Privacy – Policy and Procedure-40

Policy Risk Assessed = (10)

BACKGROUND AND OBJECTIVES

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

Privacy Compliance

It is the policy and practice of Specialist Surgicentre is that all efforts will be made to maintain patient privacy while attending the Centre and all records are kept securely in accordance with privacy principles.
Specialist Surgicentre endeavors to inform patients of their rights by providing a copy of the privacy statement to patients prior to admission to the hospital.
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 deals with personal information in accordance with such principles. The Australian Information Commissioner has powers under the ***Privacy Act 1988*** and other legislation to make or approve legally binding guidelines and rules. These are legislative instruments and are generally required under the ***Legislative Instruments Act 2003*** to be registered and published on the Federal Register of Legislative Instruments and tabled in the Parliament.
To assist agencies, businesses and individuals, the Office of the Australian Information Commissioner (OAIC) also issues non-binding guidelines, which can be found on the **Advisory privacy guidelines** page, and resources for **agencies** and **organisations**.
The Australian Privacy Principles can be obtained through the website of the OAIC – Privacy fact sheet 17

WHAT IS PERSONAL INFORMATION?

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable. It does not matter whether it is true or whether it is oral or in writing.

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.

Sensitive personal information is information or an opinion about a person's racial or ethnic origin, political opinions, membership of a political, trade or professional association or a trade union, religious or philosophical beliefs or affiliations, sexual preferences, criminal record or health information (including biometric and genetic information).

Patient Information

Specialist Surgicentre holds the following information with respect to its patients.

- Name
- Personal address
- Postal address
- Next of Kin
- Telephone numbers
- Fax number
- Date of birth
- E-mail address
- Medical History
- Treatment plan and treatment details

The purpose of the above information is to assist the Staff – Medical, Nursing and Administrative, to carry out the operation of the hospital which is dedicated to the care and general welfare of patients referred to the facility for treatment, and to enable the facility to treat patients effectively.

Manner of collection

Information is collected from patients through the provision of information on their behalf by their treating practitioner or directly from the patient

Storage and data protection

Personal information about patients is contained in a hard copy medical history file and may be scanned on completion. Electronic information concerning patients is stored securely on the server.
Hard copy and electronic records are only accessible to authorized personnel of the facility who require access to such personal information for the purpose of carrying out their duties. All authorized personnel have signed Privacy and Confidentiality statements binding them to comply with the National Privacy Principles.

Access to records. **(This document to be used in conjunction with PP04 Managing Medical Records)**

Patients of the Specialist Surgicentre may request access to personal information by writing to the Privacy Officer. Persons entitled to access do not have to provide a reason for requesting access. The patient will be notified when their record will be available for personal viewing at the hospital.
Applications should be made in writing. Verification will be made prior to response.
Applications should be forwarded to:
The Privacy Officer
Specialist Surgicentre
Suite 15
200 Malop Street
Geelong VIC 3220

Comment

- To acknowledge and take seriously all comments and feedback made by patients and consumers.
- To discuss any concerns, questions, provide feedback or make complaints about issues related to the services provided to you, the processes involved with the service provision and any treatment undergone at Specialist Surgicentre.

Patients Responsibilities

- To participate and cooperate with an agreed treatment and care program or inform staff of your intention not to comply.
- To be considerate of staff and other patients, treating them with courtesy and respect.
- To provide the relevant information about your health, to assist the staff involved in your care, including the possibility of infectious diseases.
- To inform staff if you are covered by any special benefits/ schemes.
- To contribute to a safe and comfortable environment in relation to noise, alcohol, smoking and illicit drugs.
- Consider your ability to meet your financial obligations to pay any accounts and fees for which you are responsible
- To advise Specialist Surgicentre if you are unable to keep an appointment within at least 24 hours notice.

Informed Consent

Specialist Surgicentre has mechanisms in place to align the information provided with the patient's capacity to understand such as:

- Arranging for a guardian/carer to attend pre-admission and admission if the patient is intellectually disabled.
- Having available a clinical staff member or interpreter to communicate with patients whose first language is not English

The compliance and assessment of the processes for informed consent are reviewed through internal surveillance system audits and external audits. The IIIR System to monitor serve exception is used to document the process and action taken to reduce any identified risk.
Specialist Surgicentre has developed and maintained a system of informed consent through planned management processes such as:

- Development and implementation of a website inclusive of patient information
- Consent for Treatment Form.
- Patient discharge information form.
- The patient survey monitors patient feedback.

Privacy – Policy and Procedure-40

Privacy

It is the policy and practice of Specialist Surgicentre that all efforts will be made to maintain patient privacy while attending the hospital and all records are kept securely in accordance with privacy principles.
Specialist Surgicentre endeavors to inform patients of their rights by providing a copy of the privacy policy to patients prior to admission to the hospital.

Privacy Compliance

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 deals with personal information in accordance with such principles. The Australian Information Commissioner has powers under the ***Privacy Act 1988*** and other legislation to make or approve legally binding guidelines and rules. These are legislative instruments and are generally required under the ***Legislative Instruments Act 2003*** to be registered and published on the Federal Register of Legislative Instruments and tabled in the Parliament.
To assist agencies, businesses and individuals, the Office of the Australian Information Commissioner (OAIC) also issues non-binding guidelines, which can be found on the **Advisory privacy guidelines** page, and resources for **agencies** and **organisations**.
The Australian Privacy Principles can be obtained through the website of the OAIC – Privacy fact sheet 17

Patient Information

Specialist Surgicentre holds the following information with respect to its patients.

- Name
- Personal address
- Postal address
- Next of Kin
- Telephone numbers
- Fax number
- Date of birth
- E-mail address
- Medical History
- Treatment plan and treatment details

The purpose of the above information is to assist the Staff – Medical, Nursing and Administrative, to carry out the operation of the hospital which is dedicated to the care and general welfare of patients referred to the facility for treatment, and to enable the facility to treat patients effectively.

If a person believes that information held by the hospital is incorrect, incomplete or inaccurate they may request amendment of that personal information. The hospital will consider if the information requires amendment. If the hospital does not agree that there is any ground for amendment it will, if the person seeking the amendment requires, place with that person's personal information, a statement from that person as to why the information is not accurate or up to date.
If patients wish to obtain access to or notify any changes to their details kept at the hospital, they should contact the Privacy Officer for a copy of the protocol to gain access to records.

WHAT IS A PRIVACY BREACH?

A privacy breach occurs if we hold personal information about an individual and breach:

- Our legal obligations in relation to its collection, handling, use or disclosure;
- The provisions of our Privacy Policy and Procedure

When you identify an actual or possible privacy breach, report it to the Privacy Officer immediately.

WHAT IS AN ELIGIBLE DATA BREACH?

When an 'eligible data breach' occurs, we must usually report it to the OAIC and affected individuals within strict timeframes. However, this may not be required if we act quickly to manage the breach and ensure that it will not cause any serious harm to an individual.

A privacy breach is an eligible data breach if it results in:

- Unauthorised access to or disclosure of personal information
- Information being lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur

And this is reasonably likely to result in serious harm to an individual.

What is serious harm?

Serious harm can include identity theft and serious physical, psychological, emotional, financial or reputational harm.

Some kinds of personal information breaches are more likely than others to cause serious harm e.g. those that involve sensitive information such as medical or health information, information or documents commonly used for identity theft (e.g. Medicare details, driers licence or passport information) or financial information. Combinations of different types of personal information (as opposed to a single piece of information) may be more likely to result in serious harm.

National Data Breach

The NDB laws are an extension of the Privacy Act and cover the entire of business activities at Specialist Surgicentre Facilities.
The following may be included in breaching the National Data Breach laws:
Any hard copy document containing any patient or the facilities private information left in an unsupervised area.
Emailing or faxing patient information to the wrong practice or patient
A missing file
There are no set 'rules' to identifying a data breach within a day hospital, however Security should be at the forefront of peoples' minds at all times.

In terms of the IT there are a few items that may assist to reduce the risk of data breaches:

- Set a password change interval for staff logons
- Require complex passwords with special characters (eg. @$&) and a minimum of 6 characters.
- Limit Remote Desktop user accounts - currently in place for the Remote Desktop server.
- Ensure 'Remote Desktop Gateway' secured with an SSL Certificate for Remote Desktop access, as this is a key source of hacking attempts.
- Remind staff regularly not to click on suspicious emails and/or websites, particularly when new are employed
- Limit access to the server to IT consultant

Data breaches world wide are increasing at an alarming rate. Refer to:
https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/quarterly-statistics-report-january-2018-march-2018

All staff are aware of security of paper waste. Staff ensure all identifiable documents are placed in the labeled container provided and shredded at the end of each day.

See WI-40-01 for Specialist Surgicentre Data Breach Work Instruction Flow Chart

DATA BREACH RESPONSE PLAN

Our privacy Officer will investigate and deal with privacy breaches in accordance with the following Data Breach Response plan.

Data Breach Occurs		
Step	**Action**	**Timeframe** (Do not delete or amend these timeframes)
1	**Contain the breach and do a preliminary assessment using the IIIR system**	Within 24 hours of identification of breach

	• Take immediate steps to contain breach	
2	**Notify the privacy officer, DON immediately**	Immediately following identification of breach
3	**Collect all relevant data in preparation for privacy officer, DON**	As soon as practicable

Monitoring and compliance

Records management including patient files is regularly assessed and audited in order to maintain compliance with relevant regulatory authorities and best practice standards.
Risk assessment of records management including patient files was undertaken initially to establish facility standards. Compliance with the policy standard is monitored through the internal audit schedule and any issues raised are addressed in accordance with IIIR procedure.

Documents and records needed for this procedure, and how are they stored.

Document Title/Form Number	Paper or Electronic	Where are they kept	How long	Access restrictions	Comments
Patient Record	P/E	On Medical Wizard In administration area	7years	Authorised staff	
Staff files	P/E	In executive office/Dropbox	Life of Doc	DON/NUM	
Business Documents	P/E	In executive office/Dropbox	Life of Doc	CEO/DOC	
WI-40-01 Flow Chart	E	Dropbox	Life of DOC	DON/PO	

References

Information Privacy Act 2000 V021 2008
National Safety and Quality Health Service Standards V2
AS NZS ISO 9001:2015 Quality Management Systems - Requirements
Health Services (Private Hospitals and Day Procedure Centres) Regulations 2018
Data Breach information The Fold Compliance Pty Ltd www.thefoldlegal.com.au/product-licence-terms-conditions