Health Support Services

Privacy and Responsible Information Sharing Policy

Policy Group: Information Management
Document Number: A44044336
Document Version: 1.0
Document Version Date: 11/06/2026
Review Date: 30/06/2028

---

1. Policy statement

HSS will manage personal information in a lawful, secure and responsible manner in accordance with the *Privacy and Responsible Information Sharing Act 2024 (*the PRIS Act). HSS staff and contracted service providers must ensure personal information is collected, used, stored and disclosed in line with legislative requirements and HSS policies.

2. Purpose

This policy supports HSS' compliance with the *Privacy and Responsible Information Sharing Act 2024* by establishing requirements for the collection, use, storage and disclosure of personal information.

3. Scope

This policy applies to all HSS employees and contracted service providers.

4. Personal Information

There are two categories of personal information: personal information and sensitive personal information.

Personal information is information or an opinion that relates to an individual, whose identity is apparent or can reasonably be ascertained from the information or opinion.

Sensitive personal information is a subset of personal information, that if disclosed, could cause greater harm or distress to the affected person or people.

4.1 Personal Information - examples

Examples of personal information include:

- Name
- DOB
- Address and contact information
- Australian Tax file number / banking / financial information
- Unique identifiers

4.2 Sensitive personal Information - examples

Examples of sensitive personal information include:

- Race / ethnicity
- Gender identity
- Sexual orientation / practices
- Criminal record
- Political opinions / memberships
- Religious beliefs / affiliations
- Philosophical beliefs
- Health information

5. Information Privacy Principles (IPP's)

HSS will manage personal information in accordance with the Information Privacy Principles listed in *Schedule 1 of the Privacy and Responsible Information Sharing Act 2024.*

5.1 IPP 1: Collection

HSS will only collect personal information when it is required to perform a HSS function. In addition, HSS will only collect sensitive personal information if:

- It is required to carry out a HSS function; and
- The individual consents to the collection of the information; or
- the collection of the information is authorised under law.

When collecting personal information, HSS will provide the individual with a collection notice. Collection notices are discussed in further detail in section 6.4 below.

5.2 IPP 2: Use and disclosure

Where HSS holds personal information that was collected for a primary purpose, the information will not be used or disclosed for another purpose, unless:

- The disclosure is fair and reasonable in the circumstances.
- The person would reasonably expect HSS to use or disclose the information for the secondary purpose.
- The person consents to the use to disclosure.
- It is reasonable to believe that the disclosure is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of someone.
- Disclosure is necessary for law enforcement or an investigation into unlawful activity.

5.3 IPP 3: Information quality

Reasonable steps will be taken to ensure that the personal information HSS collects, uses or discloses, is accurate, complete and up to date.

5.4 IPP 4: Information Security

Reasonable steps will be taken to protect personal information HSS holds from misuse, loss, unauthorised access, modification or unauthorised disclosure.

5.5 IPP 4: Retention and disposal of personal information

Reasonable steps will be taken to destroy personal information that is no longer needed, unless it is required to be kept under law. Personal information will be destroyed:

- When it is no longer required.
- If it is reasonable to do so.
- In accordance with the approved retention and destruction schedules.
- In accordance with Custodian approval, as outlined in:
    - The WA health Information Governance Policy,
    - The HSS Information and Records Management Policy; and
    - The HSS Retention and Disposal procedure.

5.6 IPP 5: Openness and transparency

HSS will inform people about how their information will be used and shared. HSS will do this in the form of collection notices at the point of collecting the personal information, and via our Privacy Statement published on the HSS external website.

5.7 IPP 6: Access and correction

Contracted service providers

IPP 6 in the PRIS Act allows individuals to access and amend their personal information where it is held by contracted service providers.

IPP entities (WA government agencies)

Access and correction of personal information held by government agencies is covered under the *Freedom of Information Act (WA) 1992*.

Regardless of who holds the personal information, how the request is received, and under what legislation, a process will be established to allow people to access and/or correct their personal information. This process will be publicly available by being included in the Privacy Statement on the HSS external website.

Wherever possible, access to information will be provided. However, access will not be provided if it would be harmful to the health, welfare or safety of an individual, and/or it meets one of the subclauses listed under Schedule 1, Principle 6.1 of the PRIS Act.

If access to personal information is denied, the reasons will be provided via a written decision notice. If HSS denies the correction of personal information, HSS will provide reasons in a written decision notice, within 45 days of the request.

5.8 IPP 7: Unique Identifiers

A unique identifier will not be assigned to individuals unless it is necessary for HSS to perform one of its functions.

5.9 IPP 8: Anonymity

HSS will provide people with the option of not identifying themselves, unless:

- HSS is required under law to have the person identify themselves; or
- It is not practicable for HSS to deal with the person without identifying themselves.

5.10 IPP 9: Disclosures outside of Australia

HSS and its contracted service providers will not disclose personal information to recipients outside Australia unless the circumstances of the disclosure meets the criteria under IPP 9 in Schedule 1 of the PRIS Act.

5.11 IPP 10: Automated decision-making (ADM)

HSS must ensure that privacy obligations are addressed where automated decision-making processes and AI systems are used. HSS business units using an AI or ADM process must advise the HSS PRIS Officer.

Where an ADM or AI process is being used, HSS or the contracted service providers must:

- Conduct a privacy impact assessment (PIA) to assess the potential harm, bias or discrimination that use of AI or ADM may cause.
- Re-evaluate the ADM process periodically and/or when changes are made to the ADM.
- Notify individuals when an ADM has been used to make a decision about them.
- Provide information on request to a person about how the ADM was used to make the decision.
- Establish a process for people to request a review of the ADM by a person.

5.12 IPP 11: De-identified information

Reasonable steps will be taken to protect any de-identified information from misuse, loss, unauthorised re-identification, access, modification, or disclosure.

De-identified information will not be re-identified unless specific circumstances apply, as outlined under IPP 11 in Schedule 1 of the PRIS Act.

6. Privacy

6.1 Privacy Statement

A Privacy Statement must be published on the HSS external website, which explains the personal information collected by HSS and how this information is handled and disclosed.

6.2 Privacy Complaints Process

A process will be established where individuals can lodge a privacy complaint. This process will be advertised on the HSS external website. The HSS PRIS Officer will be responsible for coordinating a response to the complaint.

6.3 Privacy Management Plan (PMP)

A PMP must be created that provides an overview of HSS's level of compliance in relation to the requirements set down in the PRIS Act. The PMP will outline where HSS is compliant, where HSS is not compliant, and the plans to address areas of non-compliance. The PMP must be provided to the Information Commissioner upon request.

6.4 Collection Notices

A collection notice must be provided when personal information is collected. The collection notice must give the individual information about:

- Why the information is being collected.
- Details of any law it is being collected under.
- How the personal information will be used, and who it will be disclosed to.
- The consequences if the information is not provided.
- The contact details for enquiries relating to the collection.

6.5 Privacy Impact Assessments (PIA)

A Privacy Impact Assessment must be conducted before performing a function or activity that will have an impact on privacy. The purpose of the PIA is to assess the impact on the privacy of people and identify options for managing the impacts.

The PIA must be documented within the WA health *PRIS Privacy Impact Assessment tool*.

6.6 Contracted Service Providers

Contracted service providers must comply with privacy obligations of the PRIS Act. Their capacity to comply with this policy and the PRIS Act must be evaluated as part of awarding the contract, and the monitoring of their compliance must be undertaken as part of managing the contract.

6.7 Privacy Code of Practice and dealings with the Information Commissioner

A Privacy Code of Practice (PCOP) allows for agencies to make changes to its policies and procedures that differ from the IPP's outlined in Schedule 1 of the PRIS Act.

A PCOP comes into effect after it has been approved by the Information Commissioner.

The consultation process that must take place when establishing a PCOP:

1. IMGAG - HSS must receive approval from IMGAG before a PCOP can be submitted.
2. HSS General Counsel – The PCOP must be reviewed and approved by the HSS General Counsel.
3. Legal and Legislative Services – The PCOP must be consulted with before the PCOP is sent to the Information Commissioner.
4. Information Commissioner - After approval is provided in steps 1 to 3, the PCOP can be submitted to the Information Commissioner.

The HSS PRIS Officer has responsibility for managing the PCOP process and coordinating dealings with the Information Commissioner on privacy matters.

7. Responsible Information Sharing

7.1 Department of Health Information Governance Policy and Model

In accordance with the WA health Information Governance Policy and Information Governance Model, Custodians must be appointed to maintain governance controls around managing information. This includes decision-making surrounding the disclosure of information.

7.2 HSS Information Release Policy and Model

All HSS staff are responsible for protecting privacy, for ensuring that personal information is shared responsibly, and ensuring the correct processes are followed with regards to obtaining authorisation to share information.

Responsibility around authorising disclosure of information is set out in the HSS Information Release Policy and HSS Information Release Model. All HSS staff must comply with the HSS Information Release Policy and HSS Information Release Model.

7.3 Information Sharing Agreements

To facilitate responsible information sharing between HSS and external agencies, information that is regularly shared outside of the WA health system should be shared under a formal Information Sharing Agreement. Contact the HSS PRIS Officer if you require assistance in establishing an information sharing agreement.

A Privacy Impact Assessment (PIA) must be conducted before entering into a formal Information Sharing Agreement that requires the sharing of personal information with an external agency.

The PIA must be documented and saved within the WA health PRIS Privacy Impact Assessment tool.

The Information Sharing Agreement must also be assessed concerning sensitive Aboriginal information, and compliance with responsible sharing principles.

Information Sharing Agreements must be reviewed by the HSS PRIS Officer.

7.4 Information Sharing Directions from a Minister

Under section 163 of the PRIS Act, the Minister for Health can issue a direction to HSS, directing HSS to enter into an information sharing agreement with another public or external entity.

If such a direction is received, HSS must notify the WA health Information Management Governance Advisory Group (IMGAG).

This reporting will be managed by the HSS PRIS Officer.

7.5 Dealings with the Information Commissioner and Chief Data Officer

All instructions, notices and dealings from and with the WA Information Commissioner and Chief Data Officer will be coordinated by the HSS PRIS Officer.

8. Information Breaches and Data Breach Reporting

8.1 Notifiable Information Breaches – Definition and Examples

A notifiable information breach is an incident where personal information is lost, accessed without authorisation, or disclosed without authorisation, and is likely to result in **serious harm** to the individuals involved.

Categories of breaches

- Malicious attack - where there is a deliberate attack to gain access to personal information for criminal activity.
- Human error / accidental or unintended disclosure. (For example, sending personal information to the wrong email address).
- Loss of items (phone, laptop, USB, physical file).
- Insecure disposal – disposing of physical documents, or electronic devices, without proper shredding, deletion or de-identification.
- Inadequate system controls on business information systems.

Examples of a notifiable breach

An incident becomes notifiable if the personal information that has been breached, poses a real risk of serious harm in the form of identity theft, financial theft, or a risk to physical safety. For example:

- The address of an employee is provided to another person who is subject to a domestic violence related court order.
- An employee provides login details through a phishing scheme, giving access to systems to people whose intent is on stealing personal data.
- Deliberate disclosure of personal information by an aggrieved employee or former employee with an intent to cause harm, and/or financial gain.
- Theft or loss of unencrypted devices – laptops, USB devices.
- Theft or loss of unredacted physical records containing personal information.

8.2 Comply with HSS information breach policy

All HSS staff and contracted service providers must comply with the HSS Information Breach policy.

All breaches must be reported to HSS Governance Risk and Compliance team in the first instance, and then to the Department of Health Information and Performance Governance Unit.

8.3 Notifiable information breaches - reporting

A notifiable breach involves notifying:

- The relevant Information Custodian; and
- The WA health system Information Management Governance Advisory Group (IMGAG); and

- The affected individual(s); and
- The Information Commissioner.

Notifications for notifiable breaches will be coordinated by the HSS PRIS Officer, in conjunction with the Information Custodian, Information Steward, IMGAG, the HSS Security and Risk team, and the HSS Communications team.

9. HSS Reporting, Compliance and Monitoring

9.1 Responsibility for internal monitoring

HSS Executive Directors, Directors and Managers are responsible for ensuring staff within their areas comply with requirements of this policy.

Compliance with this policy is supported through a combination of:

- Line management oversight and supervision of staff practices;
- Use of approved information systems and associated controls (e.g. record capture and storage requirements); and
- Periodic reviews, audits, or maturity assessments undertaken at a directorate or organisational level

Instances of non-compliance may be identified through operational issues, audits, or reported incidents, and are to be addressed through appropriate management action and escalation pathways where required.

Non-compliance with this policy may result in breaches of legislative obligations and reputational damage.

9.2 Compliance or enforcement notices

If HSS receives a compliance or enforcement notice from the Information Commissioner, IMGAG must be notified. This will be coordinated by the HSS PRIS Officer.

9.3 Information management maturity assessments

All HSP's must report the results of their two yearly self-assessed Information Management Maturity Assessment to the Department of Health Information Performance Governance Unit. This will be coordinated by the HSS PRIS Officer.

10. Target audiences

This Policy applies to all Health Support Services employees and contracted service providers.

11. Legislative context

This policy supports HSS' compliance with the following legislation:

- *Privacy and Responsible Information Sharing Act 2024*
- *Freedom of Information Act 1992*

12. Mandatory requirements

Under this policy, HSS staff must comply with the following mandatory WA Health policies and instruments:

12.1 Mandatory Policies

- HSS Recordkeeping Plan 2021
- HSS Information Release Policy and Information Release Model
- HSS Information Breach Policy
- WA Health Code of Conduct
- WA Health System Information Governance model
- WA Health Information Management Governance Policy – MP 0152/21
- Information Security Policy - MP 0067/17
- WA Health Information Quality Policy – MP 0178/23
- WA Health Establishment and Workforce Data Policy – MP 0157/21
- WA Health Information Access Use and Disclosure Policy – MP 0015/16
- WA Health Information Breach Policy MP 0135/20
- WA Health Information Classification Policy - MP 0146/20
- WA Health Information Retention and Disposal Policy – MP 0144/20
- WA Health Information Storage Policy – MP 0145/20
- WA Health Cloud Policy – MP 0140/20
- WA Health Aboriginal Data Governance Policy - MP 0190/25
- WA Health Data Linkage Policy - MP 0184/24
- WA Health Artificial Intelligence Policy – MP 0193/25

**Any mandatory requirement document that references the Hospitals and Health Act 1927 must be interpreted as a requirement under the Health Services Act 2016.*

12.2 Mandatory training

Custodians must complete any custodian related training, as part of understanding their role in managing information, and making decisions around responsible information sharing, and managing data breaches.

All employees must complete WA health mandatory training, (that includes elements around confidentiality and handling of information):

- Code of Conduct
- Accountable and ethical decision making
- Recordkeeping awareness training

13. Related Documents

This policy should be read in conjunction with the following documents:

- HSS Privacy Statement
- HSS Privacy Management Plan
- HSS - Contact Centre – Information Breach Procedure
- HSS Records Destruction procedure
- WA Health Information Access Use and Disclosure Standards
- WA Health Privacy Impact Assessment tool

14. Roles and responsibilities

All HSS staff and contracted service providers are responsible for the protection of personal information, maintaining confidentiality and privacy, and sharing of information in a responsible manner. Additional responsibilities for certain staff are as follows:

Role	Responsibility
Chief Executive	The Chief Executive, though the HSS Executive is to ensure that HSS is compliant with legislative requirements and best practice standards.
Executive Directors, Directors and Managers	Executive Directors, Directors and Managers are responsible for ensuring their staff, including contracted service providers, complete mandatory training, create business records as evidence of their decisions, and save these records to the recordkeeping system. Executive Directors, Directors and Managers may also be required to act as Information Custodian. In their capacity as a Custodian they will be required to make decisions around the lawful and responsible disclosure of information.
All HSS Staff and contracted service providers	All HSS staff and contracted service providers must: • Comply with HSS and WA health system policies and procedures. • Report any directions from the Information Commissioner or Chief Data Officer to the HSS PRIS Officer. • Raise any privacy concerns with the HSS PRIS Officer. • Liaise with the HSS PRIS officer regarding information sharing arrangements.
HSS PRIS Officer	The HSS PRIS Officer is responsible for implementing and coordinating PRIS functions and activities within HSS. The Manager Governance, Risk and Compliance is the designated HSS PRIS Officer.
Information Custodians	Responsibilities of the Information Custodian are set out in the WA Health Information Governance Model. Information Custodians are responsible for the operational aspects of managing information, such as approving disclosure and authorising destruction of the information.
IMGAG	The Information Management Governance Advisory Group (IMGAG) is responsible for the governance of privacy and responsible information sharing related activities across the WA health system's entities. The HSS representative on this committee is the Chief Information Officer.

Role	Responsibility
Department of Health Information Performance Governance Unit	The IPG Unit will be responsible for systemwide privacy and responsible information sharing related activities, including: • tabling submissions and notifications with the IMGAG; • reviewing submissions and notifications to the IMGAG; • providing education and training resources.

Policy owner

Director, Office of the Chief Executive

Review

Date	Review requirements
30 June 2028	This policy will be reviewed in accordance with changes to the WA Health Policy Framework

Approval

Date	Position	Name
17 June 2026	Director, Office of the Chief Executive	Sam Matyear

Compliance

In their role in making decisions around the responsible release of information, Information Custodians will be required to undertake training as advised by the Department of Health Information Performance Governance Unit.

Glossary

Term	Definition
Automated decision-making process (ADM)	An automated decision-making process is a process under which: • a decision is made by an automated system without the involvement of any individual, or • the making of a decision is materially assisted by an automated system.
Contracted Service Provider	A party to a state services contract who providers services to, or on behalf of an outsourcing entity under the contract.

Term	Definition
	A person who is a subcontractor (whether direct or indirect) of a person referred to above, for the purposes of a state services contract. See Section 8(2) of the PRIS Act for definition.
Information Breach	An incident in which personal or confidential information, or non-personal information that could be sensitive or commercial is compromised. The information may be subject to unauthorised access, use or disclosure, or is lost, damaged or destroyed.
Information Privacy Principle (IPP's)	Guiding principles that govern the collection, use, disclosure and security of personal information across the public sector.
Notifiable Information Breach	An information breach, relating to personal information, that is likely to result in serious harm to any individual to whom the information relates.
Personal Information	Information or an opinion that relates to an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
Privacy Code of Practice	A code of practice providing information on: • modifications to the application of one or more of the IPPs, by prescribing standards at least as stringent as the standards prescribed by the IPPs • how one or more of the IPPs are to be applied or complied with.
Privacy Impact Assessment (PIA)	An assessment of a function or activity that identifies potential impacts and makes recommendations to manage, minimise or eliminate any impacts on the privacy of an individual.
Privacy Management Plan (PMP)	A strategic planning document that outlines how an organisation manages personal information to ensure compliance with privacy laws and regulations.
Responsible Information Sharing Principles	Guiding principles that provide a framework in which to responsibly share government information.
State Services Contract	A contract between a public entity (the outsourcing entity) and another person (other than a public entity), under which services are provided to the outsourcing entity or to other persons on behalf of the outsourcing entity. See section 8(2) of the PRIS Act.