



## **Response by the Department of Health Western Australia**

### **to the Privacy and Responsible Information Sharing: Discussion Paper**

25 October 2019

The Department of Health is fully supportive of the proposed Privacy and Responsible Information Sharing legislative framework. It is envisaged that legislative reform will assist to enable and facilitate the Department of Health's own program of reform aimed at maximising the appropriate use and sharing of information as an operational and strategic, high value asset. These changes are designed to support WA Health continue to meet its vision to deliver a safe, high quality, sustainable health system for all Western Australians.

#### **1) What issues should be considered when developing privacy and information sharing legislation for Western Australia?**

There are several issues that need to be considered when developing privacy and information sharing legislation for Western Australia. Key issues include ensuring:

- Privacy legislation does not restrict the access, use and disclosure of information when it is required or permitted by other written laws. An example is the legal provisions in the *Health Services Act 2016* and the *Health Services (Information) Regulations 2017* which allow information to be collected, used or disclosed when it is reasonably necessary to lessen or prevent a serious risk to the life, health or safety of any individual.
- Privacy provisions in the legislation do not inadvertently undermine the intent of the information sharing provisions and result in more restrictive information sharing practices. This includes ensuring existing information sharing arrangements between agencies are not restricted by the proposed legislation.
- There are not significant cost burden on agencies to implement changes as a result of Privacy and information sharing legislation.
- The legal purposes for which information can be shared are not too specific or restrictive to ensure that information is available to improve service delivery and benefit the community.
- The role of the WA Privacy Commissioner does not result in a more risk adverse approach to information sharing by agencies.
- Proposed information breach processes align and support existing processes that are considered effective and appropriate within larger agencies.
- The role of the Chief Data Officer does not result in a risk avoidance culture to the application of information by agencies.
- Third party provisions are adequately addressed in the legislation to allay community concerns. Similarly, when necessary, ensuring data is appropriately de-identified may be difficult. There are privacy concerns for open release of public sector data about individuals, even if they are not obviously identifiable.



- It is important that any legislative changes ensure that Aboriginal peoples' trust, expectations and understanding of data ownership are recognised. This includes the recognition of ownership of Aboriginal personal and community information as stipulated in the National Aboriginal and Torres Strait Islander Health Data Principles and the Indigenous Data Sovereignty which recommends that:
  - the Australian Government thoroughly consider matters/issues related to Aboriginal data/information, and
  - work closely with Aboriginal communities and stakeholders to ensure the right and appropriate approach to data sharing.
- Adequate provisions to address issues that are specific to information sharing with a range of entities including, but not limited to:
  - state government agencies
  - federal government agencies
  - non-government entities for research purposes
  - non-government entities for commercial gain
  - public reporting
- The ability to include provisions within the legislative framework that override restrictive information sharing provisions in existing legislation (such as the legislation for many of the statutory collections in the WA health system).

## **2) What privacy principles should WA adopt for regulating the handling of personal information by the public sector? Are any of the existing Australian Privacy Principles or principles in other Australian jurisdictions, unsuitable for WA?**

WA should adopt a modified version of the Australian Privacy Principles.

There are however some Australian Privacy Principles that may not be suitable for WA in their current form including:

- *Principle 2: Anonymity and pseudonymity - Giving the individuals the option of not identifying themselves or of using a pseudonym with limited exceptions applying.* The exceptions for this principle need to be considered thoroughly. This principle would undermine several existing agreements the Department of Health has with other agencies and limit the Departments ability to undertake data linkage. Consideration also needs to be given to ensure risks to patient safety are not introduced due to difficulties in the correct identification of patients.
- *Principle 6: Use or disclosure of personal information – outlines the circumstances in which an entity may use or disclose personal information that it holds.* This principle needs to have the provision that it does not restrict the use and disclose of personal information without consent where it is permitted or required by law.
- *Principle 9: Adoption, use and disclosure of government related identifiers.* It is important that the limited circumstances in which an organisation may adopt government related identifiers of an individual supports current data linkage activities that are critical for the improvement of patient care and service provision.



- *Principle 12: Access to personal information.* It is important this principle aligns to the *Freedom of Information Act 1992*.

### **3) What should the role of a Privacy Commissioner be, and how can this role best protect privacy and ensure public trust?**

The Privacy Commissioner's role should be to address and protect against misuse and inappropriate disclosure. It is however critical that the role of the Privacy Commissioner does not result in a more risk adverse approach to information sharing by agencies. It is also important that there is governance oversight of the Privacy Commissioner's powers so that information sharing remains a priority.

It is not clear if there will be a complaint mechanism for individuals and if this mechanism will be managed by agencies or the Privacy Commissioner. The Department of Health's preferred mechanism in such instances is that individual agencies initially manage complaints by individuals with the Privacy Commissioner only intervening where escalation is required.

### **4) How should breaches of privacy be managed, and what action should be taken in response to a breach?**

It is important that any breach process that is established supports and complements existing processes that large agencies already have in place.

The WA health system has an established information breach process. The actions staff are required to take are mandated in the Information Breach Policy. The breach process in the Information Breach Policy is aligned to the national approach adopted by the Office of the Australian Information Commissioner. The policy is based on the four steps to:

- contain the information breach
- assess the impact of the information breach to determine the extent of the damage and harm caused
- take actions to remediate any risk of further harm (including notifying impacted individuals where appropriate)
- review the incident and take preventative actions.

WA health system staff are also provided support and advice from subject matter experts including:

- Health Service Provider Integrity Units and System-wide Integrity Services
- Legal and Legislative Services and Health Service Provider General Counsels
- Ethics Committees
- Research Governance, and Information Governance Units
- Data Custodians and Data Stewards.

It needs to be acknowledged that smaller agencies may require assistance to develop and implement appropriate information breach processes.



What actions should be taken in response to breaches should be dependent on the type and cause of the breach and an appropriate model should be developed in consideration of the relevant sections of the Public Sector code of conduct and agency-specific policies.

**5) When should government agencies be allowed to share personal information? Are there any circumstance in which it would not be appropriate to do so?**

Personal information in a health setting is often required to realise the maximum benefits to the individual and the community. The intent of the privacy and information sharing legislation is to provide a legislative framework to promote appropriate information sharing between agencies. It is important that the legislation allows personal information to be used and disclosed when it:

- benefits the individual or the WA community through:
  - better informed decision making
  - improved government policies
  - more effective and efficient government service delivery
  - research discoveries and innovations
  - improved quality and validation of data collected by agencies

It may not be appropriate for government agencies to share personal information where it would be against the individual's best interests or safety. As mentioned in the Discussion Paper, in the health context this may include the sharing of certain health data with third parties including, but not limited to, health insurance companies.

**6) What should the role of a Chief Data Officer be? How can this role best support the aims of Government and the interests of the public?**

The Chief Data Officer's role should be to:

- engage in data leadership
- promote best practice
- provide advice, information and resources to stakeholders
- develop information architecture, particularly for smaller agencies.

The Chief Data Officer's role should ensure information held within the WA public sector is appropriately shared and available to fully realise the value of the information. It is important that the Chief Data Officer's role supports existing procedures and information architecture of larger agencies.

**7) Should the WA Government facilitate sharing of information outside the WA public sector? What should be considered when making a decision to share outside the WA public sector?**

Information should only be made available to organisations outside of the WA public sector when it is lawful to do so and it will improve service delivery or provide a benefit to the WA community.



### **8) What criteria should be included as part of a risk management framework such as the Five Safes?**

The Five Safes, as proposed, is better suited to addressing risk mitigation strategies for individual projects rather than for ongoing sharing of larger datasets and programs of work between government agencies. The proposed 'project' safe could be renamed to the 'purpose' so that it reflects the legislation's aim to promote broader information sharing that is not project specific. It is important that the Five Safes and any associated guidelines are designed in such a way that they scale effectively to support larger interagency information sharing initiatives, not just projects with a defined scope.

### **9) Under what circumstances would it be considered acceptable to share confidential information within the public sector?**

Information should be shared when it:

- empowers agencies to realise the value of the information to benefit WA communities
- fosters better decision making
- improves government policies
- supports more effective and efficient government service delivery
- enables research discoveries and innovations
- is appropriately managed to prevent misuse and inappropriate disclosure.

### **10) What should the WA Government be doing to support successful implementation of privacy and information sharing?**

Supporting information should be developed. A guide could provide key information and resources to stakeholders. Similarly, a help desk and a website with appropriate resources would also prove helpful.