

Risk Assessed = 10**1. Background and Objectives**

The Privacy Act 1988 and the Australian Privacy Principles protect personal information belonging to individuals by placing restrictions on how information may be collected, handled, used and disclosed.

It is the policy and practice of Specialist Surgicentre that all reasonable efforts are made to maintain patient privacy while attending the facility and to ensure all records are kept securely in accordance with applicable privacy principles.

Specialist Surgicentre endeavours to inform patients of their rights by providing a copy of the Privacy Statement prior to admission.

Specialist Surgicentre is bound by the Australian Privacy Principles (Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Privacy Act 1988). Specialist Surgicentre manages personal information in accordance with these principles.

The Australian Information Commissioner has powers under the Privacy Act 1988 and other legislation to make or approve legally binding guidelines and rules. The Office of the Australian Information Commissioner (OAIC) also issues non-binding guidelines and resources to assist agencies, businesses and individuals.

The Australian Privacy Principles can be accessed through the OAIC website.

1.1 NSQHS Standards Alignment

This policy supports compliance with NSQHS Standard 1 – Clinical Governance:

- **Action 1.4:** Systems are in place to ensure compliance with legislative and regulatory privacy requirements.
- **Action 1.7:** Risk management processes are used to protect consumers from harm related to misuse of personal information.
- **Action 1.8:** Processes are in place to identify, report, investigate, and manage privacy and data breaches.

2. Scope

This policy applies to the collection, storage, use, disclosure and management of personal and sensitive information held by Specialist Surgicentre.

This policy applies to:

- Chief Executive Officer (CEO)
- Director of Nursing (DON)
- Administration Staff
- Nursing Staff
- Visiting Medical Officers (VMOs)
- Other staff and contractors as appropriate

3. Definitions

Personal Information: Information or an opinion about an identified individual or an individual who is reasonably identifiable, whether true or not, and whether recorded in material form or not. In effect, it is information or an opinion that can identify a person, for example, their name, physical description, address, date of birth, sex, phone number, email address, driver's licence number and information about their employer/place of work, salary and employment, business activities, investments, assets and liabilities, or any combination of these.

PP40 Privacy			Author: Quality Manager		UNCONTROLLED WHEN DOWNLOADED	
	Approval: BOM	Last Review: JAN 2026	Next Review: JAN 2029		Owner: DON	Page 1 of 4

Privacy Policy and Procedure - PP40

Sensitive Information: Information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political, trade or professional association or trade union, religious or philosophical beliefs, sexual orientation or practices, criminal record, or health information (including genetic and biometric information).

4. Patient Information Held

Specialist Surgicentre holds the following information in relation to its patients:

- Name
- Personal and postal address
- Next of Kin
- Telephone numbers
- Email address
- Date of birth
- Medical history
- Treatment plans and treatment details

The purpose of collecting this information is to enable medical, nursing, and administrative staff to provide safe, effective, and appropriate care and to support the operational requirements of the facility.

5. Manner of Collection

Information is collected either directly from the patient or via the patient's treating practitioner.

6. Storage and Data Protection

Personal information is contained within hardcopy medical records and may be scanned following completion.

Electronic patient information is stored securely on the organisation's server.

Hardcopy and electronic records are accessible only to authorised personnel who require access for the performance of their duties. All authorised personnel have signed Privacy and Confidentiality Statements, binding them to comply with the National Privacy Principles.

7. Access to Records *(To be read in conjunction with PP-04 Managing Medical Records)*

Patients may request access to their personal information by submitting a written request to the Director of Nursing. A reason for the request is not required.

The patient will be notified when the record is available for viewing at the facility. Verification of identity will be undertaken prior to access being provided.

Requests should be forwarded to:

Director of Nursing
Specialist Surgicentre
Suite 15
200 Malop Street
Geelong VIC 3220

PP40 Privacy			Author: Quality Manager		UNCONTROLLED WHEN DOWNLOADED	
	Approval: BOM	Last Review: JAN 2026	Next Review: JAN 2029		Owner: DON	Page 2 of 4

8. Amendment of Records

If a person believes that personal information held by Specialist Surgicentre is incorrect, incomplete, or inaccurate, they may request an amendment.

Specialist Surgicentre will consider whether the information requires amendment. If the organisation does not agree that amendment is required, and the individual requests, a statement from the individual outlining why the information is not accurate or up to date will be attached to the record.

9. Privacy Breaches

A privacy breach occurs where Specialist Surgicentre breaches:

- Its legal obligations relating to the collection, handling, use, storage, or disclosure of personal information; or
- The provisions of this Privacy Policy and associated procedures.

All actual or suspected privacy breaches must be reported immediately to the Director of Nursing.

10. Eligible Data Breaches

An eligible data breach occurs where:

- There is unauthorised access to or disclosure of personal information; or
- Personal information is lost in circumstances where unauthorised access to or disclosure is likely; and the breach is reasonably likely to result in serious harm to an individual.

Serious harm may include physical, psychological, emotional, financial, or reputational harm.

Eligible data breaches are managed in accordance with the Notifiable Data Breaches (NDB) Scheme.

11. National Data Breach Obligations

The Notifiable Data Breaches scheme applies to all business activities undertaken by Specialist Surgicentre.

Examples of potential data breaches include:

- Hardcopy documents containing patient or organisational information left unattended
- Incorrect emailing or faxing of patient information
- Missing or misplaced medical records

All staff are required to remain vigilant at all times in relation to information security.

12. Data Breach Response Plan

Privacy breaches and eligible data breaches are managed in accordance with WI-40-01 Data Breach Flow Chart and the Incident, Issue and Improvement Reporting (IIIR) system.

Where a breach occurs:

PP40 Privacy			Author: Quality Manager		UNCONTROLLED WHEN DOWNLOADED	
	Approval: BOM	Last Review: JAN 2026	Next Review: JAN 2029		Owner: DON	Page 3 of 4

Privacy Policy and Procedure - PP40

1. The breach is contained and a preliminary assessment is undertaken using the IIIR system within 24 hours.
2. The Director of Nursing is notified immediately.
3. Relevant information is collected to support investigation and response as soon as practicable.

13. Monitoring and Compliance

Compliance with this policy is monitored through internal audits and quality activities.

Any identified issues are managed through the Incident, Issue and Improvement Reporting (IIIR) system.

14. Records and Documents

Document	Format	Location	Retention	Access
Patient Records	P / E	Medical Wizard / Administration	7 years	Authorised staff
WI-40-01 Data Breach Flow Chart	E	Dropbox	Life of document	DON / ANUM

15. References

- Privacy Act 1988 (Cth)
- Australian Privacy Principles
- National Safety and Quality Health Service Standards, Version 2
- Health Services (Private Hospitals and Day Procedure Centres) Regulations 2024
- Department of Health Victoria – Rights and Privacy
- Office of the Australian Information Commissioner (OAIC)