MTHFRSUPPORT
Pioneers in Health. Science. Genetics.

Data Retention Policy

1. Purpose

The purpose of this policy is to establish guidelines and procedures for the retention, storage, and disposal of patient health records and other sensitive information for our business. This policy ensures compliance with Australian regulatory requirements for record keeping and protection of patient data.

2. Scope

This policy applies to all data, records, and information generated, processed, or stored by employees during the course of their work.

3. Data Categories

3.1 Patient Health Records

- Patient health records, including consultation notes, treatment plans, medical histories, and test results, will be retained as mandated by the Australian Health Records and Information Privacy Act 2002 (HRIP Act).

3.2 Administrative and Financial Records

- Administrative records, such as billing information, insurance claims, and financial transactions, will be retained for the periods specified by relevant Australian laws and regulations.

3.3 Employee Records

- Employee records, including contracts, training records, and performance evaluations, will be retained in accordance with Australian labor laws.

4. Data Retention Periods

4.1 Patient Health Records

- Patient health records will be retained for a minimum of 7 following the last patient interaction, as required by the HRIP Act.

4.2 Administrative and Financial Records

- Administrative and financial records will be retained for a minimum of 5 years as specified by applicable Australian laws.

4.3 Employee Records

- Employee records will be retained for a minimum of 7 years following the termination of the employee's contract, in accordance with Australian labor laws.

5. Data Storage and Protection

5.1 Electronic Records

- Electronic health records will be stored securely on authorised systems, servers, or cloud platforms as per the Access Control Policy.

5.2 Encryption

- Sensitive data stored electronically will be encrypted to prevent unauthorised access.

5.3 Physical Records

- Physical health and business records will be stored in locked, secure environments to prevent unauthorised access or damage.

6. Data Disposal

6.1 Data Lifecycle & Disposal

- At the end of the data retention period, patient information will be de-identified, all files will be removed from their patient file, and their patient record will be archived. d
- At the end of the data retention period, other data will be securely disposed of using methods that render it unreadable and unrecoverable.

6.2 Documentation of Disposal

- Records of data disposal, including date, method, and responsible personnel, will be maintained for audit and compliance purposes.

7. Legal and Regulatory Compliance

7.1 Compliance Monitoring

- The business will monitor changes in Australian privacy and record keeping regulations and update the policy accordingly.

8. Breach and Compliance

8.1 Breach

Any suspicion of a breach of this Policy must be reported immediately to the business owner. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

8.2 Compliance

- Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to the businesses reputation, personal injury, harm or loss.
- Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Company premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract.
- Such non-compliance may also lead to legal action against the parties involved in such activities.

9. Data and Personal Information Requests

- The business will only disclose patient personal information for the purpose or purposes of consultation with another practitioner or as otherwise permitted by law, and only with patient consent, unless mandated by a court order. This may include disclosure of information to doctors, insurance providers, other health professionals or legal officers.