	SEYMOUR HEALTH Title: **PRIVACY POLICY** Scope: Organistion wide Responsible Department: Executive Authorised by: Executive

PURPOSE

This policy provides the organisation with the framework necessary for ensuring the privacy of information provided to Seymour Health by all clients and patients. Seymour Health is obliged to abide by the Information Privacy Principal contained within both the Health record Act 2001 (Vic) and the Information and Privacy Act 2000(Vic).

This policy addresses the collection, use and disclosure, quality, security and data retention, access and correction of personal and health information.

POLICY

Principle 1 - Purpose of Collection of Personal Information

Personal information must only be collected by Seymour Health if the information collected is relevant for:

- a lawful purpose connected with a function or activity of Seymour Health
- a lawful purpose connected with providing a service to an individual or the community
- This purpose has been clearly and precisely defined by Seymour Health
- Is limited to necessary, relevant information for the stated purpose

Principle 2 - Source of Personal Information

Seymour Health when collecting personal information must collect the information directly from the individual concerned or their authorised representative.
It is not necessary for Seymour Health to comply with Principle 2 (1) if:

- The individual (or representative) has authorised the collection of information from another person or organisation, having been made aware of the matters set out in Principle 3 (1)
- The individual is unable to provide the information directly, or authorise the collection of information from another person or organisation, because of age, intellectual disability, mental illness, medical condition or some other recognised condition or circumstance
- Compliance would prejudice the health, welfare and safety of the individual, any other individual or the community

Non-compliance is necessary for:

- The maintenance of the law by any public sector agency including the prevention, detection, investigation, prosecution and punishment of offences
- The protection of the public revenue
- The conduct of proceedings before any court or tribunal
- The collection from a person other than the individual concerned is required or authorised by law

Principle 3 - Providing Notification when Personal Information is collected

When Seymour Health collects personal information directly from an individual, or from the individual's representative, Seymour Health must take reasonable steps to ensure that the individual (or representative) is aware:

- that the information is being collected
- the purpose for which the information is being collected
- whether or not the supply of information is legally required
- of the consequences (if any) if all or part of the requested information is not provided
- of any other persons or organisations to whom information may be disclosed of the rights of access to, and correction of, personal information
- of any legal obligation which Seymour Health has to provide details to relevant authorities

It is not necessary for the Seymour Health to comply with the information is being collected if -

- compliance would prejudice the health, welfare and safety of the individual, any other individual or the community

Non-compliance is necessary for:

- the maintenance of the law, including the prevention, detection, investigation, prosecution and punishment of offences
- the protection of the public revenue
- the conduct of proceedings before any court or tribunal
- If, due to changed circumstances, the exceptions under Principle 3 (2) no longer apply, then Seymour Health will make the provisions of Principle 3 (1) known to the individual (or representative) as soon as practicable

Principle 4 - Manner of Collection of Personal Information

Personal information shall be collected by Seymour Health by

- lawful means
- means that are appropriate to the service provided
- not unreasonably intrusive
- Sensitive to the individual's circumstances, including cultural awareness

Principle 5 - Storage, Security and Transmission of Personal Information

Seymour Health holding personal information must ensure that the information is protected, by security safeguards appropriate to its sensitivity, against:

- loss
- Inadvertent access, destruction, use, modification or disclosure; and other misuse
- That, if it is necessary for Seymour Health to disclose personal information to another person and/or organisation, that person and/or organisation must comply with the applicable State or Federal Privacy Legislation, and by way of provision of a Privacy Policy. Adequate security safeguards must protect the transmission of information.
- Seymour Health shall designate an individual or individuals who are responsible for the organisation's compliance with the Department of Human Services prescribed Privacy Principles

Principle 6 - Maintaining a Policy of Openness

Seymour Health involved in the collection, storage and use of personal information shall make readily available to individuals, specific information about its policies and practices relating to the management of personal information.

Principle 7 - Right of Access to Personal Information

Where Seymour Health holds personal information about an individual, then this individual is entitled to:

- obtain from the Seymour Health confirmation of whether or not the organisation holds this information
- obtain access to their information

Where an individual is given access to personal information, under Principle 7 (1b), the individual must be advised that under Principle 8 they may request correction of the information. The application of Principle 7 (1) and (2) are subject to applicable provisions of relevant legislation where Seymour Health is not required to grant an individual access to their personal information:

- Where a request for access, alteration or deletion of personal information is not granted to an individual, Seymour Health refusing this request, must provide reasons for the denial and advise the individual of any further action the individual can take

Refusal of access to information may occur where the information:

- is prohibitively costly to provide
- relates to investigations or potential court action
- would be likely to endanger the physical or mental health of the person making the request or any other person

Seymour Health shall acknowledge all requests for access to personal information as soon as practicable. Seymour Health shall also notify an individual of any charges that are required to service the request.

Principle 8 - Correction and Accuracy of Personal Information

Where Seymour Health holds personal information about an individual, then this individual is entitled to:

- request correction of the information
- request that there be attached to the information a statement of any request made but refused
- Dissent from or add to any opinion, diagnosis or assessment. The individuals may request that their own comments be attached as an addendum to the record, where this attachment is technologically possible
- As the holder of personal information, Seymour Health must, if so requested or on its own initiative, take such steps to correct the information as is reasonable, to ensure that the purpose for which the information may lawfully be used and for the period in which the information is stored, it is:
  - accurate
  - up-to-date
  - complete
  - Not misleading

- Where Seymour Health, the holder of personal information, is not willing to correct the information in accordance with a request, Seymour Health must, if so requested, take reasonable steps to attach to the information, in such a manner that it will always be read with the information, any statement provided by the individual of the correction sought
- Where Seymour Health has taken steps under Principle 8 (2) or (3), Seymour Health must, if reasonably practicable, inform each person or body or agency to which the personal information has been disclosed of those steps
- Where Seymour Health receives a request made under clause (1), Seymour Hospital must inform the individual concerned of the action taken as a result of the request

Principle 9 - Retention and Disposal of Personal Information

- Unless there is a legal requirement for Seymour Health to retain personal information, such information must not be kept for longer than is required for the purposes for which the information was collected or any directly related purpose
- Information retained will be archived in such a manner that facilitates ease of retrieval in the event that either the individual, or the individual's representative, or Seymour Health seeks access to this information
- Where personal information held is no longer required under Principle 9 (1), it is to be disposed of in a secure manner

Principle 10 - Limits on Use and Disclosure of Personal Information

Seymour Health holding personal information shall only use or disclose this information where:

- the use or disclosure of the information is for a purpose for which the information was originally collected or a directly related purpose
- the use or disclosure is authorised by the individual concerned or the individual's authorised representative where the individual is deceased, or unable to give his or her authority under this rule due to age, intellectual disability, mental illness, medical condition or some other recognised condition
- the use or disclosure is necessary to prevent or lessen a serious and imminent threat to:
- public health, welfare or safety
- the health, welfare or safety of the individual concerned or another individual
- the use or disclosure is necessary for:
- the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences
- the protection of the public revenue
- the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonable in contemplation)
- improving the health, welfare or safety of the community where the use or disclosure is authorised by an appropriate ethics committee
- the use or disclosure is required or authorised by law

Principle 11 - Unique Identifiers

- Seymour Health shall only assign a unique identifier to an individual if the assignment of that identifier is necessary to enable Seymour Health to carry out any one or more of its functions efficiently and to ensure the health, safety or welfare of its patients
- Seymour Health in assigning unique identifiers to an individual must take steps to ensure that unique identifiers are assigned to only those individuals whose identity is clearly established through the collection of other pieces of relevant information
- Unique identifiers should not be used by multiple organisations or for multiple purposes in a manner, which fails to meet the privacy protection standards established in these Principles
- When seeking a service from Seymour Health it should not be compulsory for an individual to provide a unique identifier unless it is required or authorised by law or unless it is in connection with a purpose (or directly related purpose) for which the identifier was assigned

Key Aligned Documents

Confidentiality Policy
http://system.prompt.org.au/download/document.aspx?id=13464161&code=8476FB8E9AABC6CB2C595506E006DB85

Persona File access policy
http://system.prompt.org.au/download/document.aspx?id=13464009&code=0CBF0D3C03FB0E4A9EB9F268F66911E4

Key Legislation, Acts & Standards

- Australian Commission on Safety and Quality in Health Care (October 2012) - National Safety and Quality Service Standards – Standard 1.19.2
- Accident Compensation Act 1985 (Vic)
- Health Records Act (Victoria) 2001 (Vic)
- Health Services Act (Victoria) 1988 (Vic)
- Information Privacy Act (Victoria) 2001

References

Kilmore District Hospital (2014) Privacy Policy
http://system.prompt.org.au/download/document.aspx?id=10994684&code=563CD60F0EB7F2EE8A77E7E54A9DB494

Author/Contributors

Name	Position	Service / Program
Sandy West	HIM	Kilmore Hospital
Debra Bourne	DQSD	Executive

Reviewed by

Committee	Date
Leadership and Management	20 November 2014

Approved by

Name & Position	Signature	Date
C. McDonnell – CEO		25 November 2014