DATA PROTECTION POLICY

Document Control

Status

Version Number: 1.0 **Date:** **[24/06/2020]**

File Location: [Incon Health Clinics HO]/ Operations / Compliance

Version No.	Review Date	Reason for Change	Author	To be Reviewed By
1.00	Review date 24th June 2021	To assess any changes to be made.	Gert Jacobus Visagie	Gert Jacobus Visagie
2.00	27 October 2021	Schedules and change in Information Officer	Gert Jacobus Visagie	Gert Jacobus Visagie Lucretia Thomas

Version No.	Approval Date	Acceptance Name	Acceptance Title
1.0	24th June 2020	Lucretia Thomas	Operations /QMS manager.

Revision History

Document Approval

CONTENTS

CLAUSE

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their Personal Information is handled. During the course of our activities we shall Process Personal Information about our clients, clients' employees, suppliers, other third parties and own Personnel. We recognise that the correct and lawful treatment of this data will maintain confidence in the company, providing for successful business operations.

1.2 This policy applies to all INCON HEALTH CLINICS (Pty) Ltd ("INCON HEALTH") Personnel (including You). You must read, understand and comply with this policy when Processing Personal Information on our behalf and attend training on its requirements. This policy sets out what We expect from You in order for Us to comply with applicable law. Your compliance with this policy is mandatory.

1.3 Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The types of Personal Information that INCON HEALTH ("We" / "Us") may be required to handle include information about current, past and prospective clients', clients' employees and others that we communicate with and our own employees or contractors. The Personal Information, which may be held on paper or on a computer or other media, is subject to certain conditions specified in the Protection of Personal Information Act 2013 (the Act) and other regulations and where applicable the General Data Protection Regulation (EU) 2016/679 ("GDPR")

2.2 This policy and any other documents referred to in it sets out the basis on which We shall process any Personal Information We collect from Data Subjects, or that is provided to us by Data Subjects or other sources.

2.3 This data protection policy ensures that INCON HEALTH:

Complies with data protection law and follows good practice;

Protects the rights of Personnel, clients, clients' employees, and partners;

Is open about how it stores and processes individuals' information;

Protects itself from the risks of a data breach.

(a)

(b)

(c)

(d)

2.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.5 This policy sets out rules on data protection and the legal conditions that must be satisfied when Personal Information is Processed.

2.6 Where You have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Privacy Standard or otherwise then you must comply with the Related Policies and Privacy Guidelines.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 "**Automated Decision-Making (ADM)**": when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. Take note that Automated Decision-Making is not Automated Processing..

3.2 "**Consent**" means an agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Information relating to them.

3.3 "**Data**" is information which is stored electronically, on a computer, or in certain paperbased filing systems.

3.4 "**Data Privacy Impact Assessment (DPIA)**" means tools and assessments used to identify and reduce risks of a data Processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Information.

3.5 "**Data Subjects**" for the purpose of this policy means a Person to whom the Personal Information relates and whom we hold Personal Information for. A Data Subject need not be a Republic of South Africa national or resident. All Data Subjects have legal rights in relation to their Personal Information.

3.6 "**Data Users**" are those of our Personnel whose work involves Processing Personal Information. Data Users must protect the Data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.7 "**Explicit Consent**": consent which requires a very clear and specific statement, that is, not just action.

3.8 "**Operators**" (referred to as "Processors" under the GDPR) 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. Employees of Responsible Parties are excluded from this definition, but it could include suppliers which handle Personal Information on behalf of INCON HEALTH. We act as Operator where we Process Personal Information on behalf of third parties.

3.9 "**Person**" means identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

3.10 "**Personal Information**" means information relating to a 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.

3.11 "**Personnel**" means all employees, workers, contractors, agency workers, consultants, directors, members and others.

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

3.13 "**Privacy by Design**" means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the Act and GDPR.

3.14 "**Privacy Notices**" or "**Privacy Policies**" means separate notices setting out information that may be provided to Data Subjects when INCON HEALTH collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

3.15 "**Processing**" or "**Process**" 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.

3.16 "**Responsible Party**" (referred to as "Controller" under the GDPR) 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. The Responsible Party is responsible for establishing practices and policies in line with the Act. We are the Responsible Party/ Controller of all Personal Information used in our business for our own commercial purposes.

3.17 "**Special Personal Information**" means:

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(b) the criminal behaviour of a data subject to the extent that such information relates to—

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

Special Personal Information can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DUTIES AND RESPONSIBILITIES

4.1 All Personnel that work for or has been instructed by INCON HEALTH have a responsibility to ensure that INCON HEALTH Data is Processed appropriately.

4.2 Each Data User that handles Personal Information must ensure that it is handled and processed in line with this policy and data protection principles.

4.3 However, the following people have key areas of responsibility:

(a) The board of directors is ultimately responsible for ensuring that INCON HEALTH meets its legal obligations.

(b) The Information Officer is responsible for:

(i) Keeping the board updated about data protection responsibilities, risks and issues;

(ii) Ensuring a compliance framework is developed, implemented, monitored and maintained;

(iii) Ensuring internal measures are developed together with adequate systems to process requests for information or access thereto;

(iv) Reviewing all data protection procedures and related policies, in line with an agreed schedule;

(v) Ensuring Personal Impact Assessments are done so as to ensure that adequate measures and standards exist and thereby ensuring our compliance with the legal Processing of Personal Information;

(vi) Ensuring the development of a Section 51 Promotion of Access to Information Manual as well as monitoring and maintaining the manual and ensuring it is made available to interested parties. A fee, as prescribed by the Regulator from time to time, may be charged for any copies of the manual;

(vii) Arranging data protection training and advice for the people covered by this policy. The training must include awareness session on the provisions of the POPI Act, codes of conduct and other information as obtained from the Regulator;

(viii) Handling data protection questions from Personnel and anyone else covered by this policy;

(ix) Dealing with requests from individuals to see the Data which INCON HEALTH holds about them (also called 'Data Subject access requests').

(x) Checking and approving any contracts or agreements with third parties that may handle the company's clients', their employees or our employees' Personal Information, Special Personal Information or Confidential Information.

(c) The IT manager is responsible for:

(i) Ensuring all systems, services and equipment used for collecting and storing Data meet acceptable security standards.

(ii) Performing regular checks and scans to ensure security hardware and software is functioning properly.

(iii) Evaluating any third-party services, the company is considering using to store or Process Data. For instance, cloud computing services.

(d) The marketing manager is responsible for:

(i) Approving any data protection policies / statements attached to communications such as emails, websites or letters.

(ii) Addressing any data protection queries from journalists or media outlets like newspapers.

(iii) Where necessary, working with other Personnel to ensure marketing initiatives abide by data protection principles, including those relating to direct marketing.

(e) The Information Officer ("IO") or the person responsible for the IO obligations must ensure compliance with the Act and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Information Officer on compliance@incon.co.za. In the following circumstances you must **always** contact the IO:

(i) if you are unsure of the lawful basis which you are relying on to process Personal Information (including the legitimate interests used by INCON HEALTH (see paragraph 8.2 below);

(ii) if you need to rely on Consent and/ or need to capture Explicit Consent;

(iii) if you need to draft privacy policies or statements (see clause 12);

(iv) if you are unsure about the retention period for the Personal Information being Processed (see clause 9.6);

(v) if you are unsure about what security or other measures you need to implement to protect Personal Information (see clause 13);

(vi) if there has been a Personal Information breach (clause 13.6(h));

(vii) if you are unsure on what basis to transfer Personal Information outside the RSA or whether you are allowed to Process Personal Information obtained from the EEA (see clause 15);

(viii) if you need any assistance dealing with any rights invoked by a Data Subject (see clause 14);

(ix) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see clause 18) or plan to use Personal Data for purposes others than what it was collected for;

(x) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see clause 19);

(xi) if you need help complying with applicable law when carrying out direct marketing activities (see clause 17); or

(xii) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see clause 16).

5. GENERAL PERSONNEL GUIDELINES

5.1 The only persons able to access Data covered by this policy should be those who need it for their work.

5.2 Data should **not be shared informally**. When access to Confidential Information is required, Personnel can request it from their line managers.

5.3 INCON HEALTH will provide **training** to all Personnel to help them understand their responsibilities when handling data.

5.4 Personnel should keep all **data secure**, by taking sensible precautions and following the guidelines below.

5.5 In particular, **strong passwords** must be used and must not be shared.

5.6 Personal Information should **not be disclosed to unauthorised people**, whether internally at INCON HEALTH or externally. When shared externally an agreement with reference to the relevant data protection conditions should be agreed to by the external third party (see clause 16 below)

5.7 Data should be regularly **reviewed and updated** when it is found to be outdated. When no longer required, it should be **deleted and disposed** of.

5.8 Personnel should request help from their line manager or the Information Officer if they are unsure about any aspect of data protection.

6. DATA PROTECTION CONDITIONS / PRINCIPLES

Anyone processing Personal Information must comply with the eight enforceable conditions of good practice. The eight conditions are as follow, setting out the method in which and basis on which Personal Information must be processed:

(a) **Accountability** - Processed fairly and lawfully.

(b) **Processing Limitation** - Processed for limited purposes and in an appropriate way.

(c) **Purpose specific** - Adequate, relevant and not excessive for the purpose.

(d) **Further Processing limitation** – the processing of Personal Information outside the initial (original) reason is strictly limited.

(e) **Information Quality** – all Personal Information held must be accurate, complete and kept up to date

(f) **Openness** – all Processing must be done in light of the Data Subjects rights.

(g) **Security Safeguards** – all Processing must be executed in line with our Data Protection Policy.

(h) **Data Subject Participation** – the Data Subject is entitled to participate in the Processing of his/her/its Personal Information.

7. ACCOUNTABILITY (FAIR AND LAWFUL PROCESSING)

7.1 The Act is not intended to prevent the Processing of Personal Information, but to ensure that it is done lawfully, fairly and in a transparent manner without adversely affecting the rights of the Data subject. The Act and GDPR restricts our actions regarding Personal Information to specified lawful purposes.

7.2 When Special Personal Information is being processed, additional conditions must be met. When Processing Personal Information as Responsible Parties in the course of our business, we shall ensure that those requirements are met.

8. PROCESSING LIMITATION

8.1 In the course of our business, we may Process Personal Information. This may include Data we receive directly from a Data Subject (for example, by completing forms or by corresponding with us by mail, phone, e-mail or otherwise) and Data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

8.2 Personal Information can only be processed on one of the following legal grounds set out in the Act. These include, among other things: -

(a) the Data Subject's **Consent** to the processing, or

(b) that the Processing is **necessary to carry out actions for the conclusion or performance of a contract** to which the Data Subject is party,

(c) for the **compliance with a legal obligation** to which INCON HEALTH is subject to, or

(d) Processing **protects a legitimate interest of the Data Subject**;

(e) for **the legitimate interest of INCON HEALTH or other Responsible Parties** that INCON HEALTH may contract with or the party to whom the Data is disclosed.

8.3 You must identify and document the legal ground being relied on for each Processing activity.

8.4 Where a Data Subject has given his/her Consent we have the responsibility to record the Consent and be able to present such proof when required;

8.5 A Data Subject may withdraw his/her/its Consent to Processing at any time – You must establish the reason for said withdrawal, where reasonably possible;

8.6 We shall only process Personal Information for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the Act. We shall notify

those purposes to the Data Subject when we first collect the data or as soon as possible thereafter.

8.7 Personal Information must be collected directly from the Data Subject, except where: -

(a) the information is contained in or **derived from a public record** or has deliberately been **made public by the Data Subject**;

(b) the Data subject has **Consent** to the collection from another source;

(c) collection of the information from another source would **not prejudice a legitimate interest of the Data Subject**.

(d) compliance would prejudice a lawful purpose of the collection; or

(e) compliance is not reasonably practicable in the circumstances of the particular case.

8.8 **Object against Processing**

(a) A Data Subject may object, at any time, to the Processing of Personal Information: -

(i) in terms of paragraphs 8.2(d) and 8.2(e), above, in the prescribed manner (PAI Manual), on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

(ii) for purposes of direct marketing other than direct marketing as stated under paragraph 17 below.

(b) All objections must be dealt with on an urgent basis and directed to the Information Officer.

(c) Subsequent to receipt of an objection and removal of the Data Subject's Personal Information, we shall no longer be allowed to Process the Data Subject's Personal Information.

(d) Consent may need to be refreshed if you intend to Process Personal Information of the particular Data Subject for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

~~9. PURPOSE SPECIFIC~~

9.1 If we collect Personal Information directly from Data Subjects, we shall inform them about:

(a) The **purpose or purposes** for which INCON HEALTH intend to process the Personal Information.

(b) The types of third parties, if any, with which we shall share or to which we shall **disclose** that Personal Information.

(c) The means, if any, with which Data Subjects can **limit our use and disclosure** of their Personal Information or exercise their rights.

9.2 If we receive Personal Information about a Data Subject from other sources, we shall provide the Data Subject with this information as soon as possible thereafter.

9.3 We shall also inform Data Subjects whose Personal Information we Process that we are the Responsible Parties with regard to that Data, and who the Information Officer is.

9.4 Where we process Personal Information on behalf of a third party (acting as the Responsible Party) we shall confirm in writing to the third party that INCON HEALTH will act as Operator only. This must be stated and agreed to in writing between INCON

HEALTH and the third party before we start the processing of Personal Information on their behalf.

9.5 To these ends, INCON HEALTH has a Privacy Policy, setting out how data relating to Data Subjects is used by INCON HEALTH. This is available on request. A version of this Privacy Policy is also available on INCON HEALTH's website.

9.6 **Retention**: We shall not keep Personal Information longer than is necessary for the purpose/s for which they were collected unless: -

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

(b) the responsible party 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 has consented to the retention of the record.

9.7 We shall take all reasonable steps to destroy, or erase from our systems, all Data which is no longer required in a manner that prevents its reconstruction in an intelligible form.

10.1 We shall not Process Personal Information for any other purpose as originally stated to the Data Subject, unless: -

(a) the Data Subject consents thereto;

(b) the information is available from public records or has been made available to the public by the Data Subject;

(c) it is required in order to comply with the law; or

(d) the information is used for historical, statistical or research purposes, subject to de-identification of the Personal Information.

11. INFORMATION QUALITY

11.1

We shall ensure that all Personal Information held by us is accurate, complete and kep up to date. We shall check the accuracy of any Personal Information at the point of collection and at regular intervals afterwards. We shall take all reasonable steps to amend or destroy inaccurate or out-of-date data.

11.2 The law requires INCON HEALTH to take reasonable steps to ensure Data is kept accurate and up to date.

11.3 The more important it is that the Personal Information is accurate, the greater the effort INCON HEALTH should put into ensuring its accuracy.

11.4 All Data Users who work that Data has the responsibility to take reasonable steps to ensure it is kept as accurate and up to date as possible. The following shall apply:

(a) Data will be held in as few places as necessary. Personnel may not create any unnecessary additional data sets.

(b) Personnel should take every opportunity to ensure Data is updated. For instance, by confirming a client's details when they call.

(c) INCON HEALTH shall enable Data Subjects to easily update their information, as held by INCON HEALTH. For instance, via the company website or contact details on its Privacy Policy. The Data Subject has a right to rectify inaccurate Data or to be able to complete incomplete Data we may host.

9.8 We shall only collect Personal

Information to the extent that it is required for the specific purpose notified to the Data Subject.

10. FURTHER PROCESSING LIMITATION

(d) Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

(e) It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every 6 (six) months.

12. OPENNESS

12.1 We shall process all Personal Information in line with Data Subjects' rights, in particular their right to:

(a) Request access to any Data held about them by Responsible Parties (see also clause 14).

(b) Prevent the processing of their Data for direct-marketing purposes, unless Data Subject has consented thereto.

(c) Ask to have inaccurate Data amended.

(d) Prevent Processing that is likely to cause damage or distress to themselves or anyone else.

12.2 On our website we shall make available INCON HEALTH's section 51 Promotion of Access to Information Act (PAI Act) Manual. The Manual will enable Data Subjects to understand what information INCON HEALTH may process and which process to follow to participate and request information from INCON HEALTH.

12.3 The INCON HEALTH Privacy Policy shall be presented to all Data Subjects where INCON HEALTH collects Personal Information as a Responsible Party (Controller for purposes of GDPR). INCON HEALTH shall further indicate:

(a) the full name and address of INCON HEALTH;

(b) whether or not the supply of the information by that Data Subject is voluntary or mandatory; and

(c) any particular law authorising or requiring the collection of the information.

13. SECURITY SAFEGUARDS

13.1 We shall process all Personal Information we hold in accordance with our Data Protection Policy.

13.2 We shall put in place procedures and technologies to maintain the security of all Personal Information from the point of collection to the point of destruction. Due regard will be given to generally accepted information security practices and procedures in INCON HEALTH's specific industry.

13.3 We shall take reasonable steps to: -

(a) identify all reasonably foreseeable internal and external risks to Personal Information in our possession or under our control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

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

13.4 Personal information will only be transferred to an Operator and processed accordingly if: -

(a) There is a written contract between INCON HEALTH and the Operator, addressing the security safeguards of Personal Information;

(b) Operator process information only with the knowledge or authorisation of INCON HEALTH;

(c) Operators agrees to treat Personal Information as confidential and will not disclose it to any third party, unless required by law;

(d) The Operator agrees to comply with the policies and procedures as set out under this Policy, or that it puts in place adequate measure as set out under 13.3 above; or

(e) The Operator immediately notifies INCON HEALTH where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised Person.

13.5 We shall maintain data security by protecting the confidentiality, integrity and availability of the Personal Information, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that Personal Information should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the Data if they need it for authorised purposes.

13.6 Security procedures include:

(a) **Entry controls.** Any stranger or unauthorised Personnel seen in entrycontrolled areas must be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold Confidential Information of any kind. (Personal Information is always considered confidential.)

(c) Employees should make sure **paper and printouts** are not left where unauthorised people could see them, e.g. on a printer or copier or openly on your desk when not working therewith, irrespective of whether you are at your desk or not.

(d) **Transfer of electronic Data:** Personal Information must be **encrypted when being transferred electronically and/or sent via a secure online facility**.

(e) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be formatted and where they are no longer required, they should be physically destroyed.

(f) **Equipment.**

(i) Data Users must ensure that individual monitors do not show Confidential Information to passers-by and that they log off from their PC when it is left unattended or that the screens are locked.

(ii) Security will take priority during the review of new equipment and the implementation of it.

(g) When **data is stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

(i) Data should be protected by strong passwords that are changed regularly and never shared with others, including your colleagues.

(ii) If data is stored on removable media (like a CD, DVD or flash disk), these should be kept securely locked away when not being used.

(iii) Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service**.

(iv) Servers containing Personal Information should be sited in a secure location, away from general office space.

(v) Data should be backed up frequently. Those backups should be tested regularly, in line with INCON HEALTH's standard backup procedures.

(vi) Confidential Information should never be saved directly to laptops or other mobile devices like tablets or smart phones but stored on INCON HEALTH's central computer system.

All servers and computers containing Data should be protected by approved security software and a firewall.

(h) **Notification of security compromise / Data breach**:

Where there are reasonable grounds to believe that Personal Information has been accessed or acquired by any unauthorised party, do not attempt to investigate the matter yourself. Immediately report the incident to compliance@incon.co.za and follow the Incident Response Policy and Procedures. You should preserve all evidence relating to the potential Personal Information Breach.

14. DATA SUBJECT PARTICIPATION

14.1 All Data Subjects who are the subject of Personal Information held by INCON HEALTH are entitled to:

(a) Ask what information the company holds about them and why.

(b) Ask how to gain access to it.

(c) Be informed how to keep it up to date.

(d) Be informed how the company is meeting its data protection obligations.

14.2 Should an individual contact the company requesting the above information, it is called a **Data Subject access request**.

14.3 Data Subjects must make a formal request for information held by us about them. This must be made in writing and in accordance with INCON HEALTH's Promotion of Access to Information Manual. The preferred method of submitting said request is on the prescribed form (see manual) and to the Information Officer's email address: compliance@incon.co.za. Employees who receive a written request should forward it to their line manager or the Information Officer immediately.

14.4 When receiving telephone enquiries, we shall only disclose Personal Information we hold on our systems if the following conditions are met:

(a) The caller's identity must be checked and confirm to ensure that information is only given to a Person who is entitled to it; and

(b) Where there is uncertainty as to the caller's identity and their identity cannot be confirmed, we shall suggest that the caller put their request in writing. Reference should also be made to INCON HEALTH's Promotion of Access to Information Manual available on the INCON HEALTH's website. A copy of the manual is also available from the Office of the Information Officer.

14.5 Data Subjects will be charged a prescribed fee (see manual) per Data Subject access request. INCON HEALTH will aim to provide the relevant data within the prescribed number of days (see manual).

14.6 In difficult situations our Personnel will refer the request to their line manager or the Information Officer for assistance. Personnel may not be bullied into disclosing

Personal Information. Any attempts at such bullying must be reported to your line manager and the Information Officer.

14.7 Before handing over any information, the Information Officer or line manager must always verify the identity of anyone making a Data Subject access request.

14.8 In addition to the above and where applicable, European Data Subjects are entitled, under the GDPR, to the right to:

(a) receive certain information about the Data Controller's Processing activities;

(b) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed;

(c) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(d) request a copy of an agreement under which Personal Data is transferred outside of the European Economic Area ("EEA");

(e) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(f) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; and

(g) make a complaint to the supervisory authority.

15. CROSS BORDER TRANSFER OF PERSONAL INFORMATION

15.1 We may not transfer/ transmit/ send Personal Information about a Data Subject to a third party who is in a foreign country or allow Personnel operating outside RSA borders (working for us or our suppliers) to process Personal information, unless: - (a)

the Data Subject has given his/her/its consent (preferred option);

(b) the third party who is the recipient of the Personal Information is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection similar to the Act;

(c) the transfer is necessary for the performance of a contract between the Data Subject and INCON HEALTH, or for the implementation of precontractual measures taken in response to the Data Subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between INCON HEALTH and a third party;

(e) the transfer is for the benefit of the Data Subject, and (i) it is not reasonably practicable to obtain the consent of the Data Subject to that transfer and (ii) if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give it; or

(f) the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

15.2 (Where applicable) Where we occasionally process Personal Information of Data Subjects that reside in any of the EU member states, we may only transfer said Personal Information outside the EEA if one of the following conditions applies:

(a) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks;

(b) the transfer is necessary for one of the other reasons set out in the GDPR *including* the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is

physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest;

(c) the European Commission has issued a decision confirming that the country to which we transfer the Personal Information/Data ensures an adequate level of protection for the Data Subject's rights and freedoms; or

(d) appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism.

16. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

16.1

We may share Personal Information we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in the Companies Act 2008.

16.2 We may also disclose Personal Information we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose Personal Information we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case Personal Information we hold will be one of the transferred assets.

(c) If we are under a duty to disclose or share a Data Subject's Personal Information in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our Personnel, clients, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

(d) We may also share Personal Information we hold with selected third parties for the purposes set out in the Schedule, below.

16.3 We may also share Personal Information with third party service providers. Where Personal Information is shared with third party service providers the following shall apply: -

(a) No Personal Information shall be shared with any third party prior to the third party signing the INCON HEALTH standard processing of Personal Information Agreement;

(b) The Processing of Personal Information Agreement shall refer to all relevant conditions/principles under the applicable data protection legislation;

(c) Where required (depending on the sensitivity of the personal information) an assessment of the third party technological and organisational measurements shall be done prior to making available any Personal Information to the third party. This is especially critical as medical ("health") information, which forms the basis of our services, are considered to be Special Personal Information with a higher level of responsibility attached thereto.

17. DIRECT MARKETING

17.1 We may only use Personal Information for purposes of direct marketing (by means of any form of electronic communication, including automatic calling machines, SMSs or e-mail) where the Data Subject: -

(a) has Consented to the use of his/her/its Personal information for direct marketing purposes; or

(b) is a client or clients' employee of INCON HEALTH, the contact details have been obtained in the course of providing services to that Data Subject and the direct marketing relates to services and/or products similar to the services and/or products that the Data Subject is or has received from INCON HEALTH or any of the INCON HEALTH's group companies;

17.2 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

17.3 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

17.4 The Data Subject may at any time withdraw its consent for purposes of direct marketing or request you to refrain from further direct marketing activities;

17.5 You must comply with the INCON HEALTH's policy or guidelines on direct marketing to clients or clients' employees as applicable from time to time.

18. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

18.1 We are required to implement Privacy by Design measures when Processing Personal Information by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner and by doing so ensuring compliance with the data privacy conditions (principles).

18.2 We must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Information by taking the following into account:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity to the rights and freedoms of Data Subjects as posed by the Processing.

18.3 INCON HEALTH must also conduct a DPIA in respect to high risk Processing.

18.4 A DPIA (which must be overseen by the Information Officer) must also be conducted when implementing major system or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) Automated Processing including profiling and Automated Decision-Making ("ADM");

(c) large scale Processing of Special Personal Information; and (d) large scale, systematic monitoring of a publicly accessible area.

18.5 A DPIA must include:

(a) a description of the Processing, its purposes and INCON HEALTH's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

18.6 A Data Protection audit shall be conducted on an annual basis to determine the effectiveness of the INCON HEALTH's Data Protection workability of this policy.

19. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING (“ADM”)

19.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has given Explicit Consent;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

19.2 If certain types of Special Personal Information are being processed, then grounds (b) or (c) will not be allowed but such Special Personal Information can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

19.3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subject must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights, freedoms and legitimate interests.

19.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

19.5 A Data Subject may object to decisions based solely on Automated Processing, including profiling.

19.6 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

19.7

Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with the Company's guidelines on profiling and ADM.

20. DATA PORTABILITY

20.1

A Data Subject has the right to request his/her/its Personal information from INCON HEALTH in a format that is structured, commonly used and machine readable for transfer to the Data Subject or any third party at any time;

20.2 Data Portability should always form part of the functional specification during any Privacy by Design process;

20.3 If a Data Portability function is not available to the Data subject, a request for a Data Subject’s Data to be made available must be directed to the Information Officer.

21. RIGHT TO BE FORGOTTEN (RIGHT TO ERASURE)

21.1 Data Subjects have the right to have their Personal Information erased if:

(a) the Personal Information is no longer necessary for the purpose for which it was originally collected or processed ;

(b) we are relying on Consent as our lawful basis for holding the information, and the Data Subject withdraws (in a similar manner as obtaining the Consent) his/her/its Consent;

(c) we are relying on legitimate interests as our basis for Processing, the Data Subject objects to the processing of their information, and there is no overriding legitimate interest to continue this processing;

(d) we are Processing the Personal Information for direct marketing purposes and the individual objects to that Processing;

(e) we are required to do it in order to comply with a legal obligation.

21.2 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such Data, where applicable.

21.3 Caution must be had at destroying information relating to direct marketing. Rather than deleting a Data Subject's details entirely, it is advisable to suppress the Data. Suppression involves retaining just enough information to ensure the Data Subject's preferences are respected in the future. Suppression will allow us to ensure that we do not send marketing communication to Data Subjects who have opted-out, as we shall have a record against which to screen marketing lists.

21.4 You will ensure Data Subjects are informed, in any applicable Privacy Policy, of the period for which Data is stored and how that period is determined.

22. RECORD KEEPING

22.1 We shall keep full and accurate records of all our data Processing activities.

22.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Company's record keeping guidelines.

22.3

These records should include, at a minimum:

(a) the name and contact details of the Responsible Party and the Information Officer;

(b) clear descriptions of the Personal Information types;

(c) Data Subject types;

(d) Processing activities;

(e) Processing purposes;

(f) Third-party recipients of the Personal Information;

(g) Personal Information storage locations;

(h) Personal Information transfers;

(i) The Personal Information's retention period; and (j) a description of the security measures in place.

In order to create such records, data maps should be created. The data maps should include the details set out above together with appropriate data flows.

23. TRAINING AND AWARENESS

23.1 All INCON HEALTH Personnel will be provided with data protection awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards.

23.2 An appropriate summary of the data protection policy or INCON HEALTH's requirements in terms of information security and data protection must be formally delivered to any contractors, prior to any supply of services.

23.3 INCON HEALTH is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise data protection and information security.

23.4 Periodic training for the Information Officer, to educate and train in the latest development, threats and data protection techniques, is to be prioritised.

24. AUDIT

24.1 You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Information.

24.2 A compliance audit shall be executed by our attorneys (Data Protection division) once per annum to ensure we are compliant with the applicable data protection legislation.

24.3 An IT Security assessment shall be executed by a third-party IT Security service provider once per annum to ensure that we maintain appropriate technological measurements to safeguard all Personal information.

25. BREACH OR VIOLATION

Any failure and/ or refusal to comply with the provisions of this Policy will result in disciplinary action which may include dismissal or liability for damages.

26. REVIEW OF POLICY

26.1 This policy shall be reviewed annually by a review committee comprising the Information Officer, IT Manager, Legal Advisor and QMS Manager.

26.2 We reserve the right to change this policy at any time. Where appropriate, we shall notify Data Subjects of those changes by mail or e-mail.