A: PROTECTION OF PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

1. **PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013 MEDILINKSA POPI POLICY 2021**

2. **DEFINITIONS**

2.1. **Client** means a natural or juristic person who has entered into an agreement with Medilink for the rendering of services by Medilink;

2.2. **Consent** means the voluntary, specific and informed expression of will;

2.3. **Data Subject** means the natural or juristic person to whom the Personal Information relates;

2.4. **Direct Marketing** means approaching a Data Subject personally for the purpose of selling them a product or service, of requesting a donation;

2.5. **Medilink** means Medilink (Pty) Ltd with Registration 2016/259491/07

2.6. **POPI (hereinafter "POPI")** means the Protection of Personal Information Act, No. 4 of 2013;

2.7. **Personal Information** means information relating to an identifiable, living, natural person, or an identifiable, existing juristic person, as defined in POPI or in any other legislation with equivalent standing where applicable;

2.8. **Processing** means *inter alia* an operation or activity, whether or not by automatic means, concerning Personal Information, as defined in POPI.

3. INTRODUCTION

MedilinkSA (Pty) Ltd ("Medilink") is an Independent Medical Switching Software company that is obligated to comply with The Protection of Personal Information Act 4 of 2013.

POPI requires Medilink to inform their data subjects as to the manner in which their personal information is stored, used, disclosed and destroyed. Medilink guarantees its commitment to protecting its data subjects' privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

The Policy sets out the manner in which Medilink deals with their data subjects' personal information and stipulates the purpose for which said information is used. The Policy is made available on the Medilink website www.medilinksa.co.za and by request from Medilink's office at 38 Saturn Crescent Linbro Park, Johannesburg.

4. SCOPE OF THE POLICY

The Policy applies to all Medilink employees, directors, sub-contractors, agents, and appointees. The provisions of the Policy are applicable to both on and off-site processing of personal information.

5. PERSONAL INFORMATION COLLECTED

Section 10 of POPI states that "*Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.*"

Medilink collects and processes personal information for purposes of Claims switching. The type of information will depend on the need for which it is

collected and will be processed for that purpose only. Whenever possible, Medilink will inform the data subject or client as to the reason information is required and the information deemed optional. Examples of personal information belonging to data subjects, that Medilink collects includes, but is not limited to:

Entity Type	**Personal Information Processed**
Natural Persons	Names; contact details; date of birth; ID; gender; confidential correspondence.
Customer – Juristic Persons / Entities	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; authorised signatories.
Contracted Service Providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; authorised signatories;
Employees / Directors	Gender; pregnancy; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being.

Medilink also collects and processes data subjects' personal information for marketing purposes in order to ensure that its products and services remain relevant to its clients and potential clients.

Medilink aims to have agreements in place with all product suppliers, insurers and third-party service providers to ensure a mutual understanding with regard to the protection of the data subjects' personal information. Medilink suppliers will be subject to the same regulations as applicable to them.

For purposes of this Policy, clients include potential and existing clients.

6. THE USAGE OF PERSONAL INFORMATION

The data subjects' Personal Information will only be used for the purpose for which it was collected and as agreed. This may include:

- Providing products or services to clients and to carry out the transactions requested;
- For billing;
- Assessing and processing claims;
- Conducting credit reference searches or verification;
- Confirming, verifying and updating client details;
- For submitting a claim to the relevant medical aid scheme on behalf of the client;
- For purposes of claims history;
- For purposes of managing processing adjustments of the medical aid schemes;
- For the detection and prevention of fraud, crime, money laundering or other malpractices;
- Conducting market or customer satisfaction research;
- For audit and record keeping purposes;
- In connection with legal proceedings;

- Providing Medilink services to clients, to render the services requested and to maintain and constantly improve the relationship;
- Providing communication in respect of Medilink and regulatory matters that may affect clients; and
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

According to section 11 of POPI, personal information may only be processed if certain conditions, listed below, are met along with supporting information for Medilink processing of Personal Information:

a) The data subject consents to the processing: consent is obtained from clients during the introductory and on-boarding stage of the relationship.
b) The necessity of processing: as provided for in paragraph 6.
c) Processing complies with an obligation imposed by law on Medilink;
d) Processing is necessary for pursuing the legitimate interests of Medilink or of a third party to whom information is supplied: in order to provide Medilink clients with products and or services, both Medilink and any of its product suppliers require certain personal information from the clients in order to make an expert decision on the unique and specific product and or service required.

7. DISCLOSURE OF PERSONAL INFORMATION

Medilink may disclose a data subject's personal information to any of the Medilink companies or subsidiaries, joint venture companies and or approved product or third-party service providers whose services or products clients elect to use. Medilink has agreements in place to ensure compliance with confidentiality and privacy conditions.

Medilink may also share client personal information with and obtain information about clients from third parties for the reasons already discussed above. Medilink may also disclose a client's information where it has a duty or

a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary to protect Medilink's rights.

8. SAFEGUARDING CLIENT INFORMATION

It is a requirement of POPI to adequately protect personal information. Medilink will continuously review its security controls and processes to ensure that personal information is secure. The following procedures are in place to protect personal information

The **MEDILINK INFORMATION OFFICER** is Robert Jubber whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI. He is assisted by Abbas Sheik who will function as Medilink's Deputy Information Officer;

THIS POLICY has been put in place throughout Medilink and training on this policy and the POPI Act has already taken place;

Each new employee will be required to sign an **EMPLOYMENT CONTRACT** containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;

Every employee currently employed by Medilink will be required to sign an addendum to their **EMPLOYMENT CONTRACTS** containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;

- Medilink product suppliers, insurers and other third-party service providers will be required to sign a **SERVICE LEVEL AGREEMENT** guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.

- All electronic files or data are **BACKED UP** on Xneelo and 1 Grid which is subject to the same privacy rules and conditions.
- Karabo IT is responsible for system security that protects third party access and physical threats. Karabo IT is responsible for Electronic Information Security.

CONSENT to process data subjects' information is obtained from clients (or a person who has been given authorisation from the data subject to provide the data subject's personal information) during the introductory and on-boarding stage of the relationship.

9. ACCESS AND CORRECTION OF PERSONAL INFORMATION

Data subjects have the right to access the personal information Medilink holds about them. Data subjects and clients also have the right to ask Medilink to update, correct or delete personal information on reasonable grounds. Once a data subject objects to the processing of their personal information, Medilink may no longer process the said personal information. Medilink will take all reasonable steps to confirm its clients' identity before providing details of data subjects' personal information or making changes to their personal information.

9.1. The details of Medilink's Information Officer and Head Office are as follows:

INFORMATION OFFICER DETAILS

NAME: Robert Jubber

TELEPHONE NUMBER: 0746669777

E-MAIL ADDRESS: robert@medilinksa.co.za

DEPUTY INFORMATION OFFICER DETAILS

NAME: Abbas Sheik

TELEPHONE NUMBER: 0834126166

E-MAIL ADDRES: abbas@medilinksa.co.za

HEAD OFFICE DETAILS

TELEPHONE NUMBER: 011 679 4625

POSTAL ADDRESS: P.O Box 552, Wendywood, 2144

PHYSICAL ADDRESS: 38 Saturn Crescent, Linbro Park, Johannesburg

E-MAIL ADDRESS: info@medilinksa.co.za

WEBSITE: www.medilinksa.co.za

10. AMENDMENTS TO THIS POLICY

Amendments to, or a review of this Policy, will take place on an *ad hoc* basis or at least once a year. Clients are advised to access Medilink's website periodically to keep abreast of any changes. Where material changes take place, clients will be notified directly, or changes will be stipulated on the Medilink website.

11. AVAILABILITY OF THE MANUAL

This manual is made available in terms of Regulation Number R. 187 of 15 February 2002.

12. RECORDS THAT CANNOT BE FOUND

If Medilink searches for a record and it is believed that the record either does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken the attempt to locate the record.

13. THE PRESCRIBED FORMS AND FEES

The prescribed forms and fees are available on the website of the Department of Justice and Constitutional Development at www.justice.gov.za under the forms section.

B: POLICY ON THE RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS

1. PURPOSE

1.1. To exercise effective control over the retention of documents and electronic transactions:

1.1.1. as prescribed by legislation; and

1.1.2. as dictated by business practice.

1.2. Documents need to be retained in order to prove the existence of facts and to exercise rights Medilink may have. Documents are also necessary for defending legal action, for establishing what was said or done in relation to business of Medilink and to minimize its reputational risks.

1.3. To ensure that Medilink's interests are protected and that its and clients' rights to privacy and confidentiality are not breached.

1.4. Queries may be referred to the Information Officer.

2. SCOPE & DEFINITIONS

2.1. All documents and electronic transactions generated within and/or received by Medilink.

2.2. Definitions:

2.2.1. **Clients Client** means a natural or juristic person who has entered into an agreement with Medilink for the rendering of services by Medilink

2.2.2. **Confidential Information** refers to all information or data disclosed to or obtained by Medilink by any means whatsoever and shall include, but not be limited to:

2.2.2.1. financial information and records; and

2.2.2.2. all other information including information relating to the structure, operations, processes, intentions, product information, know-how, trade secrets, market opportunities, customers and business affairs but excluding the exceptions listed in clause 4.1 hereunder.

2.2.3. **Constitution**: Constitution of the Republic of South Africa Act, 108 of 1996.

2.2.4. **Data** refers to electronic representations of information in any form.

2.2.5. **Documents** include books, records, security or accounts and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.

2.2.6. **ECTA**: Electronic Communications and Transactions Act, 25 of 2002.

2.2.7. **Electronic communication** refers to a communication by means of data messages.

2.2.8. **Electronic signature** refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.

2.2.9. **Electronic transactions** include e-mails sent and received.

2.2.10. **PAIA**: Promotion of Access to Information Act, 2 of 2000.

3. ACCESS TO DOCUMENTS

3.1. All Medilink and data subject information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances:

3.1.1. where disclosure is under compulsion of law;

3.1.2. where there is a duty to the public to disclose;

3.1.3. where the interests of Medilink require disclosure; and

3.1.4. where disclosure is made with the express or implied consent of the client or data subject.

3.2. Disclosure to 3rd parties:

3.2.1. All employees have a duty of confidentiality in relation to Medilink and data subjects:

3.2.2. Information on clients:

3.2.3. Medilink's clients' and data subjects' right to confidentiality is protected in the Constitution and in terms of ECTA. Information may be given to a 3rd party if the client has consented in writing to that person receiving the information.

3.2.4. Requests for company information:

3.2.5. These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like Medilink, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

3.2.6. In terms hereof, requests must be made in writing on the prescribed form to the Information Officer. The requesting party has to state the reason for wanting the information and has to pay a prescribed fee.

3.2.7. Confidential company and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of Medilink must be kept strictly confidential at all times.

3.2.8. Medilink views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

4. STORAGE OF DOCUMENTS

4.1. *HARD COPIES*

4.1.1. **Documents are stored in an archive in a different location.**

a. **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.

b. 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;
- Services rendered;
- 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.

c. 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 the Magistrate's Court Act No 32 of 1944:

- Civil Court Judgments

Documents with a required retention period of 2 years:

- 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.

d. 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.

e. 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.

f. 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.

g. 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.

h. 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.

i. 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.

j. 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.

k. 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 the return 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) requires 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.

l. 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.

m. 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.

5. ELECTRONIC STORAGE

- All electronically held Personal Information must be saved in a secure database;
- As far as reasonably practicable, no Personal Information should be saved on individual computers, laptops or hand-held devices;
- All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently;
- Medilink shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day;
- Electronical Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant

database. The employee must ensure that the information has been completely deleted and is not recoverable.

- Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

6. DESTRUCTION OF DOCUMENTS

- Documents may be destroyed after the termination of the retention period specified herein, or as determined by Medilink from time to time.
- Each department is responsible for attending to the destruction of its documents and electronic records, 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.
- The documents must made available for collection approved document disposal company.
- Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.