



Premium Support Services Australia Pty Ltd - Confidentiality Agreement

Between Premium Support Services Australia Pty Ltd and the Customer/Practice Owner/Practice Manager

Regarding the handling of Patient Clinical Information and any sensitive business related information that we come across in the performance of our duties to support the business.

This Confidentiality Agreement ("Agreement") is entered into on [Insert Date], between:

Premium Support Services Australia Pty Ltd ("Service Provider"), a company providing IT services, with its principal place of business at 1/20A Gavegan Street, BUNDABERG NORTH, Queensland 4670 ; and

[Customer/Practice Owner/Practice Manager Name – insert name here] ("Customer"), representing [Insert Practice Name Here], located at [Insert Address].

1. Purpose

This Agreement governs the handling of Patient Clinical Information and any Sensitive Business Related Information that we come by, as a Service Provider, in the course of providing Managed Services or As Needs Support to the Customer, ensuring compliance with Australian Privacy Laws, including the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). The Service Provider acknowledges the sensitive nature of Patient Clinical Information as well as Sensitive Business Related Information, and agrees to protect its confidentiality and privacy.

2. Definitions

a. Patient Clinical Information: Refers to any personal information, including health information, as defined under the Privacy Act 1988 (Cth), that identifies or can be used to identify a patient, such as medical records, treatment plans, diagnoses, or other health-related data.

b. Sensitive Business Related Information includes confidential data like trade secrets, financial records, customer details, strategic plans, and proprietary technology. This is also covered under the Privacy Act 1988 (Cth), and protection

under privacy laws to prevent unauthorized access, disclosure, or misuse, which could lead to financial loss or reputational damage.

c. Australian Privacy Laws: Includes the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and any relevant state or territory legislation governing health records, such as the Health Records (Privacy and Access) Act 1997 (ACT) or the Information Act (NT).

d. Confidential Information: Encompasses Patient Clinical Information and any other information provided by the Customer to the Service Provider in confidence, which is not publicly available.

3. Obligations of the Service Provider

a. Compliance with Australian Privacy Laws: The Service Provider agrees to handle Patient Clinical Information in strict compliance with the Privacy Act 1988 (Cth) and the APPs, ensuring that such information is only collected, used, disclosed, or stored as permitted under these laws.

b. Confidentiality: The Service Provider shall:

i. Not use or disclose Patient Clinical Information for any purpose other than the primary purpose of providing IT services to the Customer, unless expressly authorized by the Customer or required by law.

ii. Ensure that Patient Clinical Information is not disclosed to third parties without the Customer's prior written consent, except where such disclosure is permitted under the APPs (e.g., for a directly related secondary purpose within the patient's reasonable expectations).

iii. Take reasonable steps to protect Patient Clinical Information from misuse, interference, loss, unauthorized access, modification, or disclosure, including implementing appropriate technical and organizational security measures (e.g., encryption, access controls).

c. Access Restrictions: The Service Provider shall ensure that only authorized personnel, who have signed confidentiality agreements and are trained in privacy obligations, have access to Patient Clinical Information, and only to the extent necessary to perform their duties.

d. Cross-Border Disclosure: If Patient Clinical Information is to be disclosed to an overseas recipient, the Service Provider must take reasonable steps to ensure the recipient complies with the APPs, as required by APP 8, and remains accountable for any breaches by the recipient.

e. De-Identification: Where possible, the Service Provider shall de-identify Patient Clinical Information before using it for purposes such as system testing, staff training, or quality assurance, ensuring that individual identities are not revealed.

4. Obligations of the Customer

a. The Customer shall ensure that patients have been informed of, or have consented to, the sharing of their Patient Clinical Information with the Service Provider for the purpose of IT service provision, where required under Australian Privacy Laws.

b. The Customer shall provide the Service Provider with only the minimum amount of Patient Clinical Information necessary to fulfill the agreed services.

5. Permitted Use and Disclosure

a. The Service Provider may use or disclose Patient Clinical Information:

i. For the primary purpose of providing IT services to the Customer, such as system maintenance, data recovery, or cybersecurity support.

ii. For a secondary purpose directly related to the primary purpose, only if within the reasonable expectations of the patient (e.g., troubleshooting a system issue affecting patient records).

iii. Where required or authorized by Australian law, such as under a court order or mandatory reporting obligation.

b. The Service Provider must notify the Customer immediately if a disclosure is made under clause 5(a)(iii) and provide details of the disclosure.

6. Data Breach Notification

a. In the event of a suspected or actual data breach involving Patient Clinical Information, the Service Provider shall:

i. Notify the Customer within 24 hours of becoming aware of the breach.

ii. Cooperate fully with the Customer to assess the breach and comply with the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act 1988 (Cth), including notifying the Office of the Australian Information Commissioner (OAIC) and affected patients if required.

iii. Take immediate steps to contain and mitigate the breach.

b. The Service Provider shall not notify third parties, including the OAIC or patients, directly without the Customer's prior written consent, unless legally required to do so.

7. Return or Destruction of Information

Upon termination of services or at the Customer's request, the Service Provider shall return all Patient Clinical Information to the Customer or securely destroy it, ensuring no copies are retained, unless retention is required by law.

8. Term and Termination

a. This Agreement remains in effect for the duration of the Service Provider's engagement with the Customer and continues to apply to any Patient Clinical Information retained after termination.

b. Either party may terminate this Agreement with 30 days' written notice if the other party breaches its obligations under this Agreement and fails to remedy the breach within 14 days of notification.

9. Indemnity

The Service Provider agrees to indemnify the Customer against any loss, damage, or liability arising from the Service Provider's breach of this Agreement or Australian Privacy Laws, including legal costs or penalties imposed by the OAIC.

10. Governing Law

This Agreement is governed by the laws of [Insert State/Territory], Australia, and the parties submit to the non-exclusive jurisdiction of the courts of that state/territory.

11. Signatures

The parties acknowledge that they have read, understood, and agree to be bound by the terms of this Agreement.

Premium Support Services Australia Pty Ltd

Name: John Stacey

Title: CEO - Premium Support Services Australia Pty Ltd

Signature: _____

Date: [Insert Date]

Customer/Practice Owner/Practice Manager

Name: [Insert Name]

Title: [Insert Title]

Signature: _____

Date: [Insert Date]