

Adeney Private Hospital – Privacy & Confidentiality Policy

POLICY

Adeney Private Hospital (APH) is bound by the Australian Privacy Principles under the Privacy Act 1988 (Cth) (Privacy Act) and other relevant laws about how private health service providers handle information (including but not limited to personal information).

The hospital is committed to the protection of personal and health information in accordance with the privacy laws which govern how the information is collected, used, disclosed and stored.

EXPECTED OUTCOME

- ☑ Adherence to the Health Privacy Principles (HPPs) as detailed in the Health Records Act 2001, (VIC) and the Australian Privacy Principles (APPS) as detailed in The Privacy Act 1998 (Cth).
- ☑ The privacy of patients, employees, Visiting Medical Officers (VMOs), authorised contractors and other customers is protected.
- ☑ Access to and disclosure of personal information is appropriate, audited and recorded

SCOPE

This policy refers to patients, employees, potential employees (i.e. job applicants), VMOs, , medical and nursing students and authorised contractors who are engaged with patient care at Adeney Private Hospital.

Definition:

Personal Information

Personal information is data or information about an identified individual or information that can be used to identify an individual. Personal information can include an opinion about an identified individual recorded in a material form, or not. Personal information does not need to be true or accurate to be classified as identifiable.

Sensitive Information

Sensitive information is a type of personal information that is afforded a higher level of protection by privacy laws. It includes health, genetic and biometric information as well as information about race or ethnic origin, political opinions, membership of political, professional or trade associations or trade unions, religious beliefs, sexual orientation or practise and criminal record.

References in this policy to personal information include sensitive information.

POLICY OUTCOMES

This policy explains how the hospital will collect, hold, use, disclose, secure and manage both the personal and health information of the individuals who utilise, access, contribute to or are identified within APH's services.

Collection and Retention of Personal Information

The type of information collected depends on who the individual is and their relationship with the hospital. Information is collected from patients admitted to the hospital, health service providers (e.g. other hospitals, pharmacy, pathology), next of kin, carers, guardians, emergency contacts, significant others, persons responsible for paying the account (health funds, TAC, DVA, WorkCover) and job applicants.

Information Collected Includes:

- Contact details for an individual and identified emergency contacts, including name, address, email, telephone numbers and next of kin.
- Demographic information including gender, date of birth, marital status, occupation, religion, country of birth and indigenous status.
- Health information including medical history, social history, medications, diagnostic imaging and reports, pathology results, diagnosis, observations, symptoms, plan of care and treatment given.
- Billing information such as credit card details, health fund membership details, workers compensation, TAC or other insurance claims, Medicare details and concession card details.

Collection of Personal Information

Adeney Private Hospital will usually collect information directly from the individual concerned but sometimes it may be collected from a third party. The hospital will only do this if consent has been obtained or where it is not reasonable or practical for us to collect this information directly from the individual.

Third parties who the hospital may collection information from include:

- A responsible person, guardian, or representative
- Another health service provider / specialist
- A treating specialist or health care professional
- Health insurance agency or other insurer
- Family or carer
- Other sources where necessary to provide our services (e.g. pathology labs)
- Job referees and applicants

Anonymity

Patients have the option of dealing with the hospital anonymously or by using a pseudonym; however, this may limit the services that the hospital can provide if it is impractical for us to deal with you in such an unidentified manner.

Use and Disclosure of Personal Information

Your information may be used and/or disclosed for these reasons to these service providers:

- To assist the treating team (doctors, nurses and other health professionals) in providing care and treatment.

- ☒ To provide necessary follow-up treatment and ongoing care, liaising with health care providers.
- ☒ To verify an individual's identity.
- ☒ For internal administrative requirements, including processing admission, discharge and billing.
- ☒ To health funds, Medicare, Transport Accident Commission, WorkCover and the Department of Veterans Affairs for accounts purposes.
- ☒ In an emergency where life is at risk and the individual cannot consent.
- ☒ To conduct patient experience surveys and outcome measures with the aim of evaluating and improving services.
- ☒ To assist in the management of the hospital, including service monitoring, complaints handling, feedback and evaluation.
- ☒ For safety and quality improvement activities, maintaining Accreditation.
- ☒ To address liability indemnity arrangements and reporting with insurers, medical defence organisations and lawyers as well as for the defence of anticipated or existing legal proceedings.
- ☒ For reporting of summarised de-identified information to the Victorian Health Department, Australian Bureau of Statistics Private Hospital Data Bureau and other Government agencies.
- ☒ Health service providers used by Adeney Private Hospital (e.g. pharmacy, pathology)
- ☒ To undertake research and the compilation or analysis of statistics relevant to public health and safety.
- ☒ Assess job applications.
- ☒ To comply with legal and regulatory compliance.

Personal Information is not used for unrelated secondary purposes without the patient's consent. Examples of unrelated secondary purposes include:

- ☒ promotional offers and special events
- ☒ fundraising
- ☒ marketing.

APH may disclose an individual's personal information to the following third parties for the above purposes to:

- ☒ Other health service providers or diagnostic services involved in the individual's treatment.
- ☒ Private health insurers and other insurers.
- ☒ Health profession students undertaking clinical placements (unless individual has opted out).
- ☒ A responsible person (e.g. parent, guardian, spouse) if the individual is incapable or cannot communicate, unless the individual has requested otherwise.
- ☒ Other facilities as part of employment processes.
- ☒ The hospital's insurers and legal representatives.

An individual's consent is obtained prior to providing information to other health service providers. *Refer to the Request for Information procedure for further information.*

Transborder Disclosure

From time to time the hospital may need to disclosure personal information to and collect personal information from other states and territories or other countries, this will always be in accordance with privacy laws. Information will not be sent overseas without the patient's written permission.

Security and Storage

The Hospital stores personal information in both paper and electronic form. The security of personal information is maintained by a number of methods:

- ☑ All staff are required to maintain confidentiality.
- ☑ Document security measures are in place.
- ☑ Security measures for access to computer systems.
- ☑ Policy and procedures governing access to information.

Data Breach

A data breach occurs when personal information that is held by the Hospital is subject to misuse or loss or to unauthorised access, modification or disclosure.

A data breach can be caused deliberately as a result of a malicious act from an external or internal party. It can also be caused by human error or by a failure of an organisation to implement effective information management or security systems.

Examples of data breaches include:

- ☑ When an employee takes paper records, an unencrypted USB stick or laptop out of the office and the information is lost or stolen.
- ☑ When an organisation mistakenly provides personal information to the wrong person.
- ☑ When an organisation's database is illegally accessed by staff members or by individuals outside of the organisation.

When notified of a suspected breach Adeney Private Hospital will take each situation seriously and immediately investigate, taking steps to:

- ☑ Contain the breach and conduct a preliminary assessment
- ☑ Evaluate the risks associated with the breach
- ☑ Remediate and notify (and other steps to mitigate harm)
- ☑ Review the cause of the breach and your organisation's response and take steps to improve practices and lessen the likelihood of future breaches.

Accuracy

Adeney Private Hospital will take reasonable steps to ensure that the personal and health information it collects uses or discloses is accurate, complete and up to date and relevant to its functions or activities. Measures taken include appropriate medical record forms, employee selection, training, computer edits and accuracy audits. The accuracy of the information depends largely on the quality of the information provided to the hospital.

Access to Information

All individuals have the right to access information held by APH. During an admission, the health care team is the best source of information about care and treatment.

Fees are applicable as per the Privacy Act 1998 (Cth) and the Health Records Act (VIC) 2001.

If APH refuses a request for access the requestor will be notified in writing explaining the reasons for the refusal and how they can complain if they are not satisfied with the explanation.

Complaints

For questions regarding privacy, the policy or the way in which we manage personal information, if Privacy rights have been breached or if there is a complaint -

Contact the Privacy Officer

By Mail - Adeney Private Hospital

209 Cotham Rd
KEW 3101

The Privacy Officer will endeavour to provide a written acknowledgement of receipt of the complaint within 7 days and provide a written response to the complaint within a reasonable timeframe.

If an individual is not satisfied with APH's response to the complaint or if an individual requires more information about privacy, they may contact the Office of the Australian Information Commissioner (OAIC)

By Mail - Office of the Australian Information Commission
GPO Box 5218
Sydney NSW 2001
By Email – enquiries@oaic.gov.au
Telephone - 1300 363 992
Website - www.oaic.gov.au

REFERENCES AND RELEVANT DOCUMENTS

- Health Privacy Principles (HPPs)
- Health Records Act 2001
- Australian Privacy Principles (APPs)
- Privacy and Data Protection Act 2014 (Vic)
- Privacy Amendment Act 1998 (Cth)
- <https://ovic.vic.gov.au>