etadi
WELLNESS CENTRE
love yourself, value yourself

Subject: Your compliance with the Protection of Personal Information Act, 2013 (POPI Act)

As a responsible, forward looking business, ETADI recognise at senior levels the need to comply with the POPI Act and, as a responsible party, has taken steps to ensure that effective measures are in place to protect the personal information of our CLIENTS/PASIENTS, employees and other stakeholders, and to ensure that it is processed lawfully, reasonable and transparently.

Your organisation acts as an operator on our behalf for some of the personal information we are a responsible party and, as part of meeting our mutual legal obligations, we are required to have in placed an operator agreement (or similar contractual arrangement) with you.

With respect to the processing of personal information you perform on our behalf, this agreement is required to cover:

a) The subject matter and duration of the agreement
b) The nature and purpose of the processing
c) The type of personal information and categories of data subjects
d) Required contractual terms.

If we are nor already, we will be working with you to ensure that such an agreement is in place and that both parties' legal responsibilities are fulfilled.

Further to this agreement, we would like to confirm with you that:

a) A policy is in place for the protection of personal information within your organisation which has been approved by management and communicated to all employees and other relevant people.
b) All your employees have received awareness training regarding the protection of personal information and the POPI Act.
c) Everyone in your organisation understands their roles in the protection of personal information and has received training where needed.
d) Tested procedures and, if appropriate, online user facilities are in place to assist us in promptly processing and fulfilling data subject access request, such as consent withdrawal, access and correction of information.
e) Procedures and facilities are in place to comply with our published timescales for the retention of personal information and for the deletion or return of data at the end of the contract.
f) You are keeping records of processing as required by the POPI Act (section 17)
g) Where you are using agreed sub-operators, all your contracts with these parties have been updated to comply with the requirements of the POPI Act.
h) All your employees are subject to confidentiality obligations with respect to personal information.
i) Where appropriate, a personal information impact assessment approach which is in line with the requirements and recommendations of the POPI Act and relevant best practices, will be used.

j) You have tested procedures in place to fulfil your obligations to us as a responsible party, in the event of a breach (security incident) of personal information.

k) You have policies and other controls in place to provide appropriate protection of our personal information, based on a careful assessment of risk.

l) You have appointed an Information Officer whose contact details have been provide to us.

Please respond to each of the above points, stating clearly whether they are in place, and describing your plans, including timescales, where they are not.

We trust that you will continue to develop and improve your protection of personal information policies and controls over time, guided both by legal requirements and the needs and preferences of ourselves as a customer.

We appreciate your cooperation in this matter.

Your sincerely

etadi
WELLNESS CENTRE
love yourself, value yourself

1. ***CONFIDENTIAL INFORMATION***

1.1. Any information, including but without limiting the foregoing, any and all information relating to **ETADI WELLNESS CENTRE** (hereinafter referred to as the Organisation) including Personal Information of its clients/patients, or otherwise proprietary to **Organisation** issued to, used by or disclosed to or developed by Seven Lemons hereinafter referred to as the Supplier) in connection with the performance of the Agreement are confidential ("Confidential Information").

1.2. **Supplier** shall not, without the prior written consent of the **Organisation**, disclose **Organisation** Personal Information to any person or entity except to its employees who require same in connection with performing **Supplier** obligations under this Agreement, and who agree to act in compliance with the confidentiality obligations set out in this Agreement and **Supplier** Privacy Code.

1.3. On completion or termination of this Agreement for any reason, **Supplier** shall forthwith return to the **Organisation** all the Personal Information either obtained or developed in the course of this Agreement. **Supplier** obligations with respect to Personal Information shall survive the expiration or other termination of this Agreement for any reason.

2. ***PROTECTION OF PERSONAL INFORMATION***

General

a. In addition to Article 1 above, which applies to Personal Information generally, there are additional obligations required with respect to Personal Health AND BEAUTY Information as set out below which the Parties shall comply with.

b. The parties acknowledge that this Agreement is intended in good faith to meet the requirements set out in all applicable legislation and regulations dealing with the protection of Personal Information and acknowledge that they shall work together to ensure that any new privacy legislation introduced, shall be complied with.

c. The **Supplier** and the **Organisation** shall be responsible for ensuring compliance with the provisions of this Agreement for the Protection of Personal Information.

The **Organisation** acknowledges that it is aware of the current rules governing the confidentiality of personal information pursuant to applicable legislation and regulations there under. The **Organisation** further acknowledges that its obligations under such legislation and regulations are not obviated by entering into this Agreement and engaging the services of **Organisation**.

The Supplier

a. Shall fulfil the same confidentiality obligations that apply to the **Organisation** in respect of **Supplier's** provision of Services under the Agreement.

b. Shall be entitled to use the Personal Information provided by the **Organisation** solely for purposes of providing the Services and for no other purpose whatsoever.

c. Shall ensure that its employees are aware of and agree in writing to be bound by the confidentiality provisions that are set out in this Agreement.

d. A breach of the confidentiality provisions by any of employees of **the Supplier** shall be grounds for immediate dismissal. Neither **the Supplier** nor its employees shall provide access to or use, disclose or dispose of any Personal Information except in accordance with the provisions of this Agreement.

Confidentiality Safeguards

a. In order to safeguard the confidentiality of the Personal Information that are transferred by the **Organisation** to **the Supplier**, the following procedures shall be followed:
b. Transfer of Personal Information: All original personal information shall remain at the **Organisation.**
c. The **Organisation** shall ensure that it limits its transfer of Personal Information to **the Supplier** to that which is necessary for the provision of Services under this Agreement.
d. The parties commit to safeguarding the confidentiality of the Personal Information through jointly approving the processes to be used to transfer **Organisation** data to **the Supplier** and back to **the Organisation.**
e. **The Supplier** shall destroy the Personal Information confidentially in a manner agreed to by the parties or return it to the **Organisation** within insert days of the completion of the Services on the information.
f. No Personal Information shall be retained by **the Supplier**.

Access to Data

The **Supplier** shall institute confidentiality policies, procedures and protocols as set out in its Privacy Policy, that protect against the disclosure of information to people who are not authorized to have that information.

Misuse of Data

a. **The Supplier** shall institute auditing mechanisms that are used to detect unauthorized access or attempts to access Personal Information after they have taken place and monitoring systems so that such unauthorized access or attempts to access Personal Information can be recognized while they are occurring.
b. In the event that **the Supplier** becomes aware that a person has obtained access to Personal Information other than in accordance with this Agreement or **the Supplier** has used, disclosed or disposed of the Personal Information other than in accordance with the Agreement, **the Supplier** shall immediately notify the **Organisation** and meet all requirements prescribed by law.

Quality Control of Compliance with Confidentiality Requirements

a. **The Supplier** shall perform audits and undertake monitoring activities to assist in ensuring that the confidentiality provisions of this Agreement are being followed by its employees.
b. The **Organisation** may, upon reasonable notice, assess and review the **Supplier**'s procedures for receiving and processing Personal Information under this Agreement, for the purposes of ensuring that the confidentiality provisions of this Agreement are being complied with. For these purposes, **the Supplier** shall provide the **Organisation** with reasonable access to the policies, procedures and protocols used for purposes of providing the Services and any documents, which may be relevant.
c. In the event that the **Organisation** makes a formal complaint to **the Supplier** in respect of its compliance with the confidentiality provisions of this Agreement, **the Supplier** shall, within 2 Business Days of receipt of the complaint,

investigate the matter and provide the **Organisation** with an oral report stating the cause of the deficiency, if any, and the steps taken to prevent a recurrence, if required. Within a further 3 Business Days, **the Supplier** shall provide the **Organisation** with a written report documenting the complaint, investigation, deficiency, if any, and the steps taken to prevent a recurrence, if required.

etadi
WELLNESS CENTRE
love yourself, value yourself

Third Party (Operator) Name: Seven Romans		Return Complete: 15 August 2021
Question	YES/NO/NA	REMARKS/RESPONSE
1. Do you have a formally appointed information officer? If so, please provide the name and contact information of both officers.		
2. Is your information security program based on an industry accepted framework? If so, what framework did you choose?		
3. Do you have formal information security policies and procedures? If so, please provide an equivalent copy for the following: • Information Security Management • Information Access Management (i.e. physical and electronic) • Auditing & Monitoring Access • Physical Security/Facility Security • Incident (security) Management • Breach Management/Notification • Security Awareness & Training (i.e. for end-users, privileged users, IT administrators and management) • System Security Administration • Information Classification and Handling • Mobile Device & Portable Media Security • Business Continuity Plan/Disaster Recovery Plan • Risk Management • Asset Management & Disposal • Sanction Policy • Change Management		
4. Do you have a formal disaster recovery plan? If so, please provide a copy of the plan?		

5. When was the last time you performed a disaster recovery exercise, what was the scenario and what was the results of the exercise?		
6. Have you implemented encryption on all mobile devices and media in which protected health information is stored?		
7. Have you implemented encryption for all transmission of sensitive/confidential information outside of your organization's network?		
8. Do you anticipate disclosing ETADI's personal information to a sub-contractor? If so, are they outside of the RSA? Do you have a signed operator's agreement with them? Please provide organization name(s) and contact information.		
9. Have you performed an information security risk assessment within the last year? If so, was this an internal self-assessment or performed by a 3rd party? Please provide a summary copy of this risk assessment, including findings and corrective action taken or still being remediated. NOTE: If performed by 3rd party, please provide contact information of assessor in addition to an attestation letter.		
10. Has your datacenter undergone a formal audit within the last year? If so, please provide a summary of the audit and results, to include findings and corrective action that still needs to be remediated.		
11. When was the last time your organization performed an internal/external technical vulnerability assessment? Was the assessment performed internally or by a 3rd party? Please provide a summary of the assessment and un-remediated corrective actions.		
12. Has your organization experienced any reportable breaches of personal/special personal information in the last two years? If		

etadi
WELLNESS CENTRE
love yourself, value yourself

so, provide a summary of the breach and corrective actions taken.		
13. Describe how often and what type of training you provide your employees.		

All NO or NA (not applicable) responses requires an explanation in the Remarks/Response column. Failure to fully complete this document or return this document by the deadline may result delay doing business with, or void your contract with ETADI WELLNESS CENTRE.

NAME/TITLE/SIGNATURE OF PERSON COMPLETING FORM

PHONE NUMBER/EMAIL ADDRESS OF PERSON COMPLETING FORM