



PURPOSE

This policy explains how we collect, hold, use, disclose, secure and otherwise manage the personal information, including the health information of patients who use our services. It describes the types of information we collect and hold and why, how to access and correct the information and how to make a privacy complaint.

SCOPE

This policy applies to all ACHA facilities.

POLICY

The ACHA Health policy on Privacy is:

- ACHA is committed to the protection of personal and health information in accordance with privacy laws in the provision of its integrated health services through the private hospitals, medical centres and pathology services it operates and manages.**

Introduction to Privacy

The Australian division of the ACHA Group is required to comply with the *Privacy Act 1988* (Cth) (as amended) (**Privacy Act**), and handles the personal information (including health information) that it collects and holds in accordance with the Australian Privacy Principles (**APPs**) contained in the Privacy Act. ACHA must also handle health information it collects and holds in compliance with applicable State and Territory based health records laws.

ACHA is committed to the protection of personal and health information in accordance with these privacy laws in the provision of its integrated health services through the private hospitals, medical centres and pathology services it operates and manages.

All new patients are provided with a copy of the ACHA Privacy Brochure, as it is current from time to time, where possible and practicable to do so. Patients are to be advised that a copy of the ACHA Privacy Policy.

Definition

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable, whether that information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

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 practices and criminal record.

References in this policy to personal information include sensitive information.

THIS IS A CONTROLLED DOCUMENT	
APPROVED	Paul Evans
DESIGNATION	CEO, Hospital Operations
DATE	August 2019



Dealing with ACHA anonymously

Where it is lawful and practicable to do so, individuals may deal with us anonymously or use a pseudonym (e.g. when enquiring about our services generally). However, in many instances we need to identify you when you deal with us, including to provide our services and to respond to complaints. If we do not receive all of the personal information we request, we may not be able to do these things.

What personal information do we collect and hold?

The information we collect will depend on who the individual is, such as a patient admitted to one of our hospitals, or attending one of our medical centres or pathology services, a health service provider, a next of kin, a guardian or other responsible person, an emergency contact or person responsible for paying an account, and may include an individual's:

- name, address (postal and email) and telephone numbers
- gender
- date of birth
- marital status
- occupation
- religion
- country of birth
- indigenous status
- next of kin
- payment information such as credit card details
- health fund and health insurance cover details
- workers compensation or other insurance claim details
- Medicare details
- concession card details
- medical history and other health information we are provided with or we collect in the course of providing our services
- other details an individual provides for admission to or discharge from one of our hospitals
- practice details if the individual is a general practitioner; and
- other information we need to provide our services.

In certain circumstances, we are required by Australian law to collect some of this information, such as Medicare details.

Collection of Personal Information

We will collect personal information directly from the individual concerned where it is reasonably practicable to do so. This may take place when the individual completes documents such as an admission, health insurance claim or other form, provides information over the telephone, is treated at an ACHA hospital, or applies for a job with us.

However, depending on who the individual is, we may also collect their personal information from third parties such as:

- a responsible person or representative (e.g. guardian)

THIS IS A CONTROLLED DOCUMENT	
APPROVED	Paul Evans
DESIGNATION	CEO, Hospital Operations
DATE	August 2019



- an individual's health service provider including specialists
- a health professional who has treated the individual
- an individual's health insurer or other insurer
- an individual's family
- an individual who we are admitting (e.g. we ask them to provide emergency contact details)
- job referees
- other sources where necessary to provide our services (e.g. pathology labs) or to assess job applicants (e.g. police checks).

We collect sensitive information about an individual, either directly or from a third party, with the individual's consent (which may be implied or express, depending on the circumstances).

For what purposes do we use and disclose personal information?

ACHA uses the personal information it collects and holds to:

- assess and understand the health and other needs of individuals to provide them with the appropriate services and advice including for admission and discharge from our hospitals, or treatment at any ACHA facility
- ensure continuity of care of individuals treated in our facilities and provide ongoing treatment options
- contact individuals to respond to enquiries, to follow up, in an emergency, for authorisation in relation to any services
- enable the provision of education and training to students of the health profession
- effectively administer, manage, monitor and improve our services
- funding, planning, evaluation and complaint-handling
- communicate with individuals by various means about our services, events, offers and options available from our hospitals and other facilities
- charging, billing, processing health insurance claims and collecting debts
- assess job applications
- verify an individual's identity
- ensure the health and safety of our staff and individuals who use our services or attend our facilities
- comply with quality assurance or clinical audit activities
- undertake accreditation activities
- provide health insurance funding
- respond to feedback
- address liability indemnity arrangements and reporting
- prepare the defence for anticipated or existing legal proceedings
- undertake research and the compilation or analysis of statistics relevant to public health and safety
- conduct patient experience surveys with the aim of evaluating and improving services; and
- enable our facilities and our service providers to comply with their legal and regulatory obligations.

We may also use personal information in circumstances where we are required or authorised by Australian law to do so or where we otherwise have consent of the individual or their representative.

THIS IS A CONTROLLED DOCUMENT	
APPROVED	Paul Evans
DESIGNATION	CEO, Hospital Operations
DATE	August 2019



Direct Marketing

We will only use personal information for direct marketing and promotional activities with the individual's express consent. All direct marketing communications will include the option for an individual to opt out of receiving direct marketing communication. Individuals can opt out at any time.

Disclosure of Personal Information

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

- other health service providers involved in the individual's treatment or diagnostic services
- private health insurers (some of which are located overseas) and other insurers
- students of the health profession undertaking clinical placements, but not when an individual has opted out of student teaching activities
- a responsible person (e.g. parent, guardian, spouse) when the individual is incapable or cannot communicate, unless the individual has requested otherwise
- close family members, in accordance with the recognised customs of medical practice
- our insurers and legal representatives
- service providers engaged to provide services to our hospitals and other facilities including manufacturers and suppliers of medical devices, providers of pathology and radiology services, some of whom may be located overseas or interstate; and
- companies within the ACHA Group.

Trans-Border Disclosures

We operate and communicate with organisations throughout Australia and overseas.

We may therefore disclose personal information outside the State or Territory in which the individual resides and also in some circumstances to related entities within the ACHA Group who are located overseas. Countries where overseas recipients are located include Malaysia, Singapore, Canada, the United Arab Emirates, France, USA, Vietnam, Costa Rica, Belgium and New Zealand.

Management of Privacy Preferences and Capacity

Whether a child has the capacity to make their own privacy decisions is assessed by ACHA staff on a case-by-case basis having regard to matters such as their age and circumstances. Generally an individual aged 15 years and over will have the capacity to make their own privacy decisions.

For children under 15 years or for individuals who lack capacity to make privacy decisions for themselves, we will refer or deal with requests for access, consents and notices in relation to personal information by reference to the parent and/or guardian or other responsible persons authorised by applicable laws and will treat consent given by them as consent given on behalf of a child or the individual who lacks capacity.

THIS IS A CONTROLLED DOCUMENT	
APPROVED	Paul Evans
DESIGNATION	CEO, Hospital Operations
DATE	August 2019



Storage and Security of Personal Information

We store personal and health information in both paper and electronic form. The security of personal and health information is very important to us and we take reasonable steps to protect it from misuse, interference and loss and from unauthorised access, modification or disclosure.

Some of the ways we do this include:

- requiring our staff to maintain confidentiality
- implementing document storage security
- imposing security measures for access to our computer systems
- providing a discreet environment for confidential discussions; and
- allowing access to personal and health information only where the individual seeking access to their own information has satisfied our identification requirements

Personal and health information is retained for the period of time determined by applicable Australian laws after which it is de-identified or disposed of in a secure manner.

How do we keep personal information accurate and up-to-date?

We take all reasonable steps to ensure that the personal information we collect is accurate, complete and up-to-date, and also when we use or disclose it, that it is relevant.

We will also take reasonable steps to correct the personal information we hold if we are satisfied that it is inaccurate, incomplete and out of date, irrelevant or misleading, or if an individual asks us to correct their personal information for these reasons. A request to correct personal information can be made at any time by contacting us on the details below.

However, the accuracy of that information depends largely on the quality of the information provided to us. We therefore suggest that individuals:

- let us know if there are any errors in their personal information; and
- keep us up-to-date with changes to their personal information (e.g. their name and address).

Individuals may do this by mail or email using the information provided below.

There may be circumstances in which we may have to refuse a request for correction. If this happens, we will notify the individual in writing of our reasons for the refusal and explain how they can complain if they are not satisfied.

Access to Personal Information

Individuals have a right to access the personal information that ACHA holds about them by contacting the Director of Nursing of the relevant hospital, or the Privacy Officer at ACHA Head Office.

If individuals request access to their personal information, we will need to verify their identity and may ask them to complete a request for access form. We will then grant the request within a reasonable period. However, we may refuse a request for access to some or all of the personal information in certain circumstances allowed by the Privacy Act or other applicable laws. If ACHA refuses a request for access, we will give written notice of our decision, including our reasons and how to complain if the individual is not satisfied with the decision.

THIS IS A CONTROLLED DOCUMENT	
APPROVED	Paul Evans
DESIGNATION	CEO, Hospital Operations
DATE	August 2019



We will endeavour to give access to an individual's personal information in the form they request. However if that is not possible we will provide alternative means of access or discuss how access can be given through a mutually agreed intermediary.

We may charge a fee for collating and providing access to personal and health information.

We will disclose the personal information we give access to, to the individual's authorised representative or legal adviser where we have been given written authority to do so.

Complaints

Individuals who have any questions about privacy, this policy or the way we manage personal information or who believe that we have breached their privacy rights should contact the Director of Nursing of the relevant hospital, or the relevant corporate manager at Head Office with their question or complaint.

If the Director of Nursing, Practice Manager, State Collection Services Manager, or Corporate Manager is not able to respond to the individual's question or complaint to their satisfaction, the individual may contact ACHA's Privacy Officer on the details below.

Complaints should be in writing and addressed to:

The Privacy Officer
Healthscope Limited
Level 1, 312 St Kilda Road, Melbourne VIC 3004

Email: Privacy.Officer@healthscope.com.au

ACHA will endeavour to acknowledge receipt of a written complaint within 7 days and provide a written response to the complaint within a reasonable timeframe. It may be necessary to request further information from the complainant before the matter can be resolved. Any such request will be made in writing.

If the individual is not satisfied that ACHA has resolved their complaint, they have the right to make a complaint to the Office of the Australian Information Commissioner (OAIC). If they wish to make a complaint or to find out any more information about their privacy rights the OAIC can be contacted as follows:

Website: www.oaic.gov.au

Telephone number: 1300 363 992

In writing: Office of the Australian Information Commissioner GPO Box 5218, Sydney NSW 2001

Individuals may also make a complaint regarding the handling of their health information to the statutory health complaints authority in their State or Territory.

THIS IS A CONTROLLED DOCUMENT	
APPROVED	Paul Evans
DESIGNATION	CEO, Hospital Operations
DATE	August 2019



Contacting ACHA

Individuals should first contact the Director of Nursing of the relevant hospital, either by phone or in writing. Contact details can be obtained from the hospital's website or via the Healthscope website: www.healthscope.com.au

Individuals can also contact the Privacy Officer at Healthscope Head Office, details below.

The Privacy Officer
Healthscope Limited
Level 1, 312 St Kilda Road, Melbourne VIC 3004

Email: Privacy.Officer@healthscope.com.au

Telephone: 03 9926 7500

Changes to Privacy Policy

Healthscope may review, change and update this Privacy Policy from time to time to reflect our current practices and obligations and changes in technology. We will publish our current Privacy Policy on our website at www.healthscope.com.au and the changes will take effect at the time of publishing

RESPONSIBILITIES

All staff are responsible for ensuring they familiarise themselves with this policy and any related attachments, which in effect, form part of this policy.

The General Manager carries overall responsibility for management of this Policy and any related attachments. The General Manager and the Directors of Nursing will ensure that the policy is compliant with all legislative requirements, and is responsible for ensuring the policy is reviewed and updated in line with the timeframes determined by the ACHA Executive, via the Executive Committee.

REGULATORY REFERENCES

- Chief Medical Officer and Healthscope Privacy Officer
- *Privacy Act 1988* (Cth) (as amended)
- Office of the Australian Information Commissioner website: www.oaic.gov.au

REVIEW / CONSULTATION

All General Managers	All Directors of Nursing	All Quality Managers
Pathology Cluster	All Health Information Managers	

THIS IS A CONTROLLED DOCUMENT

APPROVED	Paul Evans
DESIGNATION	CEO, Hospital Operations
DATE	August 2019