Privacy Policy Framework

issued under the Privacy Policy Directive

Version No.: V2.0
Approval date: 15/05/2019

Government of South Australia
SA Health

Contents

1. Introduction

It is critical that SA Health ensures that the right to privacy for people who come into contact with SA Health is respected and that all personal information that SA Health holds is secure and protected from unauthorised access or misuse.

Providing services in the area of health involves handling large quantities of personal information that is often highly sensitive. SA Health has an obligation to ensure that any personal information that it collects, or is collected on its behalf, is used, disclosed and stored in accordance with all relevant legislative and policy requirements.

1.1 Purpose and Objectives

The purpose of this Privacy Policy Framework is to provide detailed information on the Information Privacy Principles outlined in section 4 of the Privacy Policy Directive. These principles are based on the legislative and policy requirements that apply to SA Health for the collection, storage, use and disclosure of personal information.

The Framework also provides information on other matters where questions are frequently raised e.g. clinical photography and the use and disclosure for personal information for research and training.

1.2 Scope

The Information Privacy Principles outlined in the Privacy Policy Directive and this Framework apply to all personal information collected and stored by SA Health, and its subsequent use and disclosure.

Who do the Information Privacy Principles apply to?

The Information Privacy Principles outlined in the Privacy Policy Directive and this Framework apply to all persons who are engaged with SA Health (including the Department for Health and Wellbeing, SA Ambulance Service and the Local Health Networks [LHNs]), including employees, members of governing boards, contractors, volunteers and other health service providers who, in the course of their work, have access to personal information collected, used or stored by, or on behalf of, SA Health.

While the brand name of SA Health is used in this Framework, it is the responsibility of the Department, each LHN and SA Ambulance Service to ensure that appropriate processes and procedures are in place within their organisation to meet the requirements of this Framework.

What information is covered?

Personal information means information or an opinion, whether true or not, relating to a person, or the affairs of a person, whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

There is no clear legal authority as to whether a deceased person is considered a person or an individual under privacy legislation, and for this reason it is recommended that SA Health errs on the side of caution and applies the same protection to information relating to a deceased person.

The Privacy Policy Directive and this Framework applies to personal information regardless of its format e.g. paper or electronic records such as videos, x-rays, photographs, specimens, entries on computer databases (including patient administration systems) and emails or other electronic messaging systems. This includes information from which the names and addresses have been removed but where sufficient information remains so that the individual could potentially be identified (e.g. by way of a number, reference or details which, when combined with other information, can be related to an individual).

The Information Privacy Principles do not apply to de-identified information where all identifiers have been removed or altered to the extent that there is no possibility of identifying or linking it back to the person's identity.

A note on the *Commonwealth Privacy Act 1988*

Generally, the Commonwealth *Privacy Act 1988* ***does not*** apply to the South Australian public sector. This Act is limited to the regulation of the Commonwealth public sector and the private sector in South Australia including non-government organisations, private hospitals and health practitioners in private practice. Its provisions relating to personal information therefore do not apply to SA Health and should not be relied upon.

Health care providers practising in both the public sector and private sector (including co-located public and private hospitals) will be required to comply with the Privacy Policy Directive while in the public sector and the *Commonwealth Privacy Act 1988* when working in the private sector. Which requirement applies depends on who holds the records. For example, if the provider works in a public hospital, the record will be managed by the hospital and covered by the requirements of the Privacy Policy Directive. If the records are retained for the private practice then those records will be covered by the Commonwealth Act.

Where private sector and non-government organisations are contracted by SA Health, the provisions in the Privacy Policy Directive will apply. Where the requirements outlined in the Privacy Policy Directive differ from those imposed under the Commonwealth legislation, these providers are encouraged to seek legal advice.

However, for the purposes of data breaches involving tax file number (TFN) information, SA Health is brought under the Commonwealth *Privacy Act 1988* and any such breaches must be reported to the Office of the Australian Information Commissioner (refer to Section 13 for more information).

1.3 Roles and Responsibilities

All persons that the Privacy Policy Directive and this Framework applies to have an obligation to:

- only access personal information that they need to perform their duties
- protect the privacy and confidentiality of personal information that they may collect or hold
- not disclose personal information without legal authority
- not disclose their computer passwords
- accept responsibility for all activities undertaken using their password
- not remove confidential information from the workplace unless authorised.

1.4 Information Privacy Principles

The South Australian Government protects personal information that it holds through an administrative scheme consisting of the Information Privacy Principles Instruction (issued as Department of the Premier and Cabinet Circular No. PC012) and the Privacy Committee of South Australia. This administrative scheme applies across all public sector agencies, including SA Health.

The Information Privacy Principles (IPPs) govern the way that public sector agencies collect, store, use, disclose, access and correct personal information. However, SA Health has legislative requirements under the section 93 of the *Health Care Act 2008* and section 106 of the *Mental Health Act 2009* that take precedent over the Information Privacy Principle covering the disclosure of personal information. These legislative requirements are outlined under Section 7 of this Framework. All SA Health staff and other persons that fall within the scope of the Privacy Policy Directive and this Framework are required to comply with the legislative requirements for the disclosure of personal information. Under the legislation it is an offence to disclose personal information without a lawful authority and may attract a monetary penalty and/or disciplinary action or termination of a contract.

Under the Information Privacy Principles Instruction it is permissible for the Privacy Committee of South Australia to grant an exemption from the IPPs for a particular purpose and on such grounds as the Committee sees fit.

While the Committee may provide an exemption for the collection, storage or use of personal information, it is unable to grant an exemption for the disclosure of personal information.

Any exemption from the Information Privacy Principles in the first instance should be discussed with the Safety, Quality and Risk Management Unit (or equivalent within the LHN or SA Ambulance Service), or the

Corporate Affairs Unit within the Department for Health and Wellbeing, email: HealthLegalRequests@sa.gov.au.

How the IPPs apply to SA Health is discussed below. While the brand name of SA Health is used in this Framework, it is the responsibility of the Department, each LHN and SA Ambulance Service to ensure that appropriate processes and procedures are in place within their organisation to meet the requirements of each IPP.

2. Collection of Personal Information

IPP1: Personal information should not be collected by unlawful or unfair means, nor should it be collected unnecessarily.

Personal information may be collected by SA Health by a variety of means including verbally or in writing.

Unlawful methods of collecting personal information may include:

- computer hacking, telephone interception or listening device without a warrant, or an act of discrimination
- trespassing on private property or threatening a person in order to obtain information.

Unfair methods of collecting personal information may include the use of intimidation or deception or methods of information collection that are unreasonably intrusive.

There may be some circumstances where the covert collection of information by surveillance or other means involving a level of deception, may not be considered "unfair". Examples would include investigations of possible fraud or other unlawful activities.

In other circumstances it may be necessary to collect information in a manner that could be considered intrusive, even though the information is being collected by lawful means e.g. collecting highly sensitive information relating to a suspected victim of child abuse without the consent of the child or guardian. In this situation, the relevant legislative provisions prescribing this collection would apply.

The overriding intent is to ensure that the intrusive nature of the collection is limited to that which is necessary to gather the relevant information.

When collecting personal information it is important to be sensitive, and take all reasonable steps to minimise intrusion on the individual from whom the personal information is being collected. This requires awareness and consideration of any contextual factors and/or influences, such as ethnic and cultural background, and the physical surroundings where the information collection occurs.

What personal information is collected

SA Health has a broad role in protecting and improving the health of all South Australians by providing leadership in health reform, public health services, health and clinical research, policy development and planning, with a focus on wellbeing, illness prevention, early intervention and quality care. This inevitably means that SA Health holds a considerable amount of personal information to enable it to provide services or fulfil a particular function.

The onus is on SA Health to justify why personal information is collected from individuals for the purpose of providing a particular service or fulfilling a particular function. For example, collecting details of a patient's income is unlikely to be necessary for the provision of public health services. However, collection of information about pensioner or veteran status may be necessary if this information impacts on patient entitlements.

Where SA Health receives personal information that it has taken no active steps to collect (i.e. ***unsolicited personal information***) a determination needs to be made about whether the information is necessary for SA Health's functions or activities and whether SA Health could have otherwise collected the information by fair and lawful means.

If it is determined that SA Health ***could have collected the information*** it must be treated in accordance with the Privacy Policy Directive as if SA Health did collect the information.
If SA Health ***could not have collected the information*** it must, as far as it is lawful and reasonable, destroy the information (subject to the *State Records Act 1997)* or ensure that it is de-identified.

IPP2: An agency that collects personal information should take reasonable steps to ensure that, before it collects it or, if that is not practicable, as soon as practicable after it collects it, the record-subject is told:

(a) the purpose for which the information is being collected (the "purpose of collection"), unless that purpose is obvious;

(b) if the collection of the information is authorised or required by or under law – that the collection of the information is so authorised or required; and

(c) in general terms, of its usual practices with respect to disclosure of personal information of the kind collected.

It is important that SA Health is open and transparent about the collection and management of personal information. This includes ensuring that an individual is adequately informed about why and how their personal information is being collected, and to whom it will be disclosed.

The individual should be made aware of these matters at the time that the personal information is collected. If this is not practicable, reasonable steps should be taken to ensure the individual is notified, or made aware, as soon as practicable after the collection.

An individual may be notified or made aware of the collection of personal information through a variety of formats provided that the matters are expressed clearly. Where personal information is collected verbally the individual could be provided with a brochure or other written material, with staff providing a brief overview. Where personal information is collected in writing this could be incorporated into the document that is used to capture the information or made available via an accessible link.

Determining the appropriate measures to inform individuals about the collection of their personal information should take into account any special needs of the individual e.g. age, where English is the second language, or disability.

Why personal information is being collected (the purpose of the collection)
In most cases the purpose for SA Health's collection of personal information (the primary purpose) will be obvious e.g. to provide a health service. In these circumstances it may not be necessary to advise the individual about why their information is being collected. In other instances the purpose of the collection may be inferred from a particular function or activity, e.g. the title of a form.

At times, further information may be requested from an individual in addition to that to provide a particular service. In these situations the individual should be told why that additional information is being sought. For example, it could be to improve the quality of care provided, or to assist in planning and/or research activities. Wherever practicable, the individual should be given a genuine choice about whether or not they wish to supply these additional details. (Note that where the information is collected to fulfil a legal requirement no such choice can be offered. However, the individual should still be informed that the information is being collected for this purpose.)

Is the collection required or authorised by law?
Wherever possible an individual should be informed about any requirement under law for the collection of personal information. The person should be advised of the name of the law (or other statutory provision) that authorises the collection of their personal information.

Consequences of personal information not being collected
Where an individual chooses not to provide all, or some, of their personal information they need to be made aware of any consequences of this decision. It is not necessary to describe all of the possible or remote consequences or those that would be obvious to a reasonable person. Instead, significant consequences that could be expected to result should be described, e.g. an application for a benefit or allowance is unable to be processed, a complaint cannot be properly investigated, not all information is available for medical treatment.

In some situations an individual may not have an option to determine what personal information may be collected, e.g. where it is required by law or where it is an offence under law not to provide the information. Under these circumstances the individual should be informed about this requirement and the purpose of the collection.

Disclosure of personal information
When collecting personal information, SA Health is required to take reasonable steps to advise the individual of usual practices regarding the disclosure of information to third parties.

This does not require SA Health to advise that a particular disclosure has occurred or will occur. Rather it requires SA Health to notify or ensure awareness of its ***usual*** practices in disclosing personal information to other entities.

Part 7 of this Framework provides guidance on the disclosure of personal information by SA Health pursuant to legislative requirements.

IPP3: An agency should not collect personal information that is inaccurate or, having regard to the purpose of collection, is irrelevant, out of date, incomplete or excessively personal.

SA Health must take reasonable steps to ensure that the personal information it collects is relevant to the purpose of the collection, and not excessively personal. The personal information collected should also be complete and up-to-date.

3. Storage of Personal Information

IPP4: An agency should take such steps as are, in the circumstances, reasonable to ensure that personal information in its possession or under its control is securely stored and is not misused.

Personal information constitutes an official record under the *State Records Act 1997*. If it is no longer required for the purpose for which it was collected it must be stored or destroyed in accordance with the *State Records Act 1997*.

Reasonable steps to safeguard personal information could include:

- ***physical measures*** – locked filing cabinets, clear desk policies and restricted access to offices
- ***organisational measures*** – policies, procedures and guidelines e.g. *Acceptable Use Policy*, and the training and education of staff in the handling of personal information
- ***technological measures*** – the following policies should be adhered to:
    - SA Health ***ICT Security Policy*** – access to computers should be via a personal user identifier. Computer users are accountable for all actions performed under their own personal identifiers. Users should ensure that access to their computer is secured when it is unattended e.g. by lockable screen savers. Under no circumstances should personal user identifiers and passwords be shared.
    - SA Health ***User Access Specification*** – permits the use of generic accounts where there is a significant cost, productivity or service level impact on business operations with the use of individual user accounts. Generic accounts are only allowed access to the network, they are not permitted access to patient administration systems or to where any other patient data is recorded or stored, such as shared folders. Generic accounts should be kept to a minimum with appropriate measures adopted to ensure the integrity of the account e.g. frequently changing the password.

      User identifiers should only be established with appropriate authorisation. This may be in the form of a contract of employment or other agreement as well as authorisation by an appropriate requester. This particularly applies to the use of applications that are not generally available across SA Health.

User identifiers should be reviewed on a regular basis. User identifiers no longer required must be deleted as soon as practicable.

- SA Health ***Electronic Communications Policy*** – the use of personal devices and services for the activities of SA Health is not permitted without prior management approval.

  Where a personal device is used SA Health staff need to:
  (a) be aware of the surrounding environment when they access personal information on an approved personal device
  (b) ensure the personal device is secured by a password and where possible suitable encryption is applied to the device.

- SA Health ***Email Specification*** – business emails must not be forwarded to personal email addresses. Email external to SA Government is not a secure environment and communications may be subject to unauthorised data interception or monitoring by a third party. This is particularly important where an email may contain sensitive or confidential personal information. Message encryption should be used where possible when emailing sensitive or personal information to another entity.

- SA Health's ***Information Security Policy*** – all information is classified for the purpose of determining the security and handling requirements to ensure that it is protected appropriately. Personal health information is deemed highly sensitive and as such requires high levels of protection and must not be copied or saved in another form outside the SA Health secure electronic environment.

  SA Health staff must not:

  (a) put any information about another individual obtained through their employment with SA Health on any online social medium e.g. Facebook, Twitter, LinkedIn, Myspace, Tumblr or any blogs (either personal or open)
  (b) use online software services e.g. *Google Docs* or *Dropbox* to compile, edit or distribute personal information
  (c) use online software initiatives to collect personal information without consent e.g. SurveyMonkey
  (d) duplicate or save any personal information in another form outside the SA Health secure electronic environment.

  Even where an individual has given consent for their personal information to be stored via these resources, consideration needs to be given to the access and security of these platforms.

4. Access to Personal Information

IPP5: Where an agency has in its possession or under its control records of personal information, the record-subject should be entitled to have access to those records in accordance with the Freedom of Information Act 1991.

The *Freedom of Information Act 1991* (FOI Act) provides a legally enforceable framework for individuals to access their personal information that may be held by SA Health. It also allows SA Health to deny access to certain types of documents. For example, if the information includes the personal information of another person, or there is other legislation that overrides the FOI Act, such as the *Children and Young People (Safety) Act 2017* which requires that any information that would lead to the identity of a notifier must not be disclosed or released.

Section 3(3) of the FOI Act encourages agencies to disclose information where permitted by legislation without requiring an FOI application. Such disclosures will not breach the confidentiality provisions under section 93(3)(b) of the *Health Care Act 2008* or section 106(2)(b) of the *Mental Health Act 2009*.

Requests from an individual to access their personal information should be considered without the need to lodge a request under the FOI Act. However, there may be instances when an application under the FOI Act may be appropriate such as:

(a) when the documents include what may otherwise be exempt material (e.g. relating to the personal affairs of another person or that is subject to secrecy provisions, such as the identity of a notifier under the *Children and Young People (Safety) Act 2017*)
(b) if the application is made by another person without the consent of the individual
(c) when the individual's situation might in some way be particularly sensitive (e.g. if the individual has commenced or is reasonably likely to commence legal proceedings against the health service)
(d) when a medical practitioner or other health practitioner has expressed reservations about the effect on the individual of accessing the documents (in which case section 26(4) of the FOI Act would apply).

When determining access to personal information under the *Health Care Act 2008* or *Mental Health Act 2009* consideration must be given to the information contained in the file as if the request was made under the FOI Act. Disclosure of information that may breach another individual's privacy or secrecy provisions in legislation may expose SA Health to liability.

SA Health should take reasonable steps to give individual's access to their personal information. This may involve talking to the individual to try and work out another way of providing access to their personal information where it meets their needs but does not breach legislative requirements or the privacy of other individuals. This may include giving the individual access to only those documents that provide the information that they need.

If an individual requests access to their personal information under the FOI Act then the application should be processed in accordance with that Act.

5. Correction of Personal Information

IPP6: An agency that has in its possession or under its control records of personal information about another person should correct it so far as it is inaccurate or, having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, incomplete, irrelevant, out of date, or where it would give a misleading impression in accordance with the Freedom of Information Act 1991.

It is important to take reasonable steps to ensure that the personal information that SA Health holds is accurate, up to date and complete. This information privacy principle operates alongside and does not replace the legislative provisions of the FOI Act that provide for an individual to request a correction or amendment to personal information that may be held by SA Health.

Upon request, SA Health would, under normal circumstances, inform the individual of whether or not SA Health holds personal information about them. When doing so, SA Health should also notify the individual of the mechanisms in place to facilitate access to this information and how they may request correction of the information.

Generally the routine updating of personal information, e.g. contact details, would not be considered to require an application to be made by the individual under the FOI Act.

However, it should be noted that under the FOI Act, where an agency refuses to amend a record upon an individual's request, the individual may ask for a notation to be put on the record.

In some situations, it might be necessary for SA Health to keep a record of what was known or understood at a particular time - the information a particular decision was based upon - which would require the retention of information that was incorrect, out-of-date, or misleading e.g. for a Coronial Inquest. Legislative provisions such as the *Evidence Act 1929* may also require that such information be retained.

6. Use of Personal Information

IPP7: Personal information should not be used except for a purpose to which it is relevant.

SA Health will only use personal information for a relevant purpose. In the case of health information, the primary purpose of collecting information is usually to provide a health service to an individual. However, it is generally accepted that in providing a health service to an individual, it may also be necessary to use their information for other related purposes e.g. billing purposes or to improve health services.

The purpose to which an individual's personal information is used should not be a surprise to them. What an individual has been told at the time of the collection of their personal information will help to ascertain what an individual might reasonably expect.

IPP8: Personal information should not be used by an agency for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose (the secondary purpose) unless:

(a) the record-subject would reasonably expect the agency to use the information for the secondary purpose and the secondary purpose is related to the primary purpose of the collection;

(b) the record-subject has expressly or impliedly consented to the use;

(c) the agency using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or of some other person;

(d) the use is required by or under law;

(e) the use for that other purpose is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer;

(f) the agency has reason to suspect that unlawful activity has been, is being or may be engaged in, and discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the agency reasonably believes that the use relates to information about an individual that suggests that the individual has engaged or may engage in illegal conduct or serious misconduct in relation to a person; and

(i) the agency reasonably believes that the use is appropriate in the circumstances; and

(ii) the use complies with any guidelines issued by the Minister for the purpose of this clause.

Note that this information privacy principle only relates to the *use* of personal information *within* SA Health and *not disclosure to a third party* outside of SA Health. The disclosure of personal information outside of SA Health is subject to the legislative provisions outlined under the *Health Care Act 2008* and the *Mental Health Act 2009* as set out in section 7 of this Framework.

SA Health can use personal information for an incidental or related purpose (the secondary purpose) if one or more of the exceptions listed in the principle applies.

Whenever personal information is to be used for a purpose that is not the primary purpose, and is not covered by one of the exceptions, the consent of the individual must be obtained. This allows the individual to control how, and for what purpose, their personal information will be used, and ensures that their privacy is protected.

The use of personal information will vary depending on the:

- purpose e.g. a complaint against a service provider may only require limited personal information to be disclosed for an investigation
- type of information e.g. for sensitive information (which includes health information) the use or disclosure must be ***directly related*** to the primary purpose.

While personal information may be collected for the provision of a health service (the primary purpose), it is possible that it may be used for secondary purposes that may be directly related to this purpose such as:

- sending reminders where the person requires a follow-up service
- using information for quality assurance or clinical audit activities

- using the information to investigate complaints about care provided
- administrative activities associated with providing, following up on or receiving payment for a service.

While an individual may have an expectation that their personal information may be used for these purposes, consideration needs to be given to special requests that their information is not used.

Where personal information may be used for other purposes where it would not be appropriate to gain the consent of the individual, e.g. if there is a belief that the individual may be engaged in unlawful activity, illegal conduct or serious misconduct, the use is to be limited to that which is necessary to enforce the law, conduct an investigation, take disciplinary action or report the unlawful activity.

IPP9: An agency that uses personal information should take reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up-to-date.

SA Health must take reasonable steps to ensure that the use of the personal information is relevant to the purpose of collection, and that it is accurate, complete and up-to-date.

7. Disclosure of Personal Information

All persons that fall within the scope of the Privacy Policy Directive must not disclose personal information unless authorised or required to by an exemption specified in this section. The unauthorised disclosure of personal information is an offence under the *Health Care Act 2008* and the *Mental Health Act 2009*. These offences carry penalties of $10,000 and $25,000 respectively. There may also be disciplinary action taken.

Under sections 93 of the *Health Care Act 2008* and section 106 of the *Mental Health Act 2009* any person engaged in the public health system (i.e. persons employed or otherwise engaged by SA Health e.g. contractors), or any person formerly engaged in the public health system, must not disclose information related to another person unless certain criteria are met.

The disclosure of personal information under the Acts can only occur where:

7.1 ***The disclosure is authorised or required to be disclosed by the Chief Executive of SA Health or the Chief Executive Officer of the Local Health Network or SA Ambulance Service, or delegate*** [section 93(2) of the *Health Care Act 2008* or section 106(1) of the *Mental Health Act 2009]*

The Chief Executive of SA Health has issued "blanket" authorisations for SA Health staff to disclose personal information to other agencies in the following circumstances (this list is not exhaustive):

- under specific Government initiatives to protect persons from harm e.g. Family Safety Framework, Multi Agency Protection Services (MAPS) Project and the Information Sharing Guidelines (ISGs)
- in order to assist the Coroner when investigating a death
- in order to assist the Crown Solicitor's Office when representing SA Health.

Further information on the "blanket" authorisations is provided in section 4 of Appendix 1 of this Framework.

The Chief Executive of SA Health and Chief Executive Officers of the LHNs and SA Ambulance Service can authorise the disclosure of personal information on an ad hoc basis where there may be doubt as to whether the disclosure fits any of the criteria in section 93(3) of the *Health Care Act 2008* or section 106(2) of the *Mental Health Act 2009* outlined below.

If you require an authorisation, in the first instance contact the Risk Manager (or equivalent) within the LHN or SA Ambulance Service. The Corporate Affairs Unit within the Department for Health and Wellbeing may also be contacted. Any proposed blanket authorisation to release personal information should first be discussed with the Corporate Affairs Unit email: HealthLegalRequests@sa.gov.au or telephone 8226 6047.

7.2 ***The disclosure is required by law, or as required for the administration of the Act or a law of another State or Territory of the Commonwealth*** *[*section 93(3)(a) of the *Health Care Act 2008* or section 106(2)(a) of the *Mental Health Act 2009*]

Personal information may be disclosed if it is required or authorised by or under an Australian law or a court/tribunal order. 'Law' includes Commonwealth, state and territory legislation, and the common law.

If the law *requires* the disclosure of personal information then it must be provided. Examples of such requirements include the mandatory reporting of child abuse (under the *Children and Young People (Safety) Act 2017*) or the mandatory notification of certain communicable diseases (under the *South Australian Public Health Act 2011*).

Where the law *authorises* the disclosure of information the decision needs to be made whether to do so: the legal authority exists but there is some discretion as to whether the personal information should be handled in that way.

Note that while another law may require the disclosure of personal information, care should be taken to ensure that the provision of such information does not contravene any other provision under the Act. For example, a subpoena may compel the production of a child's medical record, however, anything that may identify a notifier of suspected or actual child abuse or neglect must not be disclosed.

If in doubt, contact the Safety, Quality and Risk Management Unit (or equivalent) within the LHN or SA Ambulance Service, or the Corporate Affairs Unit within the Department for Health and Wellbeing email: HealthLegalRequests@sa.gov.au.

Appendix 1 contains further information on the laws and SA Health policies and guidelines that refer to disclosure under this exemption.

Section 12 of this Framework includes further advice on personal information that may fall under Parts 7 and 8 of the *Health Care Act 2008* where the disclosure of personal information that may relate to an authorised quality improvement or research activity or the analysis of an adverse incident. The disclosure of personal information under these provisions is not authorised unless the individual that the personal information relates to consents. Parts 7 and 8 override any other provisions in law that may require the disclosure of personal information.

7.3 ***The disclosure is at the request, or with the consent, of the person to whom the information relates or a guardian or medical agent of the person*** *[*section 93(3)(b) of the *Health Care Act 2008* or section 106(2)(b) of the *Mental Health Act 2009*]

The key elements of consent are:

- the individual is adequately ***informed*** before giving consent i.e. there must be reasonable efforts to ensure that the individual has the information they need to understand what they are consenting to, why it is necessary or desirable, and what may be the results both of consenting and of not consenting;
- the consent should be ***reasonably specific***. A general or blanket consent could result in an individual later indicating that they were not informed of the particular usage proposed;
- the consent is ***freely given*** i.e. the individual is not coerced, pressured or intimidated. The individual should not feel that they have no choice or that they do not have enough time to make up their mind;
- the individual has the ***capacity*** to understand and communicate their consent. An individual cannot give consent if they do not have the necessary capacity to do so. Incapacity can be due to age, injury or illness, or physical or mental impairment. While incapacity is a permanent condition for some, it may be a temporary condition for others. If an individual does not have capacity to provide consent a substitute decision maker or authorised representative can give consent on their behalf;
- consent should be ***timely***. The validity of the consent is dependent on the individual's expectation e.g. consent is more likely to be questioned where a lengthy period of time has passed or the individual's personal situation has changed so markedly that there are grounds to suggest that their views may have changed;
- consent should be ***obtained in writing or verbally*** but when obtained should always be recorded e.g. a notation in the individual's file to indicate their specific and clear intention for the disclosure of their personal information.

Implied consent may be acceptable in some circumstances. Implied consent generally means that a person has not given consent verbally or in writing, but through their conduct or behaviour has "implied" consent, or by consenting to one action, they have impliedly consented to a range of other activities. For example, an individual may consent to medical treatment that includes a range of pathology tests. In providing consent to the medical treatment it could be inferred that the individual is also giving an implied consent for any necessary information to be provided to the pathology service provider. The application of implied consent should be limited to what an individual would reasonably expect or think acceptable in the circumstances. The more significant the consequences of a particular disclosure of personal information, the more important it is that express consent is obtained.

Where the personal information relates to a deceased person consent should be sought from the executor of the deceased person's Will, or the deceased person's substitute decision maker, authorised representative, or next of kin.

7.4 ***The disclosure is to a relative, carer or friend of the person to whom the information relates if the disclosure is reasonably required for the treatment, care or rehabilitation of the person, and there is no reason to believe the disclosure would be contrary to the person's best interests*** *[*section 93(3)(c) of the *Health Care Act 2008* or section 106(2)(c) of the *Mental Health Act 2009*]

However, if the disclosure is contrary to any wish expressed by the individual when the individual was capable of providing consent, then the information cannot be disclosed.

The disclosure of personal information must be limited to the extent reasonable and necessary to provide care or treatment to an individual.

Note that in relation to the *Mental Health Act 2009* if the person to whom the information relates is under a community treatment order or inpatient treatment order, their personal information may be released to a relative, carer or friend for the purposes of their treatment, care or rehabilitation even if they do not provide consent, provided that there is no reason to believe that the disclosure would be contrary to the person's interests even if the individual has given an express direction not to disclose the information in this way.

7.5 ***The disclosure is to a health or service provider and the disclosure is reasonably required for the treatment, care or rehabilitation of the person to whom the information relates*** [section 93(3)(d)(i) of the *Health Care Act 2008* or section 106(2)(d)(i) of the *Mental Health Act 2009*]

The disclosure is in the form of personal information entered into an electronic records system established for the purpose of enabling the recording or sharing of information between persons or bodies involved in the provision of health services **[within SA Health and not to a third party]** [section 93(3)(d)(ii) of the *Health Care Act 2008* or section 106(2)(d)(ii) of the *Mental Health Act 2009*]

The disclosure is reasonably required in connection with the management or administration of a hospital or SA Ambulance Service (including for the purposes of charging for a service) [section 93(3)(d)(iii) of the *Health Care Act 2008* or section 106(2)(d)(iii) of the *Mental Health Act 2009*]

As part of providing a health service there may be a directly related purpose that requires an individual's personal information to be disclosed. This may include providing ongoing care, investigating complaints about care provided and undertaking administrative activities associated with their care e.g. receiving payment for a service.

The increasing use of electronic health records also allows greater access to an individual's personal information, some of which may be regarded as sensitive. Access to electronic health records should only be on a need-to-know basis by SA Health staff or persons otherwise engaged by SA Health i.e. where it is necessary for them to undertake a particular role or function that requires access to the record.

It is considered best practice for consent to be obtained from the individual to share their personal information with another health provider. This includes the provision of discharge summaries to the person's primary health provider (e.g. general practitioner). While in most cases an individual may consent to this information being provided, there may be times when the individual does not wish details of treatment to be

disclosed to their primary health provider. SA Health may share personal information with another health provider without the consent of an individual ***if*** it is considered that the disclosure is reasonably required for the ongoing treatment, care or rehabilitation of the person. Any decision to disclose personal information without the consent of the individual should be documented in the individual's file.

7.6 ***The disclosure is reasonably required to lessen or prevent a serious threat to the life, health or safety of a person, or a serious threat to public health or safety*** [section 93(3)(e) of the *Health Care Act 2008* or section 106(2)(e) of the *Mental Health Act 2009*]

While it is considered best practice for consent to be obtained from the individual to share their personal information there may be instances where it is unreasonable or impracticable to obtain consent. This may include where there is a belief that the disclosure is necessary to lessen or prevent a serious threat. Disclosure under this subsection does not necessarily require such a threat to be imminent before action can be taken. It allows for early intervention to prevent such threats escalating to the point of realisation. The onus will be on SA Health to justify its reasonable belief that the disclosure of personal information was necessary to lessen or prevent a serious threat.

A 'serious' threat is one that poses a significant danger to an individual or individuals. This can include a threat to a patient's physical or mental health and safety. It could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. The threat may be to the life, health or safety of any individual and is not limited to the person seeking treatment and care. A 'serious threat to public health or safety" relates to the broader safety concerns affecting a number of people. For example, the potential spread of a communicable disease.

If in doubt contact the Safety, Quality and Risk Management Unit (or equivalent) within the LHN or SA Ambulance Service, or the Corporate Affairs Unit within the Department for Health and Wellbeing email: HealthLegalRequests@sa.gov.au.

7.7 ***The disclosure is for medical or social research purposes if the research methodology has been approved by an ethics committee and there is no reason to believe that the disclosure would be contrary to the person's best interests*** [section 93(3)(f) of the *Health Care Act 2008* or section 106(3)(f) of the *Mental Health Act 2009*]

Further information on the use of personal information for medical, clinical or social research purposes is provided in section 11 of this Framework.

Personal information held by SA Health should not be used to identify individuals for medical or social research i.e. data trawling.

In general only de-identified information should be used for research purposes unless the human research ethics committee has approved otherwise.

8. Clinical Photography

SA Health acknowledges the increased use of mobile devices to take and transmit photographic images as part of providing clinical care. These images can be important for tracking a condition over time (e.g. a lesion), seeking an opinion from a specialist, or for teaching and training purposes.

In accordance with the *State Records Act 1997* any such images are considered as an official record and must be retained and disposed of within the provisions of the Act. Any images taken as part of a function and activity of SA Health are considered to be the property of SA Health even if the image is taken on a device that is not owned by SA Health but authorised to be used for SA Health business.

(Note that in accordance with the Electronic Communication Policy SA Health does not permit the use of personal devices and services for the activities of SA Health without prior management approval.)

Any images taken must be downloaded to the individual's SA Health file (or if this is not possible, an entry is made in the individual's file) and deleted from the personal device as soon as practicable. Leaving clinical

images on a mobile device increases the risk of unauthorised access if the device is lost or stolen, and increases the risk of the image being sent by mistake to an unauthorised third party. Continued use of the device without downloading images also increases the risk of confusion of images between individuals.

It is advisable that a mobile device used for taking clinical images is password protected and that there is the ability to erase images remotely if the device is stolen. Care must also be taken to ensure that any clinical images are not up-loaded to any social media networks or back-up sites that may be publicly available.

The information privacy principles that apply for the collection of personal information apply to the taking of a clinical image i.e.

- the purpose for the image needs to be considered
- the consent of the individual must be obtained (preferably in writing)
- the individual needs to understand the reasons for taking the image, how it will be used and who will have access to it
- the image may only be disclosed in accordance with the *Health Care Act 2008* or the *Mental Health Act 2009*.

Particular consideration needs to be given to the taking of clinical images of children, adults with impaired capacity and intimate areas of the body. Any such images must only be taken for clinical purposes. It also needs to be recognised that some images could be considered pornographic or obscene if taken out of context and could lead to criminal charges.

When seeking consent, the purpose of taking the image should be explained to the individual. If an individual provides consent for the purposes of consulting with a specialist, it does not mean that the image can be used for teaching or research purposes. The image may only be used in accordance with the consent given. It should also be recognised that an individual's consent may change over time.

If an individual does provide consent for their image to be used for teaching or research purposes, consideration must be given to ensuring that the image is de-identified. Features such as tattoos and piercings may still be used to identify an individual. Even when these features are removed, factors such as skin colour or age could lead to an individual being identified in the case of rare conditions. Metadata stored on digital images (e.g. time and date of capture, GPS location) could also lead to the identity of an individual.

9. Anonymity and Pseudonymity

There may be occasions where SA Health is requested by an individual to deal with them anonymously or through the use of a pseudonym.

Anonymity and pseudonymity are important privacy concepts. They enable individuals to exercise greater control over their personal information and decide how much personal information will be shared or revealed to others.

There are many reasons why an individual may wish to remain anonymous or to use a pseudonym including:

- a preference not to be identified or to be 'left alone'
- to keep their whereabouts secret from a former partner or family member
- to access services without this becoming known to others.

The significance of anonymity has increased in response to the increased use and capabilities of technology, including data matching and electronic surveillance, which enables an individual's activities to be monitored.

There may be a range of circumstances where providing services anonymously or under a pseudonym may be impracticable. This could include denying a practitioner access to information that is critical for providing safe and appropriate care or compromising follow-up care if there are no contact details.

In other circumstances it is unlawful to provide a service without obtaining a name if there is a statutory requirement to obtain identifying details or where other requirements relating to the service involve identifying the person to whom it is provided. These could include:

- accessing Medicare benefits (unless Medicare has issued a card under the individual's pseudonym)
- prescriptions for restricted medicines or treatments which must include the name of the person who will receive those medicines or treatments
- where a person has been diagnosed with certain medical conditions listed as notifiable conditions under the *South Australian Public Health Act 2011*, a medical practitioner is required to record certain details, including identity, to allow the matter to be reported to the Chief Public Health Officer.

The use of pseudonyms creates some practical issues for SA Health in matching records between patient systems. These systems rely on demographic data to link patient records. If incorrect information is used an individual may be potentially linked to another individual's record resulting in incorrect clinical data.

Consistent with the *South Australian Client Identification Data Standards* an individual should be registered using their legal name, with their preferred name listed as an alias if different to their legal name. SA Health must take steps to explain to the individual why they may not be dealt with anonymously or under a pseudonym and what safeguards are in place to ensure their privacy. This could include advising the individual that the personal information collected is limited to only that which is necessary to deal with the individual or, in the case of a pseudonym, restricting access to authorised staff only.

10. Use of Government Identifiers

A government related identifier is a number assigned to an individual by a government agency to verify the identity of that individual for the purposes of performing that agency's activities or functions. An identifier may be a number, letter or symbol, or a combination of any or all of these.

While the assignment of a unique identifier does not in itself raise privacy issues, the way in which this identifier is used (or could potentially be used) may raise concerns. The use of unique identifiers could impact on the privacy of an individual by allowing personal information from different sources to be matched and linked in ways that an individual may not agree with or expect.

Consequently, it is best practice to ensure that strict criteria apply to the assignment of unique identifiers (ensuring that it is necessary for a particular purpose) and limitations placed on their subsequent use. These safeguards will minimise the likelihood of personal data being misused or shared in a manner that may be considered inappropriate.

It is therefore not appropriate for SA Health to adopt a government related identifier of an individual issued by another agency as its own identifier unless it is authorised by a court order or law, e.g. SA Health can use an individual healthcare identifier issued by the Commonwealth under the *Healthcare Identifiers Act 2010*.

Unique identifiers may also be used to facilitate the sharing of information between divisions of SA Health, but only where this is considered necessary to enable them to carry out a particular function or activity, and where this activity is carried out in accordance with this policy.

Best practice does not prevent SA Health from recording an identifier of another organisation where necessary for their functions or activities. It only seeks to prevent SA Health from using the identifier as its own. This means that SA Health may still record an identifier issued by another organisation, such as in the process of an identity check (e.g. an individual's Medicare number or a driver's licence number). However, SA Health must not organise the personal information that it holds about that individual under the reference of that number.

Unless required to do so, when evidence of individual identification is required or authorised (including by law) such as a 100-point identity requirement, consideration must be given to whether it is necessary to record the identifier. In some situations it may be sufficient to simply sight the driver's licence or other form of identification.

11. Use and Disclosure of Personal Information for Research and Training

The type and volume of personal information collected by SA Health is valuable for medical, clinical and social research. The disclosure of personal information for these purposes must take into account whether:

- the disclosure is reasonably necessary for the purpose
- de-identified information could be used for the purpose.

In accordance with the *Health Care Act 2008, Mental Health Act 2009* and the *Research Governance Policy Directive* personal information may be used for medical and research purposes only where approval has been given by either an SA Health research ethics committee or a NHMRC certified health research ethics committee under National Mutual Acceptance.

As part of the approval process the research ethics committee will take into account whether the disclosure would be contrary to the person's best interests and determine what information may be disclosed for the purposes of the research.

In general, information used or disclosed for research purposes needs to be de-identified. Generally de-identification includes two steps:

- removing personal identifiers, such as name, address, date of birth or other identifying information
- removing or altering other information that may allow an individual to be identified, e.g. because of a rare characteristic of the individual, or a combination of unique characteristics.

Where de-identified information is not suitable and it is impracticable to seek consent from individuals, then personal information may be used or disclosed provided the research has been approved by a research ethics committee.

Approval from a research ethics committee is only approval for a researcher to receive personal information that SA Health holds. It is not approval for the researcher to be given access to SA health systems or databases. To do this would put SA Health at risk of breaching the Information Privacy Principles which require SA Health to ensure that reasonable steps are taken to ensure that personal information in its possession or under its control is protected from misuse and unauthorised access or disclosure.

The same principle applies to clinical students who use patient information purely for training purposes and not for any treatment purpose. During activities where students are not directly involved in an individual's care or treatment, whenever possible only de-identified information is to be used for teaching purposes. Where the use of identifiable information purely for teaching purposes is unavoidable and justified, wherever possible, the express consent of the individual must be sought.

12. Parts 7 and 8 of the *Health Care Act 2008*

Section 7.2 of this Framework discussed section 93(3)(a) of the *Health Care Act 2008* where a disclosure of personal information could occur if it was required by law, However, the disclosure could not occur if it contravened any other provision under the Act. Parts 7 and 8 of the *Health Care Act 2008* are examples that override any other provisions in law that may require the disclosure of personal information. The disclosure of personal information in accordance with these Parts does not breach any law or principle of professional ethics, or require the consent of the individual.

Part 7 of the Act allows personal information to be provided or released to an authorised person or for an authorised activity for the purpose of improving the quality and safety of a health service or to achieve the best possible outcomes associated with the improvement of health services. The authorisation of the activity or person must be made by the Minister. Examples of current authorisations include clinical cancer registries, quality improvement committees, morbidity and mortality review committees, and incident review panels in health services.

Part 8 of the Act allows the analysis of adverse events for investigation by a root cause analysis (RCA) team to identify issues within the system that contributed to, or resulted in, the occurrence of the adverse incident and to provide recommendations to prevent the recurrence of a similar incident. The types of adverse incidents that this section relates must be gazetted by the Chief Executive, SA Health. On 21 May, 2015 the Chief Executive gazetted classes of incidents that constitute an adverse incident for the purpose of Part 8 of the Act. This includes, but is not limited to, sentinel events, the abduction of an infant from a hospital facility, and homicide or suicide.

In accordance with the Parts 7 and 8 of the *Health Care Act 2008* the disclosure of information or a document that identifies a particular individual is not authorised, even if it is required by law, unless the individual that the information relates to consents.

These provisions are examples in legislation where the disclosure would contravene any other legislative provision requiring the disclosure of personal information.

13. Dealing With Privacy Breaches and Complaints

13.1 **Privacy Breaches**

A data breach occurs when personal information that SA Health may hold is subject to unauthorised access or disclosure, or is lost.

All breaches of privacy e.g. inappropriate access or the unlawful disclosure of personal information, must be recorded in the Safety Learning System in accordance with the *Consumer Feedback Management Policy Directive*. This will ensure that the breach has been formally recorded and for remedial action to be implemented.

In accordance with the *Patient Incident Management and Open Disclosure Policy Directive* any unauthorised or unlawful disclosure of personal information identified by SA Health must be openly disclosed to the individual concerned (or their support persons) and reported in the Safety Learning System.

Data breaches containing personal information must be reported to the Privacy Committee of South Australia as soon as practicable by email: privacy@sa.gov.au in accordance with the Personal Information Data Breaches Guideline. The report should also include what remedial action and what steps have been put in place to prevent a similar breach occurring again.

Any personal data breach that relates to tax file number (TFN) information, and that is likely to result in serious harm to individuals must also be notified to the Office of the Australian Information Commissioner as soon as practicable within 30 days of the breach being discovered via the Notifiable Data Breaches Scheme.

13.2 **Privacy Complaints**

A privacy complaint is where an individual believes that SA Health has not complied with its obligations under the Information Privacy Principles, section 93 of the *Health Care Act 2008*, or section 106 of the *Mental Health Act 2009*.

Complaints about the unlawful sharing of, or access to, personal information may be made direct to SA Health or may be referred in the first instance to entities such as the Health and Community Services Complaints Commissioner, the Ombudsman or the Privacy Committee of South Australia.

Regardless of how a complaint is received, SA Health will be required to justify that it collected, used or disclosed personal information within the legislative, statutory and policy requirements applicable to SA Health or the Information Privacy Principles.

For this reason it is important that appropriate notations are made about decisions in case notes or through other systems e.g. electronic health record or the Safety Learning System, particularly where an individual has given verbal consent or where personal information has been disclosed without consent.

It is equally as important to document why personal information is disclosed as it is to document why a decision was taken not to disclose.

14. Electronic Health Records

The use of electronic health records poses different privacy and security challenges for personal information than paper records. Firstly, it is possible to have a single electronic record accessible at multiple sites, giving more people access. Secondly, it is possible to control access to an electronic record in ways that are not possible with a paper record.

While electronic records provide for sharing of information for better patient care, the requirements of the *Privacy Policy Directive* still apply. SA Health staff should only access the information stored in an electronic health record when it is necessary for them to perform their duties. Systems to audit and ensure compliance with these obligations are critical to reassure the public that their privacy will be protected.

Where electronic health records are in place the following principles should be considered:

- ***Awareness of staff*** about their responsibilities to observe the requirements of the *Privacy Policy Directive*. This can be incorporated into any education and training provided for staff who are able to access and use electronic health records. It can also be incorporated into alerts or notifications in systems where personal information is stored.
- ***Advising patients*** that their personal information will be managed using electronic systems, and that systems are in place to prevent unauthorised access to information held in these systems.
- ***Access to the electronic health record*** is to be via individual user identifiers and passwords; the use of generic accounts is not permissible. This should incorporate the possibility of reports and notifications being generated regarding access to records. Systems should be in place to appropriately manage breaches of access.
- ***Auditing*** on an ongoing basis electronic systems where personal information is stored. This should incorporate the possibility of reports and notifications being generated regarding access to records. Systems should be in place to appropriately manage breaches of access.

15. Associated Policy Directives / Policy Guidelines

Acceptable Use Policy Summary

Consumer Feedback Management Policy Directive

Electronic Communications Policy

Email Specification

Employee Use of Social Media Policy Directive

ICT Security Policy

Information Asset Classification Policy Directive

Information Sharing Guidelines for Promoting Safety and Wellbeing: SA Health ISG Appendix Policy Directive

Media Policy Directive

National Statement on Ethical Conduct in Human Research (National Health and Research Medical Council

Patient and Solicitor Access to Patient Records Standard

Patient Incident Management and Open Disclosure Policy Directive

Protective Security Policy

Police Requests for Information and Witness Statements from SA Health Policy Guideline

Research Ethics Policy Directive

Research Governance Policy Directive

Social Media Communications Policy Directive

Software and Hardware Management Policy

Subpoena and other Legal Requests for Information – guidelines on the law and procedure

User Access Specification

16. Acknowledgements

SA Health acknowledges the work of the Commonwealth Office of the Australian Information Commissioner.

17. Document Ownership & History

Document developed by: Corporate Affairs, Corporate and System Support Services
File / Objective No.: 2014-05861 | A1287782
Next review due: 01/03/2021
Policy history: Is this a new Policy Directive (V1)? **N**
Does this Policy Directive amend or update an existing Policy Directive version? **Y**
If so, which version? V1.0
Does this Policy Directive replace another Policy Directive with a different title? **N**

ISBN No.: 978-1-76083-121-9

Approval Date	Version	Who approved New / Revised Version	Reason for Change
15/05/2019	V2.0	Director, Corporate Affairs	Framework formally reviewed in line with timeframe for review, minor amendments made to section 13 (Dealing with Privacy Breaches and Complaints) and Appendix 2 to update names of Acts.
13/02/2017	V1.0	Portfolio Executive	Original PE approved version.

APPENDIX 1: Glossary of Terms

In the context of this Framework:

agency	*means* a public sector agency as defined in section 3(1) of the *Public Sector Act 2009*. This includes the Department for Health and Wellbeing, SA Ambulance Service and the LHNs, collectively branded as SA Health.
collects	*means* gathering, recording, or acquiring personal information from any source and by any means.
consent	*means* that an individual has authorised their personal information to be used for a defined purpose or handled in a particular manner. Consent may be *expressed* (i.e. given orally or in writing) or *implied* (i.e. reasonably inferred from the conduct of the individual).
de-identified information	*means* any information or opinion about a person whose identity cannot be ascertained from the information or opinion. De-identified information is exempted from the requirements of this Framework. For information to be classified as de-identified it must not contain identifiers which, if linked with other information, could lead to the identification of a person. If there is a possibility that the information is potentially identifiable, it cannot be classified as de-identified. If it is unclear whether an individual's identity can be ascertained the information should be treated as personal information and handled in accordance with the requirements of this Framework.
disclosure	*means* the communication or transfer of information, through giving a copy of the information to another organisation or individual, allowing another organisation or individual to have access to the information or giving out summaries, or giving the information in any other way. This is separate to *use*, although the privacy requirements apply to both the disclosure and use of personal information.
holds	as defined under the *Freedom of Information Act 1991*, an agency will be taken to hold a document if the agency has an immediate right of access to the document.
informed consent	*means* that an individual is aware of the implications of providing or withholding consent after being properly and clearly informed about how their personal information will be handled.
My Health Record	*means* the Commonwealth Government's electronic health record system. Unlike other electronic health records the content of *My Health Record* is controlled by the individual, including what information is shown in the record and who has access to it.
personal information	*means* information or an opinion, whether true or not, relating to a person or the affairs of a person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
primary purpose	*means* the dominant purpose for which information is collected. Most often in the health system the primary purpose will be to provide care, or an episode of care.

reasonable	the term reasonable is referenced throughout this policy e.g. reasonable steps, reasonably necessary. It should be taken to *mean* how an individual, who is properly informed, would be expected to act in the circumstances.
record	*means* – (a) any written, graphic or pictorial matter, or (b) a disk, tape, film or other object that contains information or from which information may be reproduced (with or without the aid of another object or device).
record-subject	*means* a person to whom personal information relates.
SA Health	is the brand name of the Department for Health and Wellbeing and the LHNs i.e. Central Adelaide Local Health Network, Northern Adelaide Local Health Network, Southern Adelaide Local Health Network, Women's and Children's Health Network, Barossa Hills Fleurieu Local Health Network, Eyre and Far North Local Health Network, Flinders and Upper North Local Health Network, Riverland Mallee Coorong Local Health Network, South East Local Health Network, Yorke and Northern Local Health Network and SA Ambulance Service.
secondary purpose	*means* the use or disclosure of personal information for a purpose other than the purpose for which it was collected.
third party	*means* any person who is not a staff member of SA Health (whether paid or not), or any organisation outside of SA Health. This includes contracted service providers e.g. non-government organisations, consultants, contractors, private health providers, university staff, researchers, students and volunteers.
use	*means* the communication or handling of information within SA Health. This is separate to *disclosure*, although the privacy requirements apply to both the use and disclosure of personal information.

APPENDIX 2: Other legislative, statutory and policy provisions governing the use and disclosure of personal information in SA Health

Note that the information provided below is an overview of the legislative, statutory and policy provisions only; for specific details the relevant Act or policies should be accessed from the South Australian Legislation website.

Requirements under the *Health Care Act 2008* and the *Mental Health Act 2009* are discussed in detail under section 7 of this Framework.

1. *Other legislation administered by SA Health*

There are a number of other Acts that are administered by SA Health that contain provisions about the disclosure of personal information. These Acts include:

1.1 *Advance Care Directives Act 2013*

Section 58 creates an offence for the publication of a report of proceedings under the Act where the person that is the subject of the proceedings may be identified unless consent is obtained.

It is an offence under section 61 for a person engaged in the administration of the Act to divulge or communicate personal information obtained in the course of official duties unless:

- authorised under the Act, or by another Act or law
- consent has been given by the person to whom the information relates
- the disclosure is required to give effect to the provisions of the advance care directive
- the disclosure is required to allow another agency to perform its functions.

1.2 *Ageing and Adult Safeguarding Act 1995*

Section 49 creates an offence for a person engaged, or formerly engaged, in the administration of the Act to divulge or communicate personal information obtained unless:

- authorised under the Act, or by another Act or law
- consent has been given by the person to whom the information relates
- the disclosure is in connection with the administration or administration of the Act or any other Act
- the disclosure is for a referral to a law enforcement agency or a person or agency exercising official duties under an Act relating to the care or protection of vulnerable adults
- the disclosure is to another agency or instrumentality in this State or another jurisdiction for the purposes of the proper performance of its functions
- the disclosure is reasonably necessary for the protection of the lawful interests of the vulnerable adult.

1.3 *Assisted Reproductive Treatment Act 1988*

Under section 18 it is an offence for the identity of a donor of human reproductive material to be disclosed, and for any other information to be divulged unless:

- authorised under the Act, or by another Act or law
- the disclosure is for the provision of assisted reproductive treatment
- consent has been given by the person to whom the information relates.

Information that is used for research or education may be disclosed where that information does not disclose the identity of the person.

1.4 *Controlled Substances Act 1984*

Under section 60A it is an offence to divulge information related to trade processes or medical records or details of medical treatment to a person unless it is:

- authorised under the Act, or by another Act or law
- consent has been given by the person to whom the information relates
- for legal proceedings
- to a law enforcement, prosecution or health authority of another jurisdiction.

Statistical or other information that could not reasonably be expected to lead to the identification of a person may be divulged.

1.5 *Health and Community Services Complaints Act 2004*

Section 75 prevents recording, disclosure or use of confidential information unless it is:

- authorised under the Act, or by another Act
- expressly authorised, in writing, by the person to whom it relates
- by order of a court or tribunal.

Information that is considered to be confidential includes:

- information about the identity, occupation or whereabouts of a complainant, health or community service user, or a health or community service provider
- information disclosed by a complainant, health or community service user, or a health or community service provider for the purposes of any complaint, investigation or inquiry
- information that would cause personal distress to a person if released
- information provided on a confidential basis.

Statistical or other information that could not reasonably be expected to lead to the identification of a person may be recorded, disclosed or used.

1.6 *South Australian Public Health Act 2011*

Section 99 prevents the disclosure of personal information unless:

- it is authorised under the Act, or by another Act
- it is required by law
- by order of a court or tribunal
- consent has been given by the person (or their guardian or medical agent) to whom the information relates
- unless otherwise directed, released to a relative, carer or friend for the purposes of treatment, care or recovery of the person to whom the information relates, and there is no reason to believe that the disclosure would be contrary to the person's interests
- released to a health or other service provider for the purposes of treatment, care or recovery of the person to whom the information relates
- recorded in an electronic records system for the recording or sharing of information for the management, administration or provision of health services
- it is to provide treatment to the person or prevent the transmission of a controlled notifiable condition
- it is to lessen or prevent a serious threat to public health or safety

- it is approved for medical, research or statistical purposes where it is not contrary to the person's best interests.

1.7 *Tobacco Products Regulation Act 1997*

Under section 78 it is an offence to divulge any information unless it is:

- authorised under the Act
- with the consent of the person from whom the information was obtained
- for any legal proceedings under the Act.

1.8 *Transplantation and Anatomy Act 1983*

Section 39 prevents the disclosure of information or documents that may identify a person who is either a donor of tissue for the purpose of transplantation, therapeutic, medical or scientific purposes or who is the recipient of a transplant, unless the disclosure is:

- authorised by law
- with the consent of the person to whom the information relates
- in accordance with a court order
- for the purposes of hospital administration or bona fide medical research.

1.9 *Other Acts*

There are a number of Acts administered by SA Health that include offences for the disclosure of commercial information. These include the *Food Act 2001*, *Gene Technology Act 2001*, *Research Involving Human Embryos Act 2003*, *Retirement Villages Act 2016*, and *Safe Drinking Water Act 2011*.

While provisions in these Acts relate to commercial information there may be instances where this information could be regarded as personal information. In these circumstances the information will be subject to the Information Privacy Principles.

2. *Other laws regulating information management*

2.1 *Public Sector Act 2009*

The *Public Sector Act 2009* outlines the standards expected of the public sector agencies and its employees. Section 5 of the Act requires employees to "deal with agency information in accordance with law and agency requirements."

The Code of Ethics for the South Australian Public Sector outlines the standards expected of all public sector employees, including how official information is handled. The Code may be accessed at www.publicsector.sa.gov.au.

When dealing with personal information public sector employees are to maintain the privacy of the individual and only release information in accordance with relevant legislation, industrial instruments, policy, or lawful and reasonable direction.

2.2 *State Records Act 1997*

The *State Records Act 1997* provides for the retention and disposal of records held by public sector agencies.

The Act provides a definition of what constitutes a record of an agency. An official record means a record made or received by an agency in the conduct of its business. Under the Act the record may take the form of either:

- written, graphic or pictorial matter
- disk, tape, film or other object that contains information or from which information may be reproduced.

2.3 *Freedom of Information Act 1991*

The *Freedom of Information Act 1991* (FOI Act) allows any person to apply for access to any information held by government and establishes a process for the correction of personal information.

While a person may obtain access to their own health records under the FOI Act, the *Health Care Act 2008* and the *Mental Health Act 2009* include provisions that provide a legal authority for the release of personal information at the request of the person to whom the information relates, or with their consent, to a guardian or medical agent of the person. However, the FOI Act may be used where:

- the person requests access under FOI
- the information sought relates to a number of people or is sought in the context of a family dispute or raises other contentious issues
- the information is of a medical or psychiatric nature and the agency is of the opinion that the disclosure of the information to the person may have an adverse effect on their physical or mental health or emotional state
- a person seeks information about a relative who is deceased and there is no appropriate medical agent to consent to the disclosure.

2.4 *Public Sector (Data Sharing) Act 2016*

The *Public Sector (Data Sharing) Act 2016* allows for the sharing of data between public sector agencies, and with other entities, to support policy making, program management and service delivery and planning. This data may include personal information held by an agency. The personal information must be de-identified although section 7(4) of the Act outlines instances where the data does not need to be de-identified. This includes instances where:

- the person to whom the information relates has consented to the sharing and use
- the sharing and use of the personal information is related to the purpose that it was originally collected, and there is no reason to think that the person to whom the information relates would object to the sharing and use
- the sharing and use is in connection with a criminal investigation, criminal proceedings, or proceedings where a penalty may be imposed
- the sharing and use is in connection with the wellbeing, welfare or protection of a child or children, or other vulnerable person
- the sharing and use is reasonably necessary to prevent or lessen a threat to the life, health or safety of a person
- the sharing and use of the personal information cannot be achieved through the use of de-identified data and it is impracticable in the circumstances to seek the consent of the personal to whom the information relates.

Under the Public Sector (Data Sharing) Regulations 2017 some health information is exempt from being shared under the *Public Sector (Data Sharing) Act 2016*.

Section 93 of the *Health Care Act 2008* and section 106 of the *Mental Health Act 2009* permit the disclosure of personal information where the disclosure is required or authorised by law. This would include disclosure in accordance with the *Public Sector (Data Sharing) Act 2016*, provided that the health information has not been exempted under the Public Sector (Data Sharing) Regulations.

3. *Other laws requiring the disclosure of personal information*

Other South Australian legislation requires the disclosure of personal information for specific purposes e.g. mandatory notification. The *Health Care Act 2008* and *Mental Health Act 2009* do not affect these reporting obligations. The provisions under the *Health Care Act 2008* and *Mental Health Act 2009* permit the disclosure of personal information for a purpose that is not the purpose of collection and where that disclosure is required or authorised under law.

Below is a list of South Australian Acts that may require the disclosure of personal information by law. This is not intended to be a definitive list but an illustration of Acts that may require SA Health to disclose personal information. SA Health staff should always look for the legal authority before disclosing personal information.

- *Births, Deaths and Marriages Registration Act 1996*
- *Boxing and Martial Arts Act 2000*
- *Children and Young People (Safety) Act 2017*
- *Coroner's Act 2003*
- *Correctional Services Act 1982*
- *Dog and Cat Management Act 1995*
- *Firearms Act 1977*
- *Harbors and Navigation Act 1993*
- *Health Practitioner Regulation National Law (South Australia) Act 2010*
- *Independent Commissioner Against Corruption Act 2012*
- *Intervention Orders (Prevention of Abuse) Act 2009*
- *Motor Vehicles Act 1959*
- *Ombudsman Act 1972*
- *Rail Safety National Law (South Australia) Act 2012*
- *Road Traffic Act 1961*

4. *Authorised disclosures*

Under the section 93 of the *Health Care Act 2008* the Chief Executive of SA Health, the Chief Executive Officer of an LHN, and the Chief Executive Officer of SA Ambulance Service, or their delegates, may authorise, or require, the disclosure of personal information for specific purposes.

Under section 106 of the *Mental Health Act 2009*, the Chief Executive of SA Health may authorise, or require, the disclosure of personal information for specific purposes.

It should be noted that while these authorisations provide for the release of personal information, any such disclosure is a matter of professional judgement and must be considered on a case-by-case basis in accordance with section 7 of this Framework.

4.1 *Authorised disclosures under guidelines or protocols*

A number of guidelines or protocols have been developed and subsequently authorised by the Chief Executive for the disclosure of personal information. These include:

4.1.1 *Information Sharing Guidelines for Promoting Safety and Wellbeing (ISG)*

The *Information Sharing Guidelines for Promoting Safety and Wellbeing* applies to South Australian government agencies and non-government organisations to share information when it is believed that a person is at risk of harm (from others or as a result of their own actions) and adverse outcomes can be expected unless appropriate services are provided.

On 18 January 2016 the Chief Executive issued an authorisation for the following persons to disclose personal information in accordance with the *Information Sharing Guidelines for Promoting Safety and Wellbeing* adopted by the Office of the Ombudsman and the *Information Sharing Guidelines for Promoting Safety and Wellbeing: SA Health ISG Appendix Policy Directive*:

- officers or employees of the Department for Health and Wellbeing engaged in the administration of the *Health Care Act 2008*
- persons employed under the *Health Care Act 2008*
- members of SA Ambulance Service (SAAS)
- persons otherwise engaged to work at a *Health Care Act 2008* incorporated hospital or in connection with the activities of SAAS
- persons engaged in the administration of the *Mental Health Act 2009*.

For further information refer to the *Information Sharing Guidelines for Promoting Safety and Wellbeing: SA*

Health ISG Appendix Policy Directive.

4.1.2 *Family Safety Framework*

The *Family Safety Framework* allows for the sharing of personal information between South Australian government agencies and non-government organisations to ensure that services are made available to families most at risk of violence.

On 27 September 2011 the Chief Executive issued an authorisation for the following persons to disclose personal information in accordance with the framework:

- officers or employees of the Department for Health and Wellbeing engaged in the administration of the *Health Care Act 2008*
- persons employed under the *Health Care Act 2008*
- members of SA Ambulance Service (SAAS)
- persons otherwise engaged to work at a *Health Care Act 2008* incorporated hospital or in connection with the activities of SAAS
- persons engaged in the administration of the *Mental Health Act 2009*.

For further information refer to the *Family Safety Framework and Authority to Disclose Information under the Family Safety Framework Policy Directive*.

4.1.3 *Multi-Agency Protection Services (MAPS) Project*

The *Multi-Agency Protection Services (MAPS) Project* allows for the sharing of personal information between South Australian Police, Department for Correctional Services, SA Health, Department for Communities and Social Inclusion, and Department for Education and Child Development to provide for the protection of victims, or potential victims, of domestic violence and/or child protection matters by allowing for the early identification of children and victims at risk.

On 30 June 2015 the Chief Executive issued an authorisation for the following persons to disclose personal information for the purposes of the successful functioning of the project:

- officers or employees of the Department for Health and Wellbeing engaged in the administration of the *Health Care Act 2008*
- persons employed under the *Health Care Act 2008*
- members of SA Ambulance Service (SAAS)
- persons otherwise engaged to work at a *Health Care Act 2008* incorporated hospital or in connection with the activities of SAAS
- persons engaged in the administration of the *Mental Health Act 2009*.

4.2 Authorised disclosures for specific purposes

The Chief Executive has also authorised the disclosure of personal information for specific purposes. Such authorisations may be for a specific project and generally on a time-limited basis and to specific people, or for more general operations across SA Health.

This policy only includes information on the authorised disclosures that apply generally across SA Health. Information on the more specific authorised disclosures will be made available to relevant SA Health staff at the time of the project.

SA Health staff who have concerns about the disclosure of personal information that is not covered under the provisions of section 93 of the *Health Care Act 2008*, section 106 of the *Mental Health Act 2009* or an authorisation issued by the Chief Executive should raise their concerns with their Manager.

The Chief Executive has issued authorisations for the following operations across SA Health:

4.2.1 *South Australian Coroner*

The Coroner investigates the deaths of persons who die from unnatural causes or where the cause of death is not known. Once a report of death is received (usually from the police, doctors or hospital authorities) the Coroner has legal control over the body of the deceased person to investigate the cause of death and the manner in which the death arose.

On 18 May 2011 an authorisation was made for persons employed or working at incorporated hospitals, SA Ambulance Service and staff working within the Department for Health and Wellbeing to disclose personal information during the investigation stage to the:

- South Australian Coroner
- South Australian Police Officer investigating a death on behalf of the South Australian Coroner
- any other investigator appointed under the *Coroners Act 2003* to investigate a death on behalf of the South Australian Coroner.

4.2.2 *SA Health Credentialling and Scope of Clinical Practice System*

The *SA Health Credentialling and Scope of Clinical Practice System* records the qualifications, experience and professional standing of health practitioners engaged by SA Health for the purposes of determining their competence, performance and professional suitability to provide safe, high quality health care services at a local health network.

On 15 October 2012 an authorisation was made for persons employed or working at incorporated hospitals (i.e. LHNs), SA Ambulance Service and staff working within the Department for Health and Wellbeing to disclose personal information relating to a health practitioner obtained while engaged in connection with the operation of the *Health Care Act 2008* for the purposes of the Credentialling and Scope of Clinical Practice System for:

- verification of the credentials of a health practitioner
- definition of the health practitioner's clinical scope of practice within SA Health
- any other activity that directly relates to verifying and recording a health practitioner's ability to carry out clinical activities as part of their employment or engagement with SA Health.

4.2.3 *Solicitors appointed by SA Health*

On 11 December 2011 an authorisation was made for persons employed or working at incorporated hospitals (i.e. LHNs) or SA Ambulance Service and persons working within the Department for Health and Wellbeing to make disclosures of personal information to a solicitor for the purposes of providing legal advice or representation to SA Health. For the purpose of this authorisation the reference to a solicitor includes the Crown Solicitor, solicitor employed in that office, or person assisting that solicitor for the purposes of providing legal advice or legal representation for SA Health.

4.3 *Charter of Health and Community Services Rights*

The Charter of Health and Community Service Rights (the HCSCC Charter) is established under the *Health and Community Services Complaints Act 2004*. It sets out the rights of all people who use health and community services in South Australia and of family members, carers and nominees who act on behalf of a person using a service.

One of the rights listed in the HCSCC Charter is the right to privacy and confidentiality which states:

> *I have a right to have my privacy respected and my personal information kept confidential and secure. Personal information about me may not be disclosed without my consent, unless the disclosure is required to lessen or prevent a serious threat to life, wellbeing, or safety or is required by law. I have a right to request and gain access to my records, unless there is legal restriction in place. I can nominate person/s with whom information can be shared.*