

1. Purpose

Stawell Regional Health is committed to protecting the privacy of patient, resident and staff information.

Stawell Regional Health is required to comply with Victorian legislation relating to confidentiality and privacy, including, where relevant, the Health Services Act 1988 (Vic), the Health Records Act 2001 (Vic), Information Privacy Act 2000, Freedom of Information Act 1982, Privacy Act 1988 and the Australian Privacy Principles.

This policy outlines the management of information at Stawell Regional Health to satisfy the requirements of this legislation. This policy is available to anyone who asks for further details on our information handling practices and is available on the Stawell Regional Health website and intranet.

2. Outcome

- To ensure the privacy and confidentiality of all patient, resident and staff information in accordance with current legislation.
- The confidentiality of health information is maintained and personal information is collected, accessed and released in accordance with relevant legislation and only to the extent necessary to perform the functions of an individual's role.

3. Target audience

All staff including students, volunteers, consumer representatives, board members and contractors.

4. Definitions

- **Patient:** refers to inpatient / resident / ambulatory care recipient/community care client
- **Confidentiality:** is the right of an individual to not have personally identifiable information disclosed to others without that individual's consent
- **Privacy:** is the right of an individual to have personal information used only for authorised purposes, with the information protected from misuse as well as unauthorised disclosure
- **Consent:** voluntary agreement of the individual or the individual's legally authorised representative regarding a proposed action, either express or implied, in writing or documented verbal consent
- **Disclosure:** the release of information to another party within and outside Stawell Regional Health, either in written, electronic or verbal form
- **Patient information:** includes but is not limited to any information identifying the patient such as name, date of birth and address details, information contained in the medical record, services provided, patient account details or computerised reports and also includes any subjective information such as opinions that may have been formed about a patient.

Examples of patient information include:

- Patient name, address and phone number
- Health Care Records
- Patient lists
- Registers
- Patient based computerised reports
- Patient account details
- Dictation tapes
- Other patient related documents which identifies individuals
- **Personal Information:** staff personal details, staff phone numbers, personnel files, staff contracts of employment.

- **SRH:** Stawell Regional Health

5. Roles and responsibilities

All staff including students, volunteers, consumer representatives, board members and contractors must ensure they are aware of and maintain the requirements relating to the confidential handling of patient and staff information.

Department Managers are responsible for educating staff in their team regarding their requirements for confidentiality and for taking action regarding any breaches.

The Health Information Officer is responsible for ensuring relevant legislation is up to date and for providing advice on the rules governing the access, use and disclosure of health information.

6. Privacy & Confidentiality

SRH will collect only information that is relevant and necessary to perform our functions. Information will be collected directly from the patient unless it is unreasonable or impracticable to do so. If information is collected from another source, patients shall be informed of where information will be collected from and asked for their consent to collect this unless in exceptional circumstances where it is impractical to do so. Information collected should be up to date and accurate.

Health information shall be accessed, used and disclosed only as necessary by authorised staff to the extent required to perform their role and as consented to by the patient. Care must be taken to prevent any unintentional, unauthorised release of patient information such as conversations regarding patients being overheard or information being viewed in a public place. Patients receiving services from Stawell Regional Health will be informed about the use of their personal information, who will have access to this information and their right to access and correct information.

Information should only be used or disclosed for the primary purpose for which it was collected (providing treatment for your current health condition) or a directly related secondary purpose (for billing or payment purposes e.g. your private health fund). Secondary access and disclosure of health information shall only be permitted if the individual has consented or if it is required or authorised by law. Refer to the [Release of Patient Information Policy](#) for information regarding the release of patient information and health care records.

Patients receiving services through Stawell Regional Health will receive a copy of the "Protection and Use of Your Health Information" brochure which outlines key information about the organisation's information handling practices and how a patient can access their information.

Patients, or their legally authorised representative, are required to sign the "Consent/Refusal to Use and Disclose Information" on each occasion of admission or every 12 months if the patient is receiving long term treatment or care e.g. Primary Care services, Community and Complex Care services or Oncology treatment.

SRH may from time to time transfer health information outside Victoria for the purpose of the provision of care or treatment. SRH will only do this with the patient's consent, where we believe the receiving organisation does not breach the Australian Privacy Principles.

Measures are taken to protect our record keeping and computer systems from unauthorised access, improper use, disclosure, unlawful destruction or accidental loss. Systems have controls in place which only allow access to authorised staff members and monitor any unauthorised access.

Patients are able to request access to their information held by Stawell Regional Health as set out in the Freedom of Information Act 1982. For this request, contact Health Information Services on (03)53588614 for further information and application forms.

Confidentiality and Privacy (and associated policy and procedures) are discussed at Corporate Orientation, which all new employees attend. A Privacy, Confidentiality and Security Agreement shall be signed by all staff, volunteers, consumer representatives, students and board members and any contractors or suppliers of services at the commencement of employment at Stawell Regional Health. Staff requiring access to the Stawell Medical Centre electronic patient record are required to consent to, and sign the Stawell Medical Centre Computer Information Security Policy. Failure to comply with these agreements may result in the termination of their position.

Any concerns regarding privacy or confidentiality should be referred to the Chief Executive Officer. More information regarding this process is available in the "Protection and use of your health information" brochure (see appendices).

7. Exceptions (authorised breaches)/Emergency Disclosure

Patient information may be disclosed without the consent of the patient where there is a serious risk to the individual or to the public. In this situation refer to the [Release of Patient Information Policy](#).

Patient information may be disclosed without the consent of the patient if required by law. For requests for access to information in relation to Children Protection services, Subpoenas, Coroners' requests and Notifiable Diseases, refer to the [Release of Patient Information Policy](#).

8. Evaluation

Any breaches observed shall be reported to the Department Manager and the incident logged in Victorian Health Incident Management System (VHIMS).

All staff are subject to disciplinary action if found to have breached this policy, including written warning or instant dismissal in the case of a serious breach.

Privacy Audits shall be conducted to monitor unauthorised breaches of patient and staff information.

9. Partnering with consumers

Consumers are informed of the organisations' process for maintaining privacy and confidentiality in the "Protection and use of your health information" brochure.

Consumers are informed of their right to access this policy and how to access this policy in the "Protection and use of your health information" brochure.

The "Protection and use of your health information" brochure receives consumer feedback.

Consumers are asked to provide their consent or refusal to use and disclose their information at the commencement of their care.

10. Appendices

[Appendix 1. Protection and Use of your Health Information Brochure](#)

[Appendix 2. Privacy, Confidentiality & Security Agreement](#)

11. Related Documents

[Freedom of Information Policy](#)

Management of Health Care Records policy

[Personnel Files Policy](#)

[Release of Patient Information Policy](#)

Stawell Medical Centre Computer Information Security Policy

12. References

- Children, Youth and Families Act (2005)
- Freedom of Information Act (1982), including amendments
- Health Services Act 1988 (Vic)
- Health Records Act 2001 (Vic)
- Privacy Act (1988) including the Australian Privacy Principles
- Victorian Information Privacy Act (2000)

13. Accreditation

14. Contributors

	Name	Position	Service / Program
Lead Reviewer:	Michelle Cahill	Health Information Officer	
Contributors:	Sarah Warren	Quality Manager	
Committee/s:	Health Information Committee		24/8/17

Protecting your Privacy



*Protection and use of your health
information*



Respecting your privacy

At Stawell Regional Health we respect your privacy. All staff are committed to the protection of your personal and health information in accordance with the Australian Privacy Principles (APPs) contained in the Commonwealth Privacy Act 1988.

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

Can you deal with us without providing your name?

Where it is lawful and practical to do so, you may deal with us anonymously or use an alias or assumed name (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?

When you attend Stawell Regional Health, doctors, nurses and other health care professionals need to collect information about you (e.g. name, date of birth, gender, address, Medicare and health insurance details, medical history, emergency contact details), including information on your condition and treatment outcomes whilst in hospital. This information is important for planning your treatment and discharge. A health record is created for every new patient and every time you attend the health service new information is added to your health record.



How do we collect this information?

We will collect personal information directly from you where it is reasonably practical to do so. This may take place when you attend Stawell Regional Health and complete documents such as an admission form, or provide information over the phone. We may also collect your personal information from third parties if required, such as:

- a responsible person or representative (e.g. guardian) when you are incapable or cannot communicate, unless you have requested otherwise
- your General Practitioner, including any specialists
- a health professional who has treated you
- your health insurer or other insurer
- your family
- other sources where necessary to provide our services (e.g. for blood tests or x-rays)

We only collect your personal information, either directly or from a third party, with your individual consent, which may be implied or express, depending on the circumstances. You will be provided with the 'Consent to Use and Disclose Information' form for completion prior to your hospital admission.

Why do we collect this information?

We need to collect and keep this information to provide you with suitable health care. Your health record is a source of information for the professionals involved in your care to enable them to treat and advise you appropriately.

Some information may also be used for research and planning purposes in order to provide better health outcomes for the whole community. In this case, any identifying information, such as your name and contact details, shall be removed before the information is used



How is your information stored and protected?

We store your personal and health information in both paper and electronic form. Stawell Regional Health maintains strict policy and protocol to protect your information from misuse, interference and loss, and from unauthorised access, modification or disclosure. Methods used to ensure this include:

- requirement of all staff to be bound by a strict legal duty of confidentiality
- strict document storage security
- imposing strict security measures for access to our computer systems
- providing a discreet environment for confidential discussions; and
- allowing access to personal information only when the individual seeking access to their 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 and confidential manner. Generally, your medical record is kept for 15 years after the date of last attendance, whilst certain information is required to be retained permanently.

Who has access to your information?

Stawell Regional Health staff work together for your benefit and your health information is shared among those health professionals in your treating team.

It may also be necessary for Stawell Regional Health to use some of your information for other administrative purposes related to your hospital admission. These may include:

- Contact with external service providers involved with your care, for example pathology services.
- For billing and payment purposes if applicable, for example Medicare, health insurance, Work Cover, Transport Accident Commission, Department of Veterans Affairs.
- Other hospitals - Hospitals within the Grampians region are moving to a shared electronic medical record. This means that if you attend more than one hospital within the region, clinicians involved in your care will be able to access your health information from these hospitals within the one medical record. This will assist in providing better services to you.

The following hospitals are involved in the Regional Electronic Medical Record:

Ballarat Health Services
Beaufort & Skipton Health Service
East Grampians Health Service
West Wimmera Health Service
Wimmera Healthcare Group

Hepburn Health Service
Rural Northwest Health
East Wimmera Health Service
Edenhope & District Memorial Hospital

If you are referred to another hospital, healthcare provider or community service, necessary information will be shared to arrange services and help continue your care.

Who else may request access to information about me?

After you are discharged we may notify your local doctor so that they are aware of your treatment and any special instructions related to your care. If you do not want this information to be sent to your doctor please let us know before you are discharged.

Sometimes your local doctor may contact us for additional information about your treatment. In this case, we may give them further information. If you do not want this to occur please let us know as soon as possible.

Authorised church representatives visit the hospital. If you wish to be included on the individual churches visiting list, please indicate your religion on the admission form.

Visiting Specialists

Overseas disclosure of personal information

We will not disclose any information about you to an overseas recipient without both your consent, or without being satisfied that the overseas recipient will collect, hold, use, disclose, and protect the information supplied under substantially similar requirements to those specified within the Australian Commonwealth Privacy Act 1988.

When can information be given to other agencies without my consent?

There are very few situations when information may be shared without your consent. For example, in an emergency situation, information may need to be released about you to aid emergency treatment.

In some circumstances, we are legally obliged to provide information about you. Examples include.

- where your records have been subpoenaed for a court case
- providing health records to a law enforcement agency (e.g. Police) in response to a search warrant
- reporting of notifiable diseases as appropriate and
- investigation of a complaint by the Office of the Health Services Commissioner or the Aged Care Complaints Investigation Scheme.

Research, Teaching and Quality

Stawell Regional Health may use some of your health information for the purposes of research or statistical analysis, or to evaluate and monitor the health care services we provide. Information used for these purposes will be d-identified. Satisfaction questionnaires are often distributed to patients/residents after discharge as part of our quality program.

By signing the 'Consent to Use and Disclosure of Information' form, you indicate your consent to the use of your information for these purposes. If you do not wish for this to occur it can be indicated on the form.

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

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

We also take reasonable steps to correct the information we hold if we are satisfied that it is inaccurate, incomplete, out of date, irrelevant or misleading, or if an individual asks us to correct their 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 you:



- let us know if there are any errors in your personal information
- keep us up-to-date with changes to your personal information (e.g. name and address). You may do this by mail or email using the information provided below.

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

We want to keep you informed about us

SRH Public Relations/Fundraising Department provides support to purchase equipment and enhance services for patients. They would like to send you information on the work they do. Your decision to receive this information is obtained on the 'Consent to Use and Disclosure of Information' form.

We will only use personal information for direct marketing and promotional activities with your express consent. All direct marketing communications will include the option for you to opt out of receiving direct marketing communication. You can opt out at any time.

Accessing your Health Record

You have the right to request access to your Health Record held by Stawell Regional Health through the Freedom of Information Act (1982). Requests for access to your medical record must be made to the Freedom of Information Officer. There is an application fee with additional charges for photocopying.

If you would like more information about any of Stawell Regional Health's health information policies or the Freedom of Information Act please call Health Information Services on 5358 8614 or ask a nurse to contact them for you.



Complaints

If you have a complaint that concerns privacy or confidentiality, you may contact the Senior Nurse on duty or the Chief Executive Officer.

Another option is to contact the Office of the Health Services Commissioner, an independent government funded authority on 1300 582 113. You may also contact the Aged Care Complaints Scheme on free call 1800 550 552.

A copy of Stawell Regional Health's privacy policy can be provided to you upon request, and is also accessible on the Stawell Regional Health website at www.srh.org.au

Our contact details

Stawell Regional Health
Sloane Street
Stawell Vic. 3380
Telephone: 5358 8500
Fax: 5358 8649
Email: info@srh.org.au

Last Rev: 08/2015

Information in this brochure is referenced to the:
Commonwealth Privacy Act (1988)
Health Records Act (2001)
Information Privacy Act (2000)
Freedom of Information Act (1982)
Public Record Office of Victoria, Retention
and Disposal Authority for Patient Information
Records (2011)

Sloane Street
Stawell Vic. 3380
Telephone: (03) 5358 8500
Facsimile: (03) 5358 3553
Website: <http://www.srh.org.au>
S:\baces\Flyers\Health Information\2016-1-8
Respecting your Privacy DraftV5.doc





PRIVACY, CONFIDENTIALITY & SECURITY AGREEMENT

**(For all persons associated with SRH,
including, contractors, volunteers, board members
and students)**

Issued: June 2002 updated September 2017

Stawell Regional Health is committed to ensuring our organisation complies with relevant privacy, confidentiality and security legislation—to protect our clients; our staff; and our organisation. As part of this, individuals are required to understand their obligations and responsibilities including what it means to sign this agreement.

All persons, including, contractors, volunteers and 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 ASSURANCE, PEER REVIEW
Such as reports, presentations, survey results.

All Staff are required to abide by the Privacy, Confidentiality and Security procedures of Stawell Regional Health. Staff are encouraged to make themselves aware of the content of the following documents and the impact they have on their role.

These policies are available on the SRH Intranet Site, and include specifically:

- [Privacy and Confidentiality Policy](#)
- [Release of Information Protocol](#)
- [Management of Health Care Records Protocol](#)
- [Security Policies](#)
- [Personnel Files Policy](#)
- [Social Media Policy](#)
- [Information Management and General Disposal Schedule](#)
- [Disposal of Health Care Records Protocol](#)
- [Freedom of Information Policy](#)

Further Information

If you have any questions or concerns relating to privacy, confidentiality or security of information whilst at Stawell Regional Health contact:

Health Information Services
Stawell Regional Health
Phone: (03) 5358 8614
Fax: (03) 5358 8520
Email: info@srh.org.au

Examples of Breaches (WHAT YOU SHOULD NOT DO!)

NOTE: These are examples only. They do not include all possible breaches of privacy, confidentiality or security covered by this agreement. Staff should read and understand relevant Stawell Regional Health's policies and procedures. These are listed with this agreement and can be accessed via SRH Intranet.

Accessing information that you do not need to know to do your job:

- Unauthorised reading of a your own record, a patient's medical record or an employee file.
- Random searching of Patient Master Index for familiar names.
- Accessing information on family, friends or co-workers.
- Reading pathology results of yourself, family, friends or co-workers.

Divulging personal information without individual's consent:

- Discussing or "gossiping" about patient details in situations unrelated to direct patient care.
- Conducting a conversation relating to patient or staff information in a public place.
- Telling a relative or friend about a patient or staff member you had seen.
- Discussing confidential information in a public forum.
- Leaving information unsecured in an office or public space.

Sharing, copying or changing information without proper authorisation:

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

Acknowledgement to Women's & Children's Health.

Sharing your password:

- Telling a co-worker your password so that they can access your work.
- Telling an unauthorised person the access codes for employee files or patient accounts.
- Using unauthorised shared passwords.

Using another person's password:

- Using a co-worker's password to log in to the Hospital's computer system.
- Unauthorised use of a password to access employee files or patient accounts.
- Using a co-worker's application for which you do not have rights after he/she is logged in.

Disclosing patient information without following SRH Guidelines:

- Disclosing patient details to an organisation/individual that the patient has refused.

Leaving a secure information system (ie System that is password protected) unattended while logged on:

- Being away from your desk (eg. Tea or lunch breaks) while you are logged into a secure system.
- Allowing a co-worker to use a secure system for which he/she does not have access after you have logged in.

Privacy, Confidentiality and Security Agreement

As part of my position/employment I am required to understand and comply with the laws, regulations, procedures and policies of Stawell Regional Health relating to Privacy, confidentiality and security:

1. I will comply with, and seek information relating to specific laws, regulations, procedures and policies of Stawell Regional Health.
2. I WILL ONLY access information I need to do my job.
3. I WILL NOT disclose, copy, release, sell, alter or destroy any confidential information unless it is part of my role., whereby I will follow the correct procedures.
4. I WILL NOT disclose my personal computer passwords and will only use shared passwords in authorised situations.
5. I ACCEPT responsibility for all activities undertaken using my password.
6. I KNOW that my access to confidential information may be audited.
7. I WILL NOT remove confidential information (eg. Medical records, photocopied patient forms or electronic data) from SRH unless it is an authorised work practice.
8. I WILL report any activities to my manager that I suspect may compromise the confidentiality of information. I understand these reports, made in good faith, will be held in confidence to the extent permitted by law.
9. I WILL wear my SRH identification badge at all times whilst on SRH premises.
10. I WILL protect the privacy of SRH patients and employees.
11. I AM RESPONSIBLE for my use or misuse of confidential information.
12. I UNDERSTAND my obligations under this Agreement will continue after termination of my employment.

I am aware that failure to comply with this agreement may result in the termination of my position/employment at Stawell Regional Health and/or civil or criminal legal penalties may result.

By signing this, I agree that I have read, understand and will comply with this agreement.

Signature: _____

Date: _____

Print Name: _____

Department: _____

COPY 1—to be signed and held by employee

COPY 2—to be signed and held in employee record within Human Resources