RECORDS MANAGEMENT PROCEDURES

The ongoing creation of records is necessary to provide accurate information of decisions and operations. A PI record is generated when information is created internally or received from external or other sources. It is maintained as evidence of PI's activities, decisions and operations.

Creation of Records

- PI prefers the creation and maintenance of digital records whenever possible.
- Records must be created and stored on the approved Information System, which is currently Microsoft SharePoint.

Storage of Records

- Physical records must be stored in an appropriate secure location accessible only to authorised personnel. For instance, printed Resident Information Sheets are stored in a locked drawer at each PI property and can only be accessed by the LIRC and OC.
- Relevant physical records must be scanned and stored securely on the PI electronic Information System, Microsoft SharePoint. Examples include receipts and invoices that are received in hardcopy.
- Electronic records must be stored on the electronic Information System, Microsoft SharePoint.
- Access to electronic records of a confidential nature will be determined by the CEO and password protected.
- Emails are not considered part of the approved Information System. If an email is deemed an accurate record, it should be stored on the approved Information System.
- External storage media and personal folders must not be used for record storage.
- PI will utilise an electronic classification system that enables easy access, retrieval, version control, and organisation of records.

Retention, Destruction and Disposal of Records

- Temporary Records are incomplete records, including but not limited to: Minutes to be typed up in the future, reminders and to-do lists, drafts such as internal reports and correspondence and unsolicited email (including 'spam'). Temporary records can be destroyed or permanently deleted once all final records are approved and stored.
- Final Records can be disposed of seven years after closing the file, but only with authorisation of the CEO. However, there are records that will be retained indefinitely, including:
    - Records related to the actual or alleged abuse of a child or vulnerable adult,
    - Documentation whose destruction might interfere with the administration of justice,
    - Articles of incorporation and registrations,
    - Audited annual reports and financial statements,
    - Constitution of PI and other associated entities,
    - Committee Terms of Reference,
    - Correspondence with external agencies such as the National Disability Insurance Authority (NDIA) and the ACT Community Services Directorate,
    - Minutes of Meetings – Boards and Committees,
    - Proof of Compliance Documentation,
    - Records pertaining to the disposal of records.

Responsibilities

The CEO is responsible for:

- ensuring compliance with all parts of the Records Management Policy and associated Procedures.
- authorisation over the deletion of data in accordance with this Policy.
- ensuring staff are knowledgeable about and following the Policy and Procedures.
- ensuring confidential records are password protected.

PI staff are responsible for:

- creating and managing records in accordance with this policy, and
- complying with the Record Management Policy and Procedures.

Related Documents

PI Privacy, Dignity and Confidentiality Policy

Authorisation

PI CEO, Dianne O'Hara