

Quick Reference

This information is primarily intended for Records Managers, Administrative Staff and other records management decision-makers

Relevant Privacy Principles are IPP4 and HPP4

Privacy Principles provide guidance on retention periods and archiving requirements. For useful information on standards for the management of information refer www.prov.vic.gov.au/gser/vice/standard

INTRODUCTION

Privacy Principle 4 relates to data security and data retention. This provides that an organisation must take reasonable steps to ensure that the information they hold is:

- **secured**, i.e. protected from misuse, loss or unauthorised access
- **retained** unless it is no longer needed for any purpose, in which case it should be destroyed or de-identified and
- if it is to be **destroyed**, that this is done in accordance with applicable laws. In default of any other laws, the HRA provides guidance about destruction of health information.

This information sheet deals only with retention and disposal of records. Security issues are dealt with separately in Information Sheet 8.

CURRENT LEGAL REQUIREMENTS

Where other laws such as the **Public Records Act** currently impose legal obligations relating to information retention and disposal, these laws prevail.

The following outlines requirements under privacy laws where no other relevant laws apply to the information held by an organisation.

In order to implement Privacy Principles in this context, Primary Care Partnerships (Partnerships) should include in their documented privacy protocols, requirements in relation to storage and retention of the information held by their member agencies.

DOCUMENTING A RECORDS MANAGEMENT PROTOCOL

A good protocol must include policy and procedures on how information will be protected from loss, misuse and unauthorised access. This includes measures to safeguard information from both accidental loss and intentional breaches of security. If information is not securely stored and managed, then there is an increased risk that a consumer's privacy may be breached. The protocol should clearly articulate:

- How long information will be **retained** by the service
- How information is to be **archived** and how it will be stored to allow ease of retrieval if the consumer, authorised representative or the agency seeks access to the information in the future
- When information that is being held is no longer required, how it will **de-identified or physically destroyed**
- How information will be **transferred** securely to another agency, if no longer required

RETENTION OF PERSONAL INFORMATION

Privacy protocols should clearly articulate how long different categories of personal information will normally be retained. Unless there is a legal requirement to retain certain information, it must not be retained for a period longer than required. Privacy laws provide some guidance on this issue as follows.

- In relation to **health** information, HPP 4.2 (b) specifies the minimum period that client records must be retained - that is, a minimum period of 7 years from the date of the client's last contact with the service; or in the case of a child client, until the child attains the age of 25 years.
- In relation to **non-health** personal information, IPP4 provides that in the absence of other legal requirements (which override privacy provisions), such information should be retained for so long as it is needed for any purpose.

Quick Reference

If the information is to be de-identified it should be done in such a manner that subsequent aggregation or collation of the information will not identify the consumer.

ARCHIVING CLOSED RECORDS

Privacy protocols should also set minimum standards for archiving closed client records during the appropriate retention period. This would include:

- Registration and filing standards to facilitate search and retrieval of closed records, both for the organisation's own use where a client re-presents for service, and for client access if and when requested.
- Preservation standards to ensure that archived records are protected from physical degradation.

DE-IDENTIFICATION OF RETAINED INFORMATION

For some purposes, it may be appropriate to retain information in a **de-identified** form (effectively destroying all identifying details). These purposes primarily relate to information which is of continuing value for statistical purposes (e.g. planning purposes).

Care must be taken to ensure that all identifying details are removed, including potentially identifying information such as patient code numbers, address details etc which may be matched with names or other details held elsewhere in the agency.

DISPOSAL OF PERSONAL INFORMATION

Privacy protocols should specify secure methods of physical destruction of personal information (e.g. secure shredding).

It may also be appropriate to establish audit checks to ensure that the destruction has been completed as directed, particularly where the destruction is contracted out to an external provider.

Where information has been deleted, a file note should be made, and retained in the organisation, that records the name of the person to whom the information related, the period covered by it, the date and the reason that it was destroyed.

TRANSFER OF PERSONAL INFORMATION

Where information has been permanently removed by transfer to another organisation, a file note should be made and retained in the organisation and should record the name of the person to whom the information related, the organisation to which it was transferred, the period covered by it, the date on which it was transferred and the reason for transfer.

PRIVACY IN PRACTICE – SOME 'REASONABLE STEPS' TO CONSIDER

- Archiving data securely; that is, strictly limiting when information may be accessed in the future and by whom
- Converting paper records to electronic data to reduce the physical space required for storage and to control the potential breaches that could occur
- Keeping only a summary or statistical information if this is all that will be required
- The use of shredding machines and methods of secure destruction of sensitive information to prevent any opportunity for misuse
- When a consumer changes providers, transferring the information to the new provider, if the consumer consents

LEGAL ADVICE : DISCLAIMER

Information contained within this information sheet is not intended to substitute for legal advice. Primary Care Partnerships and / or their member agencies should take advice from their legal advisors in determining whether their policies and practices comply with all relevant legislation.