


Title:	Privacy			
Section:	Governance	PRH:	Chief Executive Officer	

1. POLICY STATEMENT:

To ensure that Alexandra District Health (ADH) provides safe high quality health care and experiences to our consumers by actively following the Victorian Clinical Governance Framework and through its Consumer Participation Framework actively engage and partner with consumers.

To ensure all staff are responsible and accountable for safe and high quality care, and ADH continuous improvement will be informed by regular monitoring and evaluation of performance.

Privacy refers to a person's right to keep certain information confidential. ADH adheres to the Privacy and Data Protection Act 2014 and the Health Records Act (Vic) 2001 and supports the Department of Health (Vic) commitment to protecting the privacy of personal information in accordance with these Acts. It also ensures that requirements of the Privacy Act are complied with and to manage any grievances or breaches in relation to privacy. Only authorised staff have access to personal information which remains confidential and is only used as appropriate. Information shall only be released according to the appropriate legislative requirements.

Privacy covers all personal information held by Victorian public health services and includes information that has been collected from consumers/patients over the telephone, through mail, email, personal contact or over the Internet, and medical records.

2. POLICY OUTCOME:

Alexandra District Health is committed to protecting the privacy and confidentiality of patients and other persons that Alexandra District Health interacts with.

This policy intends to ensure that all actions by ADH staff and contracted parties are in accordance with relevant privacy legislation and that the privacy and interests of ADH, its patients, staff and visitors are respected and protected. The health service and its staff are committed to minimising any risk of incidents regarding breach of Privacy Principles.

3. ROLES AND RESPONSIBILITIES:


All staff are responsible and accountable to know, understand and support each other to meet the requirements of the Victorian Clinical Governance Framework. All staff will be aware of the Consumer Participation Framework and actively engage and partner with consumers, demonstrate ownership and accountability for safe, quality care, and participate in regular evaluation and monitoring of performance to inform improvement.

Key legislation, acts & standards:

- Australian Charter of Healthcare Rights (second edition) 2019
- Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Privacy Act 1988 (Cth)
- Health Records Act 2001 (Vic)
- Health Services Act 1988 (Vic)
- Freedom of Information Act 1982 (Cth)
- Mental Health Act 2014 (Vic)
- Privacy and Data Protection Act 2014
- My Health Records Act 2012
- Family Violence Protection Act 2008 (Vic)
- Child Wellbeing and Safety Act 2005 (Vic)

4. PROTOCOL:

Prompt Doc No: <#doc_num> v<#ver_num>	Page 1 of 6	Last Reviewed: <#last_review_date>
First Issued: <#issue_date>	UNCONTROLLED WHEN DOWNLOADED	Review By: <#next_review_date>
Version Changed: <#revision_issue_date>		

Title:	Privacy			
Section:	Governance	PRH:	Chief Executive Officer	

Principles:

The following are the main principles related to Privacy.

Collection of Information

Health information is necessary for the performance of a function or activity and should be collected with consent (or if it falls within Health Privacy Principle 1). Individuals are to be informed about what is done with the information and how they can gain access to it.

Disclosure

Use and disclosure of personal information should only be used for the primary purpose for which it was collected. Use of information for secondary purposes of disclosure should have the consent of the person involved.

Personal Information may be disclosed in a number of circumstances including the following:

- third parties where an individual consents to the use or disclosure; and
- where required or authorised by law

Patient information will not be disclosed to external agencies without written permission and will not be available to overseas companies for any purpose.

Data Quality

When collecting data ensure that the information is accurate, complete, relevant and current. It is important that individuals advise the organisation at the earliest opportunity of any changes to their personal information, so that records can be updated.

Documents will be stored and disposed of in line with Public Record Office Standards, published by the Public Records Office Victoria.

Data Security and Retention

Health Information must be secure, protected against misuse, loss and unauthorised access. Destruction of health information must be in line with relevant standards

- Documents, personal and personnel information must be stored and disposed of in line with Public Record Office Standards published by the Public Records Office Victoria.
- All personal and personnel information will be stored securely.
- Access to personal and personnel information will have secure access
- Online information must be stored securely or password protected and have appropriate back up systems

Openness/Access to Information

Health Information policies reflect clearly the management of personal information and are accessible on request. National Privacy Principles provide individuals with the right to access to their personal information and to update and/or correct it, subject to certain exceptions. If an individual wishes to access their personal information they should do so in writing.


Access to Correction

Individuals have the right to seek access to their personal information and make corrections. Access and correction will be handled mainly under the Victorian of Freedom of Information Act. (refer to the Freedom of Information Policy and Procedure)

Unique Identifier

A unique identifier is usually a number assigned to an individual in order to identify the person for the purposes of the organisation's operations. Unique identifiers facilitate data matching and reduce duplication.

Prompt Doc No: <#doc_num> v<#ver_num>	Page 2 of 6	Last Reviewed: <#last_review_date>
First Issued: <#issue_date>	UNCONTROLLED WHEN DOWNLOADED	Review By: <#next_review_date>
Version Changed: <#revision_issue_date>		

Title:	Privacy			
Section:	Governance	PRH:	Chief Executive Officer	

Anonymity

Relates to giving the individuals the option of not identifying themselves when entering transactions with organisations. This would only occur under specific circumstances and would need to be lawful and practicable.

Transborder data flows

Transfer of health information outside Victoria is subject to relevant laws and the transfer of personal information outside Victoria is restricted. Personal information may be transferred only if the recipient protects privacy under standards similar to Victoria's Information Privacy Principle's (IPPs).

Sensitive Information

The law restricts certain collection of sensitive information like an individual's political views, religious beliefs, sexual preferences, membership of groups or criminal records. Sensitive information is a special category of personal information. It is defined as information or an opinion about an individual's racial or ethnic origin, impairment or disability, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or criminal record.

Information available to another Health Service Provider

As a health service provider, you must make health information relating to an individual available to another health service provider if requested by the individual.

Personal Information

Personal information is any information or an opinion (including information or an opinion forming part of a database) that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

My Health Record


My Health Record (MHR): is a national secure online summary of an individual's health information. The individual is able to control content and access to their MHR. Content is sourced from the individual, Medicare, and healthcare providers. From February 2019, every individual with a Medicare or DVA card will now be automatically registered for an MHR, unless they have opted not to have one. Individuals can also decline access to specific documents within their MHR. They can set up a PIN Code so that only certain clinicians with permission can access their MHR. They can subscribe to SMS or email alerts that report in real time when their MHR has been accessed. All instances of access to any MHR are logged. Access to 'My Health Record' is only permitted for the purpose of delivering health care to an individual in accordance with My Health Record legislation.

Third Parties

Where reasonable and practicable to do so, we will only collect Personal Information from individuals directly. However, in some circumstances we may be provided with information by third parties. In such cases we will take all reasonable steps to ensure that the individual is made aware of the information provided to us by such third party.

Email

To minimise the risk of a privacy breach or inappropriate disclosure, staff must do the following when sending identifiable health information by email:

Title:	Privacy			
Section:	Governance	PRH:	Chief Executive Officer	

- exercise discretion in determining if email is a suitable method to communicate the information;
- do not include identifying details such as UR number, patient name, address etc unless necessary;
- only include essential information in the email;
- check the email address is correct before sending;
- send emails only to individual email addresses, not to distribution lists or group email addresses;
- use available encrypted email technology for sending patient health information such as Liquidfiles.

Social Media

Staff must not disclose health information by social media.

Exemptions

There are exemptions to information privacy in some circumstances, according to the Privacy and Data Protection Act 2014. These include the Freedom of Information Act (1982), law enforcement, information sharing under the Family Violence Protection Act 2008, the Child Wellbeing and Safety Act 2005, information sharing for quality and safety purposes under the Health Services Act 1988, and under Division 6 of Part 4A of Terrorism (Community Protection) Act 2003.

Privacy Breach

A privacy breach occurs when there is a failure to comply with one or more of the Information Privacy Principle's. Some of the most common privacy breaches happen when personal information is stolen, lost or mistakenly disclosed (e.g. a computer containing personal information is stolen, files are lost, USB sticks or computer disks are misplaced or personal information is mistakenly emailed to the wrong people). A privacy breach may also be a consequence of faulty business procedure or operational breakdown.

The four key steps for responding to a breach or suspected breach are:


1. Breach containment and preliminary assessment
2. Evaluation of the risks associated with the breach
3. Notification to the CEO
4. Identification of actions for prevention and improvement staff training, policy review or development, improved security measures, audit of information handling.

Grievance Procedure

- Complaints must be made in writing.
- Assessment and investigation of the complaint will occur in consultation with the Chief Executive Officer.
- A written response will be sent to the individual within 7 days of a complaint being received.
- If the response is found to be unacceptable to the individual, conciliation or arbitration may be suggested.
- If the individual makes a formal complaint to the Privacy Commissioner, the Chief Executive Officer is the respondent on behalf of Victoria Health

Key Steps in Responding to Privacy Breaches

Privacy breaches can occur through poor adherence to policies, lack of training, a misunderstanding of the law, a deliberate act, a technical problem or bad luck. ADH believes that

Title:	Privacy			
Section:	Governance	PRH:	Chief Executive Officer	

being prepared can significantly reduce the risk of occurrence and the impact of a breach. Privacy training for all staff is conducted on induction and refresher basis.

Incident Reporting

Any privacy breaches identified are reported through the Incident monitoring system, known as VHIMS (Victorian Health Information Management System) in a timely manner. These are investigated, contributing factors identified, and quality improvement actions put in place in order to reduce the risk of further incidents.

Privacy Impact Assessments:

A privacy impact assessment (PIA) is a systematic assessment of a project or program that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

A **program** includes a new process, project, technology, or assessing if existing programs comply with privacy obligations. Program is intended to cover the full range of an organisation’s activities that may have privacy implications, such as legislation, a project or initiative, a service, application, platform, policy, database or procedure.

This tool is designed to assist with reporting its findings and respond to recommendations.

A flexible approach can be adapted in using this tool to suit the size, complexity and risk level of the project. The term ‘project’ covers the full range of activities and initiatives that may have privacy implications.

This tool should be used in conjunction with the [Guide to undertaking privacy impact assessments | OAIC](#) and PIA eLearning course.

Privacy Threshold Assessment (PTA) is an initial, ‘broad-brush’ survey, which is undertaken early in the program life-cycle in order to determine whether a PIA needs to be performed, and if so what scope the PIA should have; providing a sense of the risk level, including whether it could be a “high privacy risk program” requiring a PIA.

A PIA tool is attached in the appendix and available on Prompt for staff to download and use.


Privacy Officer:

For the purpose of all consumer enquiries related to privacy, the health information officer will be the nominated ADH Privacy Officer.

5. REFERENCES:

Australian Government (2019)., Australian Digital Health Agency, My Health Record. What is My Health Record. Retrieved from <https://www.myhealthrecord.gov.au/for-healthcareprofessionals/what-is-my-health-record>
 Health Information Privacy Policy, Alfred Health, accessed on Prompt, 1st February, 2024.

Health Records Act 2001(Vic), Authorised Version No. 048, as at 1st September 2023.
 Health Services Act 1988 (Vic), Authorised Version No.180, as at 1st November, 2023.
 My Health Records Act, C2023C00382 (C12) as at 18th October 2023
 Privacy and Data protection Act 2014 (Vic), Authorised Version No. 030, as at 1st September, 2023.

Title:	Privacy			
Section:	Governance	PRH:	Chief Executive Officer	

Freedom of Information Act 1982 (Vic), Version C2024C00009 (C112), as at 1st January, 2024.
 My Health Record Policy, Wimmera Health Care Group, access on Prompt 22nd January, 2024

Office of the Australian Information Commissioner. Privacy Impact Assessment tool. (version September 2021) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments>,

Privacy and Data Protection Act 2014, Authorised Version No. 030, as at 1st September 2023
 Privacy Policy, Goulburn Valley Health, accessed on Prompt 22nd January, 2023
 Privacy Procedure, Northern Health, accessed on Prompt 19th January, 2024
 Privacy Impact Assessment Procedure, Barwon Health, accessed on Prompt 20th May, 2024

6. RELATED DOCUMENTS:

- [Feedbacks and Complaints Brochure](#)
- [Complaints](#)
- [Confidentiality](#)
- [ADH Privacy and Your Rights brochure](#)
- [Guide to undertaking privacy impact assessments | OAIC](#)

7. APPENDIX A: PRIVACY IMPACT ASSESSMENT TOOL:

- [Privacy Impact Assessment Tool](#)