WellBeing Space
MIND • GROWTH • CONNECTION

WellBeing Space - Data Breach Response Plan

Prepared by: Rebecca Evans, Psychologist
Date: 3rd November, 2025
Review Date: 3rd November, 2026

1. Purpose

This Data Breach Response Plan outlines the procedures for identifying, managing, and responding to data breaches involving personal, sensitive, or health information held by this practice. The plan ensures compliance with:
- The Privacy Act 1988 (Cth)
- The Australian Privacy Principles (APPs)
- The Notifiable Data Breaches (NDB) Scheme
- AHPRA record-keeping and confidentiality standards
- Professional codes of ethics, including the APS Code of Ethics.

2. Definition of a Data Breach

A data breach occurs when personal or sensitive information is lost, accessed, disclosed, or altered without authorisation. Examples include:
- Loss or theft of paper files or electronic devices
- Hacking, ransomware, or malware attacks
- Accidental disclosure (e.g., sending a report to the wrong client or GP)
- Unauthorised access by staff or third parties
- Physical intrusion into practice premises or storage areas

3. Guiding Principles

• Act promptly to contain and assess the breach.
• Prioritise client wellbeing and privacy.
• Meet all legal and ethical obligations.
• Maintain transparency and accountability.
• Document all actions taken.

4. Response Steps

Step 1: Identify and Contain

Immediately contain the breach to prevent further loss or unauthorised access.
Examples:
- Retrieve lost documents or devices if possible.
- Disable compromised accounts or network access.
- Suspend affected systems.
- Notify the Practice Director / Privacy Officer within 24 hours.

Step 2: Assess the Breach

Within 30 days, assess:
1. What information was involved.
2. How the breach occurred.
3. Who may have gained access.
4. Potential harm to individuals.
5. Whether the breach is likely to result in serious harm under the NDB Scheme.

Use the OAIC Data Breach Assessment Guide as reference.

Step 3: Notify

If the breach is likely to result in serious harm:
- Notify the OAIC via the Notifiable Data Breach form.
- Notify affected individuals as soon as practicable, including:
  - Description of the breach
  - What information was involved
  - Recommended steps they should take
  - Contact details for further information.

If uncertain whether notification is required, consult the OAIC or a legal advisor.

Step 4: Review and Prevent

After managing the incident:
- Conduct an internal review.
- Update policies, systems, and staff training.
- Improve security measures (passwords, encryption, access controls, backups).
- Document all actions in the Data Breach Register.

WellBeing Space
MIND • GROWTH • CONNECTION

5. Roles and Responsibilities

Role	Responsibility
Privacy Officer / Practice Director	Oversee data breach response, assess risk, notify OAIC and affected parties.
All Staff and Contractors	Immediately report suspected breaches. Follow containment instructions.
IT Support	Assist with system security, recovery, and forensic assessment.
Treating Psychologist	Support clients affected by breach; ensure accurate record documentation.

6. Record-Keeping

All suspected or actual breaches must be recorded in the Data Breach Register, including:
- Date and time detected
- Description of breach
- Information involved
- Containment actions
- Assessment outcome
- Notification decisions
- Follow-up actions

7. Staff Training

All staff will receive annual training covering:
- Privacy obligations and confidentiality
- Recognising and reporting data breaches
- Secure handling of health records (electronic and paper)

8. Review

This policy will be reviewed annually, or after any data breach incident, to ensure ongoing compliance with legislation and best practice.