SA Health

Policy

Privacy

Version 3.1

Approval date: 18 March 2024

PDS Reference No: D0445

Government of South Australia

SA Health

1. Name of policy

Privacy

2. Policy statement

This policy provides the mandatory requirements within the *Cabinet Circular PC012 Information Privacy Principles* (IPPs), *Health Care Act 2008*, *Mental Health Act 2009*, and the *South Australian Public Health Act 2011* for the collection, use, access, disclosure and storage of personal information.

It is an offence to disclose personal information without a lawful authority and unauthorised disclosure may attract a monetary penalty, disciplinary action, and/or termination of a contract.

3. Applicability

This policy applies to all employees, volunteers, contracted staff, and all persons otherwise engaged to work at SA Health; that is all employees, volunteers and contracted staff of the Department for Health and Wellbeing (DHW), Local Health Networks (LHNs) including state-wide services aligned with those Networks and SA Ambulance Service (SAAS).

4. Policy principles

SA Health's approach to privacy and protection of personal information is underpinned by the following principles:

- We will ensure that all personal information held by SA Health is secure and protected from unauthorised collection, access, disclosure, or misuse.
- We will ensure information that supports health care provision is accessible to authorised users.
- We will comply with Cabinet's mandatory IPPs Instruction and our legislative obligations with respect to protection of personal information.

5. Policy requirements

Any personal information (clinical or corporate) collected by DHW, LHNs or SAAS is the property of SA Health and must be managed (appropriately collected, used, stored, accessed, and disclosed) in accordance with this policy.

In addition to the specific requirements stated in the IPPs, the *Health Care Act 2008*, the *Mental Health Act 2009*, and the *South Australian Public Health Act 2011*, each SA Health entity must:

- Ensure complaints about privacy breaches (clinical and corporate) are investigated and recorded in the Safety Learning System (SLS).
- In the event of a privacy breach:
  - Record the breach (clinical or corporate) of privacy in the SLS
  - Record the breach of privacy in the patient's record (where in a clinical setting)
  - Ensure individuals who are affected by unauthorised or unlawful disclosure of their personal information are notified of the breach in accordance with the Clinical Incident Management Policy and the mandatory SA Government Personal Information Data Breaches Guideline.
  - Ensure breaches are reported in accordance with local processes established under the Risk Management, Integrated Compliance, and Internal Audit Policy.
  - Ensure data breaches are reported to the Privacy Committee of South Australia in accordance with the Personal Information Data Breaches Guideline, and
  - Ensure personal data breaches that relate to tax file number information, and are likely to result in serious harm to individuals, are notified to the Office of the Australian Information

Commissioner within 30 days of the breach being discovered via the OAIC Notifiable Data Breaches Scheme.

- Complete a Privacy Impact Assessment in accordance with the Privacy Impact Assessment Tool when establishing new projects, activities, or procedures involving personal information.
- Not disclose information about quality improvement activities collected under parts 7 and 8 of the *Health Care Act 2008*, this information cannot be disclosed even where a court order or general search warrant is produced.
- Comply with the requirements in Appendix 1: Information Sharing Guidelines for Promoting Safety and Wellbeing Mandatory Instruction when disclosing personal information under the Department of the Premier and Cabinet's Information Sharing Guidelines for Promoting Safety and Wellbeing (ISGs), as authorised by the DHW Chief Executive.
- Ensure compliance with the mandatory related documents.

6. Mandatory related documents

The following documents must be complied with under this Policy:

- Acceptable Use Policy Summary
- Cabinet Circular PC012 Information Privacy Principles
- *Children and Young People (Safety) Act 2017*
- Clinical Incident Management Policy
- Consent Policy
- Freedom of Information Policy
- *Health Care Act 2008* (sections 66, 73 and 93)
- Information Security Policy
- Information Sharing Guidelines for Promoting Safety and Wellbeing
- INFOSEC 1 – Protecting Official Information
- *Mental Health Act 2009* (section 106)
- Personal Information Data Breaches Guideline
- Protective Security Policy
- SA Government Protective Security Framework
- SA Information Classification System Overview
- *South Australian Public Health Act 2011* (sections 99, 64(9), 68(14), 84 and 100)
- *Surveillance Devices Act 2013*
- *Work Health and Safety Act 2012* (section 271)
- Workplace Surveillance Policy

7. Supporting documents

- Early intervention by sharing information – 10 top practice tips
- ISG Decision Making Steps and Guide
- Overview of implementation of the Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families 2009 to 2012

- Police Requests for Information and Witness Statements from SA Health Policy Guideline
- Privacy Guideline
- Privacy Impact Assessment Tool
- Subpoenas and other Legal Requests for Information Protocol

8. Definitions

- **Access** means inspecting, retrieving, or obtaining information.
- **Agency** means a department, an employing authority, or any other agency or instrumentality of the Crown.
- **Agency Security Executive** means the person or position appointed as the Agency Security Executive in accordance with the Protective Security Policy.
- **Breach** means the loss, unauthorised access/use/modification/disclosure/collection, or misuse of personal information.
- **Collect** means to gather/record/acquire personal information from any source 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.
- **Critical hospital** means a hospital that has a general intensive care unit.
- **Cyber security incident** means one or more acts, events, or incidents involving:
    - unauthorised access to or modification or computer data or computer program, or
    - unauthorised impairment of electronic communications to or from a computer, or
    - unauthorised impairment of the availability, reliability, security, or operation of computer data, a computer program, or a computer.

  that have had, is having, or is likely to have, a significant impact on a hospital.
- **Disclosure** means the communication or transfer of information by: giving a copy; allowing access; providing a summary; or giving the information in any other way to another organisation or individual.
- **Limited confidentiality** means the limits that exist on the confidential nature of a consumer's personal information which make it possible for information to be shared without consent where it is unreasonable or impracticable to seek consent or consent has been refused, the disclosure is reasonably necessary to prevent or lessen a serious threat to the life, health and safety of a person or group of people, and the procedures of the ISG and this Policy are followed.
- **MHR System Operator** means the Australian Digital Health Agency.
- **My Health Record** means an online summary of an individual's health information held by the Australian Government's digital health record system under the *My Health Records Act 2012,* the *My Health Records Rules 2016*, and the *My Health Records Regulation 2012*.
- **Person** means all people including infants, children and young people.
- **Personal information** means information (including health 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. Personal information includes:
    a) paper records
    b) electronic records or information systems such as videos, x-rays, photographs
    c) entries on computer databases (including patient administration systems)
    d) emails or other electronic messaging systems (including SMS)
    e) third party hosted systems (including cloud based) and SA Health supported/hosted technologies, and

f) information from which the names and addresses have been removed but where sufficient information remains so that the individual could potentially be identified (such as by way of a number, reference, or details which, when combined with other information, can be related to an individual).

- **Privacy** means an individual's right to have their personal information protected from unauthorised access or disclosure.
- **State-wide services** means State-wide Clinical Support Services, Prison Health, SA Dental Service, BreastScreen SA and any other state-wide services that fall under the governance of the Local Health Networks
- **Use** means the communication, handling, deploying of information within SA Health.

9. Compliance

This policy is binding on those to whom it applies. Implementation at a local level may be subject to audit/assessment. The Domain Custodian must work towards establishing systems to demonstrate compliance with this policy, in accordance with the Risk Management, Integrated Compliance, and Internal Audit Policy.

Any instance of non-compliance with this policy should be reported to the Domain Custodian for the Legal and Corporate Governance Policy Domain and the Domain Custodian for the Risk, Compliance and Audit Policy Domain.

10. Document ownership

Policy owner:	Domain Custodian of the Legal and Corporate Governance Domain
Title:	Privacy Policy
Objective reference number:	A3021775
Review date:	01/12/ 2028
Contact for enquiries:	healthpolicylegislation@sa.gov.au

11. Document history

Version	Date approved	Approved by	Amendment notes
1.0	13/02/2017	Portfolio Executive	Original approved version.
2.0	15/05/2019	Director, Corporate Affairs	Formal scheduled review, minor updates.
3.0	01/12/2023	Deputy Chief Executive, Strategy and Governance	Reviewed to align with the Policy Framework.
3.1	18/03/2024	Domain Custodian of the Legal and Corporate Governance Domain.	Minor edit to implement a recommendation of an internal review of privacy management in the Department.

12. Appendices

1. Information Sharing Guidelines for Promoting Safety and Wellbeing Mandatory Instruction
2. My Health Records (MHR) System – Access, Use and Disclosure Mandatory Instruction

Appendix 1: Information Sharing Guidelines for Promoting Safety and Wellbeing Mandatory Instruction

The following Instruction must be complied with to meet the requirements of this policy.

1. Using the Information Sharing Guidelines (ISGs)

All employees and contracted staff must:

- Explain 'limited confidentiality' at the earliest possible time.
- Obtain approval from an SA Health Senior Clinician or Senior Manager before sharing information under the ISGs without consent.
- Obtain approval from an SA Health Senior Clinician or Senior Manager before refusing a request to share information.
- Make a report in SLS when:
    - Information is shared under the ISGs without consent
    - Where a request for information from an external organisation has been refused, or
    - When an external agency has refused to share information.
- Record details about information sharing under the ISGs in the patient record, including whether:
    - The ISG decision making steps were followed, and
    - The ISG practice guide was followed.
- Take reasonable steps to verify the identity of the person who the information is to be provided to (and their employer), including by:
    - Using government staff listings or global email lists
    - Calling the individual at their organisation's official number, and/or
    - Calling a senior person in the organisation to verify the individual's role.
- Only provide information to another agency for a legitimate purpose, including to:
    - Divert a person from offending or harming themselves
    - Protect a person or groups of people from potential harm, abuse or neglect
    - Protect service providers in situations of danger
    - Help a service provider more effectively address risks to safety and wellbeing, and/or
    - Alert other service providers to an individual's need for assistance.
- Only share information without consent when:
    - It is unreasonable or impracticable to seek consent or consent has been refused, and
    - The disclosure is reasonably necessary to prevent or lessen a serious threat to the life, health or safety of a person or group of people.

2. Receiving Information under the Information Sharing Guidelines

- An SA Health Senior Manager or Clinician must be notified as soon as possible if information is received from another agency about a consumer outside of normal interagency case management or referral processes.

3. Students and Volunteers

Students and volunteers must:

- Not share information under the ISGs, and
- Notify an SA Health Senior Clinician or Senior Manager as soon as possible if they hear or see anything of concern and all information sharing will be undertaken by that Manager/Clinician.

4. Contracting with Non-Government Organisations (NGOs) and Private Health Care Providers

DHW, LHNs and SAAS must:

- Develop local processes on information sharing to support coordinated services and early intervention for SA Health consumers at risk of harm in line with the ISGs, and
- Ensure all contracts with NGOs or Private Health Providers include a clause which mandates compliance with the requirements of this Policy for any information sharing in line with the ISGs.

Appendix 2: My Health Records (MHR) System – Access, Use and Disclosure Mandatory Instruction

The following Instruction must be complied with to meet the requirements of this policy.

1. Access, Use and Disclosure

- When accessing or using the My Health Records (MHR) system all employees and contracted staff must:
  - Ensure they are authorised to access the MHR viewer.
  - Only access the MHR viewer in the context of an episode of care (accessing a patient's MHR record outside an episode of care (including for research purposes) constitutes a misuse of the MHR system and can attract severe penalties).
  - Ensure they are logged out of the MHR viewer at the end of a session to prevent unauthorised access.
  - Only use the emergency access function to override any access restrictions (set by a patient):
    - When it is unreasonable or impracticable to get consent from the patient, and
    - when the practitioner reasonably believes that access is necessary to lessen or prevent a serious threat to the patient or another individual's life, health, or safety.
  - Document the reason for using the emergency access function in the medical record to support the provision of written confirmation that the use of the function was necessary, to the MHR System Operator who audit each use of the function.
  - Not print documents from the MHR (unless required for clinical care) or distribute to patients or their carers.
- When contributing information to a MHR all employees and contracted staff must:
  - Take reasonable steps to comply with a patient's request not to upload records.