Name of Policy:	Privacy Policy
Policy Number:	P01-01
Purpose of Policy:	Meeting privacy obligations is an integral component of an organisations safety, quality and risk management program. Mildura Health Private Hospital (MHPH) is committed to ensuring the privacy and confidentiality of patient information.
National Standard Applicable:	Governance
Policy Applies to:	☑ All Staff ☐ Management
Approval Authority:	Safety and Quality Management Committee
Document Author:	C. Kirby
Responsible Officer:	Chief Executive Officer
Policy Date:	January 2021

Legislation:

Privacy Act 1988:

The Privacy Act regulates how private sector organisations collect, hold, use and disclose personal information, and how individuals can access and seek correction of that information.

Mildura Health Private Hospital (MHPH) is bound by the Australian Privacy Principles (APP) under the Privacy Act and other relevant laws, about how private health providers handle personal information.

Privacy Amendment (Enhancing Privacy Protection) Act 2012:

The APP's from the Privacy Amendment (Enhancing Privacy Protection) Act 2012 amends the Privacy Act 1988.

Privacy Amendment (Notifiable Data Breaches) Act 2017:

The passage of this amendment established the Notifiable Data Breaches (NDB) scheme in Australia. The NDB Scheme applies to all agencies and organisations with existing personal information security obligations under the Australian Privacy Act 1988 (Privacy Act) from 22 February 2018.

Health Records Act 2001:

The Health Records Act regulates the collection and handling of health information. The Act:

- Gives individuals a legally enforceable right of access to health information about them that is contained in records held in Victoria by the private sector; and
- Establishes Health Privacy Principles (HPPs) that will apply to health information collected and handled in Victoria by the Victorian public sector and the private sector.

The access regime and the HPPs are designed to protect privacy and promote patient autonomy, whilst also ensuring safe and effective service delivery, and the continued improvement of health services. The HPPs generally apply to:

- All personal information collected in providing a health, mental health, disability, aged care or palliative care service; and
- All health information held by other organisations.

Definitions:

Personal Information:

Personal Information: as it is defined in the Privacy Act 1988 is *information or an opinion about an identified individual, or an individual who is reasonably identifiable*, whether the information/opinion is true or not and whether the information/opinion is recorded in a material form or not.

Personal information may include the following:

- Name
- Address
- Sex
- Age
- Financial details
- Marital status
- Education
- Employment history.

Personal information also includes sensitive information which may include:

- Ethnic origin
- Religious beliefs
- Sexual preferences
- Criminal record.

Health Information:

As it is defined in the Privacy Act it is a particular subset of personal information and refers to the information or an opinion about the health or disability (at any time) of an individual; or an individual's expressed wishes about the future provision of health services; or a health service provided or to be provided to an individual, that is also personal information.

Typically for health service providers, this may include but is not limited to:

- Symptoms
- Examination and test results
- Diagnosis
- Treatment and care information
- Admission and registration information.

Collection of Information:

MHPH collects information from patients/consumers that is necessary to provide health care services. Information will be collected by fair and lawful means.

Often this may include collecting information in regard to health history, family medical and/or family social medical history, ethnic background and current lifestyle.

Only information which is believed to be required to provide a comprehensive service will be collected and will occur only after certain criteria are met:

- The patient consents (willingly providing information is usually sufficient to imply consent to collection of information), or
- The collection is required, authorised or permitted by law or law enforcement purposes, or
- The information is received through an appropriate disclosure by another health service provider with the patient's consent, or
- The collection is necessary to prevent or lessen a serious threat to life, health or safety of the individual or public

Quality of Information:
MHPH will take reasonable steps to ensure that patient/customer personal information which may be collected or disclosed is accurate, complete and up-to-date.

What is the impact when health information is not provided:
When health information is inaccurate, incomplete or withheld, the hospital may not be able to provide the patient with the services that they are seeking, provide an appropriate level of service and clinical care may be compromised.

Use and Disclosure of Information:
Used among health professionals to provide treatment:
Modern health care practices rely on treatment being provided by a team of health professionals working collaboratively. These may include (but are not limited to):

- Medical Consultants, including a patient's local General Practitioner
- Radiology and pathology providers (inclusive of contracted services)
- Allied Health Care professionals (inclusive of contracted services)
- Hospital employees
- Manufacturers and suppliers of medical equipment/supplies
- Other health service providers.

Health professionals will share health information as part of the process of providing treatment, and will only do this while maintaining confidentiality of all of this information and protecting patient privacy in accordance with the law.

Health information is only disclosed to those health care workers involved in patient treatment.

Primary and directly related secondary purposes:
Along with the provision of patient care, MHPH may collect and disclose personal information in accordance with the Australian Privacy Principles for other directly related purposes. For example:

- To liaise with Medicare, nominated health fund and/or the Department of Veteran's Affairs, and where required provide information to these entities to verify treatment as applicable and as necessary
- In an emergency where life is at risk and patient cannot consent
- To provide necessary follow up treatment or ongoing care
- For internal administrative requirements, including invoicing, billing and account management

- To assist in undertaking risk management, funding, service monitoring, complaints handling, evaluation, quality assurance, accreditation and staff training/education activities
- To address liability indemnity arrangements with insurers, medical defence organisations and lawyers
- For defence of anticipated or existing legal proceedings
- For other purposes required or permitted by law.

Information that is de-identified, ensuring that an individual's identity cannot be ascertained, is not covered by the Health Records Act 2001 and may be used and disclosed without consent.

Unrelated secondary purposes:
Health information will not be used for unrelated secondary purposes, unless with the consent of the patient.

These may include:
- to promote promotional offers and special events
- fundraising
- marketing (either to market this health facility or the product of someone else)
- research and development
- in relation to direct marketing and fundraising, if the consent cannot practically be obtained, marketing may still occur provided that:
- the patient/customer is advised they can be taken off the mailing list at any time
- the patient/customer has not previously asked to be taken off the mailing list
- the health care service clearly displays their contact details in each marketing publication
- any patient/customer can be removed from the mailing list by contacting the Privacy Officer on (03) 5022 2611

CCTV:
MHPH does use camera surveillance systems for the purpose of maintaining the safety and security of its staff, patients, visitors and other attendees to the hospital. The hospital will comply with the Australian Privacy Principles in respect of any personal information collected via this mechanism.

Disclosure of health information:
The disclosure of health information may only be undertaken with the consent of the patient. In general, use or disclosure is permitted for the purpose for which the health information was collected or, otherwise, with the consent of the person to whom it relates.

In the event that a patient is unable to give consent due to incapacity an authorised representative of the patient may. An authorised representative is defined as:
- Immediate family
  a) Parent/child/sibling
  b) Spouse/domestic partner
  c) Member of individual's household who is a relative

d) Person nominated to a health provider by the individual as a person to whom health information may be disclosed (inclusive of a person exercising a power of attorney under an enduring power of attorney).

- Parent in relation to a child
  a) Step parent
  b) Adoptive parent
  c) Foster parent
  d) Guardian
  e) Person who has custody/daily care and control of the child

The hospital may disclose health information about an individual to an immediate family member of the patient if:

- Either –
  - The disclosure is necessary to provide appropriate health services to or care of the individual, or
  - The disclosure is made for compassionate reasons; and
  - The disclosure is limited to the extent reasonable and necessary for the purposes mentioned in point a), and
- The individual is incapable of giving consent to the disclosure, and
- The disclosure is not contrary to any wish –
  - Expressed by the individual before the individual became incapable of giving consent and not changed or withdrawn by the individual before then, and
  - Of which the hospital is aware or could be made aware by taking reasonable steps, and
  - In the case of an immediate family member who is under the age of 18 years, considering the circumstances of the disclosure, the immediate family member has sufficient maturity to receive the information.

Security of Information:
Health information may be stored in hard copy and/or electronically. All reasonable measures are taken to protect personal health information within MHPH. Medical records and computer systems have controlled access (securely stored and password protected).

Health information is retained and disposed of in accordance with the guidelines from the Public Records Office of Victoria.

Security considerations:

- Misuse – personal information is misused if it is used for a purpose that is not permitted by the Privacy Act.
- Interference – occurs when there is an attack on personal information that the hospital holds that interferes with the personal information but does not necessarily modify its content.
- Loss – covers the accidental or inadvertent loss of personal information held by the hospital. This includes the physical loss of personal information (including hard copy documents, computer equipment or portable storage devices containing personal information). Loss may also occur as a result of theft following unauthorised access or modification of personal information or as result of natural disasters (flood, fire or power outrages).

- Unauthorised access – occurs when personal information is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee or independent contractor or unauthorised access by an external third party (e.g. hacking).
- Unauthorised modification – occurs when personal information is altered by someone who is not permitted to do so, or is altered in a way that is not permitted under the Privacy Act.
- Unauthorised disclosure –occurs when personal information is made accessible or visible to others outside of the organisation, and released that information from hospital control in a way that is not permitted by the Privacy Act.

Access to Information:
Patients have a right to have access to the health information which is held in their health record.

An individual may also make a request for some or all of their health information to be made available to another health service provider. The individual may also authorise the other health service provider to make this request on their behalf.

Access can be gained by contacting the Privacy Officer on (03) 50222611 and/or accessing a *Privacy Information Request* form, available from the MHPH Document Index of the Q: drive.

All efforts will be taken to respond to this request within 30 days.

If reasonable and practicable, the hospital will provide the patient/customer with the information in the manner it was requested.

Transfer outside Victoria:
If the health information is required to be sent outside Victoria, including overseas, the patient/customers written consent will first be attempted to be obtained.

If obtaining this consent is not practicable, the information may still be transferred if, as part of the agreement for transfer of that information, the other organisation agrees to comply with Mildura Health Private Hospital's privacy obligations to the patient/customer.

Access may be withheld in the following circumstances:
- providing access would pose a serious threat and imminent threat to the life or health of the person, or
- providing access would have an unreasonable impact on the privacy of others, or
- the information is subject to confidentiality where the person who provided the information to Mildura Health Private Hospital did so on the condition that it remains confidential, or
- the request is vexatious or frivolous, or
- the information relates to legal proceedings between Mildura Health Private Hospital and the information would not be required to be disclosed to a court, or
- Mildura Health Private Hospital is in commercial negotiations with the patient/customer and the information would reveal our intentions, or

- providing access would be unlawful or we are required by law to withhold access, or
- Providing access could prejudice the investigation or detection by our organisation or by a government body of an unlawful activity or some serious or improper conduct.

Where health information is withheld, a summary of that information will be considered in place of full access.

Written reasons:
If health information is withheld, a written explanation for the reasons will be provided.

Third party intermediary:
If health information is withheld, it will be considered whether the provision of access to an independent third party will meet both the needs of the patient/customer and Mildura Health Private Hospital.

Correction of Information:
Patients may request an amendment to their health record should they believe that it contains and are able to establish that the information is inaccurate, incomplete, misleading or not up-to-date.

MHPH will allow access or make the requested changes unless there is a reason under the Privacy Act or other relevant law to refuse such access or make the requested changes.

To do so patients/customers may make arrangements to alter/update the record by contacting the Privacy Officer on (03) 50222611.

If MHPH is unable to accommodate the patient/customer's request to correct the personal information, then it will provide the individual with a written notice outlining a) the reasons for the refusal and b) the mechanisms available to complain about the refusal.

Openness:
All patients are provided with information on how to contact the Privacy Officer(s), at the first point of contact with the hospital.

Identifiers and Anonymity:
A numeric identifier is allocated to each patient that attends MHPH to enable ongoing care and treatment to be provided.

In general, it is impracticable for MHPH to provide healthcare to individuals anonymously.

Modifications to the privacy policy of Mildura Health Private Hospital:
Mildura Health Private Hospital reserves the right to modify this policy at any time with reference to constitutional law. These modifications will be made available as they occur.

Information relating to Students (Nursing, Medical and Work Experience):
All students who come into contact with, or have access to confidential information have a responsibility to maintain the privacy, confidentiality and security of that information.

Confidential information may include information relating to:

- Patients and/or family members – such as medical records, conversations and financial information
- Employees, contractors, volunteers, students – such as salaries, employment records, disciplinary actions
- Business information – such as financial records, reports, memos, contracts, computer programs, technology
- Third Parties – such as vendor contracts, computer programs, technology
- Operations improvement, quality improvement, risk management, peer review – such as reports, presentations, survey results.

The information included in this policy is relevant to all personnel involved in patient care / hospital related business.

The following are examples only. They do not include all possible breaches of privacy, confidentiality or security covered by this agreement.

<u>Accessing information that you do not need to know to perform your role:</u>

- Unauthorised reading of a patient's medical record or an employee or student file.
- Random searching of the hospital's patient databases (ie DXC WebPas, Genie, Best Practice, TrendCare, etc) for familiar names and details, such as phone numbers.
- Accessing information on self, family, friends, co-workers / colleagues / classmates.

<u>Divulging personal information without the individual's consent:</u>

- Discussing or *gossiping* about patient details in situations unrelated to direct patient care.
- Telling a relative or friend about a patient, student or staff member you have seen.
- Discussing confidential information in a public area such as a waiting room, public corridor or dining room.

<u>Sharing, copying or changing information without proper authorisation:</u>

- Making unauthorised changes to a patient's medical record.
- Making unauthorised changes to an employee or student file.
- Copying and forwarding patient, student or staff information to a third party without having verbal or written consent.

<u>Disclosing patient information without following Mildura Health Private Hospital guidelines:</u>

- Faxing without including an appropriate fax cover sheet that includes a disclaimer.
- Sending unsecured emails.

- Sending information to home computers via email.

Notifiable Data Breach:
The National Data Breach (NDB) scheme introduced an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. Examples of harm include:

- Financial fraud including unauthorised credit card transactions or credit fraud
- Identity theft causing financial loss or emotional and physiological harm
- Family violence
- Physical harm or intimidation.

The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm.

This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (*Commissioner*) must also be notified of eligible data breaches.

A data breach occurs when personal information that MHPH holds is subject to unauthorised access or disclosure, or is lost. A breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems. Examples may include:

- Loss or theft of physical devices or paper records that contain personal information
- Unauthorised access to personal information by an employee
- Inadvertent disclosure of personal information due to human error e.g. email sent to wrong person
- Disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by MHPH
- This is likely to result in serious harm to any of the individuals to whom the information relates
- MHPH has been unable to prevent the likely risk of serious harm with remedial action.

Notifications in regard to an eligible data breach to the Commissioner is lodged through the Notifiable Data Breach statement form (link below):

https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

Information in regard to the MHPH NDB scheme response is in accordance with the following flowchart (link below):

https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/flowchart.pdf

Consideration should also be given to other mandatory or voluntary reporting schemes including:

- Financial service providers
- Police or law enforcement bodies
- Australian Securities and Investments Securities (ASIC)
- Australian Prudential Regulation Authority (APRA)
- Australian Taxation Office (ATO)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Cyber Security Centre (ACSC)
- Australian Digital Health Agency (ADHA)
- Department of Health
- Professional associations and regulatory bodies
- Insurance providers.

Privacy Complaints:

1. All patients are given information on how to contact the Privacy Officer(s), at the first point of contact with the hospital.

2. Staff receiving a verbal complaint should contact the area Manager who will directly address the complaint and notify the Privacy Officer. Depending on the severity of the complaint it may be prudent to notify the Privacy Officer to deal with the complaint when first received.

3. The Director of Clinical Services should be informed of the privacy breach as soon as possible after it has occurred.

4. Written complaints in relation to privacy are forwarded directly to the Privacy Officer.

5. The Privacy Officer will conduct a full investigation of the complaint which will include feedback to the complainant. Relevant documentation of the investigation and outcomes are registered in the hospital's RiskMan Feedback module and maintained by the Director of Clinical Services in collaboration with the Quality Coordinator.

6. A summary of complaints is included in the Safety and Quality report which is available to hospital staff and circulated to the Safety and Quality Management committee, Private Hospital Committee, Medical Advisory Committee and Board of Directors.

7. As complaints about interferences with privacy (breaches of Part 5 of the Act or an HPP) are handled by the Health Services Commissioner, Mildura Health Private Hospital recognises that all patients have the right to complain to the office of the Health Services Commissioner. It is anticipated however that initial attempts are made at a local level to resolve the complaint.

8. Contact details for the Health Services Commissioner including health services complaint forms, are available from the Privacy Officer upon request.

Related Policies:	P01-05 Record Management policy
Related Procedures:	PROC01-01-01 Data Breach Response Summary Flowchart
Related Forms:	F01-01-01 Student Privacy, Confidentiality and Security Agreement F01-01-02 Privacy Information Request form F01-01-03 Privacy Consent F01-14-54 Student Orientation Checklist
References:	Office of Australian Information Commissioner (OAIC)

Revision Date	Revisions Made
January 2021	Document reviewed and added to website
November 2018	Update – inclusion of National Data Breach (NDB) scheme
November 2016	Policy updated