Form Title	**Data Retention and Disposal Policy**			Form Number	BH-PO-CC-019-01
				Version Number	01-01
Effective Date	Apr-14-2026	Last Review Date	Apr-14-2026	Next Review Date	Apr-14-2027
Process Owner	Compassionate Care WA – Clinical Process and Compliance			Number of Pages	4

VERSION HISTORY

Version	Approved by	Revision Date	Description of Change	Author
1	Damian Thorp	Mar-31-2026	To establish the framework for data retention and disposal, guaranteeing that data is only retained for as long as is required.	LZP3

APPROVAL AND REVIEW

Process Owner:	Reviewed:	Approved:	I certify that the undersigned read and understand the details discussed in this policy. I acknowledge that adhering to standard practices is both required by the company and laws.
LEANDRO PERTIERRA III Clinical Process and Compliance Manager PRINT NAME | SIGNATURE | POSITION	DAMIAN THORP Chief Operating Officer PRINT NAME | SIGNATURE | POSITION	CATHERINE SUVA Director PRINT NAME | SIGNATURE | POSITION	PRINT NAME | SIGNATURE | POSITION
DATE:	DATE:	DATE:	DATE:

ADDITIONAL NOTES:

1. PURPOSE:

1.1. Sensitive and personal data protection is a top priority for Bluebird Homecare Pty. Ltd. To comply with the Privacy Act 1988 and other legal requirements, this policy establishes the framework for data retention and disposal, guaranteeing that data is only retained for as long as is required.

2. SCOPE AND LIMITATION:

2.1. Scope: All employees, contractors, and third-party providers who handle data for Bluebird Homecare Pty. Ltd. is subject to this policy. It includes all records, both electronic and physical, that include sensitive data, personal data, and commercial data.

2.2. Out of Scope: any information for which CCWA services are not responsible for ownership, collection, or retention. As stated in any collaboration agreements, this can apply to any external data ownership.

3. POLICY STATEMENT:

3.1. Establish broad guidelines to direct decisions about design and services.

3.2. Recognize the legal and policy standards that apply to the organization.

3.3. Provide guidelines on how to keep and discard customer-based data.

3.4. Describe factors that product teams should take into account to ensure that solutions allow for the appropriate evaluation of records for disposal or preservation.

4. DEFINITION OF TERMS

4.1. Classification of Data: categorizing data according to how sensitive it is and how much of an impact it might have in the event of a leak or loss.

Terms	Definition
Public	information that is freely accessible (e.g., marketing brochures).
Internal	information intended for employees but not extremely dangerous (e.g., company memos).
Sensitive or Confidential	data that needs to be protected, such as vendor contracts or corporate strategy
Restricted/Highly Sensitive	PHI (Protected Health Information) or PII (Personally Identifiable Information) that, if breached, carries severe legal repercussions.

4.2. Retention Period:

Retention Trigger	the precise amount of time that a record has to be kept, such as "7 years after contract expiration" or "3 years after employee departure".

4.3. Data: Active versus Inactive

Active Data	information that is kept on high-performance disks for easy access and is currently used for everyday operations.
Inactive Data	information that is essential for historical or legal purposes but is no longer needed for daily work. This is often moved to Archives or less expensive “cold storage.”

4.4. Litigation Hold (Legal Hold)

Legal Hold	a brief halt to the disposal procedure. Even if the data has passed its "Retention Period" expiration, an organization must halt any deletion of pertinent material when a lawsuit is filed or reasonably anticipated.

4.5. Data Destruction vs. Data Disposal

Disposal	the general process of eliminating data.
Destruction	is a specific, irreversible process that renders data unrecoverable. Example: Degaussing (demagnetizing) hard drives, shredding paper, and cryptographic erasure (removing the encryption key to leave the data permanently jumbled) are a few examples

5. RESPONSIBILITIES

5.1. Each of the following parties has specific assigned responsibilities under this policy:

Position	Responsibility
Management	responsible for the policy implementation
All employees	accountable for following disposal and storage protocols.

6. NDIS PRACTICE STANDARDS AND QUALITY INDICATORS:

6.1. Provider Governance and Operational Management, Page 9

6.1.1. Information Management

6.1.2. Outcome: Management of each participant's information ensures that it is identifiable, accurately recorded, current and confidential. Each participant's information is easily accessible to the participant and appropriately utilised by relevant workers.

6.1.3. To achieve this outcome, the following indicators should be demonstrated:

- Each participant's consent is obtained to collect, use and retain their information or to disclose their information (including assessments) to other parties, including details of the purpose of collection, use and disclosure. Each participant is informed in what circumstances the information could be disclosed, including that the information could be provided without their consent if required or authorised by law.
- Each participant is informed of how their information is stored and used, and when and how each participant can access or correct their information, and withdraw or amend their prior consent.
- An information management system is maintained that is relevant and proportionate to the size and scale of the organisation and records each participant's information in an accurate and timely manner.
- Documents are stored with appropriate use, access, transfer, storage, security, retrieval, retention, destruction and disposal

7. GUIDELINES:

7.1. A data retention policy is a formal set of rules that specify how long an organization keeps data, where it is kept, how it is safeguarded, and when it is safely deleted.

7.2. This policy ensures compliance with Australian legal responsibilities and operational requirements by defining the necessary retention periods for Bluebird Homecare Pty. Ltd. records and outlining the procedures for the secure destruction or archiving of data. It covers all records, including digital and hard copy.

7.3. **Essential components** of a strategy for data preservation

7.3.1. Establish clear policies that specify the duration of data retention, data management, and data protection.

7.3.2. Governance: Create procedures for accountability, audits, and access control.

7.3.3. Secure archiving and storage: Protect data using dependable and legal storage techniques.

7.4. **Fundamentals**

7.4.1. Purpose Limitation: No personal data will be retained for longer than is required to fulfill the purpose for which it was gathered.

7.4.2. Minimum Retention: When records are no longer needed for business, legal, or regulatory reasons, they are deleted.

7.4.3. Secure Disposal: To avoid unwanted access, data must be securely deleted.

7.5. A **data retention policy's main objectives** are as follows:

7.5.1. Ensuring Legal and Regulatory Compliance: Organizations must abide by a number of regulations, such as Australia's Telecommunications (Interception and Access) Act 1979, which mandates that certain data be kept for a minimum amount of time (e.g., two years).

7.5.2. Managing Risk and Improving Security: It lessens the footprint for possible cyberattacks by preventing sensitive data from being compromised and ensuring that data is not retained for longer than necessary.

7.5.3. Increasing Operational Efficiency: By specifying the lifecycle of data—that is, when to archive, overwrite, or remove it—it keeps systems from becoming overloaded with extraneous data.

7.5.4. Encouraging Data Governance and Privacy: It guarantees that data gathering, handling, and use follow moral and privacy guidelines.

7.5.5. Promoting Business Continuity: A clear policy guarantees the preservation of vital data for operational requirements while lowering storage expenses related to retaining outdated data.

7.6. **Data Retention Principles**: Adhere to the following principles:

7.6.1. Purpose Limitation: Data is retained only for the purpose for which it was collected or for a directly related purpose.

7.6.2. Legal Compliance: Data is kept for minimum periods required by Australian law (e.g., Fair Work Act, taxation laws).

7.6.3. Accuracy: Retained data must be accurate, up-to-date, and complete.

7.7. **Retention Periods**: The role in the system determines the retention period of the records:

7.7.1. Registered Providers: Records must be kept for at least 7 years after the date of creation. This complies with regular corporate record-keeping and tax rules in Australia.

7.7.2. Self-Managed Clients: For 5 years from the support delivery date, they are required to retain all invoices, receipts, and bank statements, especially for NDIA audit purposes.

7.7.3. Child-Related Records: Due to differing statutes of limitations for occurrences involving minors, many legal experts advise maintaining records for child-related supports until the child is 25 (or 7 years after the last contact, whichever is longer).

7.8. **Required Documents to Keep**: During an audit, you need to maintain the following in order to substantiate your claims and stay compliant:

7.8.1. Service Agreements: Contracts that you and the participant have signed.

7.8.2. Evidence of Support: Logs, rosters, or case notes that detail the date, time, length, and kind of support provided.

7.8.3. Financial Records: Tax invoices, receipts, and payment claims.

7.8.4. Consent Records: Documented evidence of a participant's agreement to data sharing or gathering.

7.8.5. Incident Reports: Detailed documentation of any incidents or grievances that need to be reported to management.

7.9. **Security and Storage Needs**: The Privacy Act and the NDIS Commission mandate that data be kept in a manner that guarantees:

7.9.1. Confidentiality: Records must only be available to employees who "need to know".

7.9.2. Integrity: Information must be shielded against loss or unwanted alteration.

7.9.3. Accessibility: Should the NDIA or the NDIS Commission seek these records, you must be able to provide them promptly.

7.10. **Methods for Disposing of Data**: Data must be securely erased at the end of its retention period to avoid unwanted access.

7.10.1. Electronic Data: Physical destruction, degaussing, or permanent erasure of storage media (USBs, hard drives).

7.10.2. Physical Information: pulping, shredding, or burning.

7.10.3. Third-Party Vendors: Bluebird Healthcare Pty. Ltd. will need a certificate of destruction if a vendor possesses data.

7.11. **Postponement of Disposal**

7.11.1. If the data is the subject of an ongoing legal dispute, an investigation, or a current legal hold, disposal will be suspended.

7.11.2. Telecommunications businesses must save a specific set of telecommunications data for at least 2 years, according to the Telecommunications (Interception and Access) Act of 1979. Subject to stringent safeguards, these duties guarantee that Australia's security and law enforcement authorities have legal access to data.

7.12. **Destruction and De-identification**: When personal information is no longer needed for any purpose for which it may be used or shared (and after the seven-year statutory term has passed), you are legally required by the Privacy Act of 1988 to destroy or de-identify it.

De-identification vs. Destruction: You have to either de-identify the record so that the person is no longer identifiable or permanently destroy it (shredding for physical or wiping for digital).

7.12.1. Method: Physical files must be shredded; digital data must be safely erased.

7.12.1.1. Secure Destruction: Professional shredding services or "secure disposal" bins are necessary for physical files. It is against the NDIS Code of Conduct to just toss files in a general trash can.

7.12.1.2. Digital Wiping: Make sure they are permanently erased; merely putting a file in the "Trash" folder is not enough to comply. Ensure digital data is purged from servers and backups rather than simply "deleted" (moved to a trash bin).

7.12.2. The Disposal Log: As proof for NDIS audits, it is recommended to keep a disposal schedule or log that details what was destroyed, when, and by whom.

7.13. **Security and Archiving**

7.13.1. Archiving: Data must be transferred to secure, restricted access storage (archived) if it is no longer needed for day-to-day operations but is necessary for legal purposes.

7.13.2. Encryption: Sensitive data that has been archived should be encrypted.

7.14. **Review**

7.14.1. This policy will be reviewed annually to ensure compliance with changing Australian legislation.

7.15. **Data Retention Schedule**

Record Category	Sample Data	Retention Period	Rationale/Legal Basis
Employment Records	Employee files, contracts, tax files	7 years after employment ends	Fair Work Act/Tax Laws
Financial/Tax	Invoices, receipts, expense reports	5–7 years	ATO Requirements
Customer Data	Name, address, transaction history	7 years post-contract	Limitation Act/Contract Law
Job Applicant Data		6 months (unsuccessful)	Privacy Act
Marketing Data	Consent records, mailing lists	Until consent withdrawn	Privacy Act (APP 11)
Telecommunications	Metadata (Service Providers)	2 years (Minimum)	TIA Act 1979
General Business	Emails, internal memos	[E.g., 3 years]	Internal Policy

8. RELATED POLICIES:

9. RELATED PROCEDURES:

10. RELATED FORMS:

8. REFERENCES:

1.1. Retention and Disposal of Customer Data Policy
https://www.service.nsw.gov.au/system/files/2024-12/retention-and-disposal-customer-data-policy.pdf

9. APPENDIX: