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

17.3.2. Any breach of this framework shall be investigated and depending on the outcome, civil and criminal legal action shall be instituted against the responsible party.

18. *FRAMEWORK APPROVAL:*

Recommended/ ~~not recommended~~

Mr. J. De Beer
Chief Director: Strategy and Systems

16/10/2023
Date

Approved/ not approved

Mr. O. E. Mongale
Head of Department
North West Department of Health

17/10/2023
Date