Government of **Western Australia**
Department of **Health**

Information Access, Use and Disclosure Policy Resource Compendium

health.wa.gov.au

Owner:	Department of Health, Western Australia
Contact:	Information and System Performance Directorate
Approved by:	Rob Anderson, A/Assistant Director General, Purchasing and System Performance
Original Approval date:	9 October 2019
Current version:	3.2
Links to:	Information Management Policy Framework https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-Management

VERSION	DATE	AUTHOR	COMMENTS
3.0	9 October 2019	Anthony Jones	Approved by Rob Anderson, A/Assistant Director General, Purchasing and System Performance
3.1	23 July 2021	Ian Barrett	Minor amendment to Appendix 1 Access and Disclosure Model to align with Information Classification Policy MP 0146/20
3.2	17 August 2023	Anthony Jones and Brooke McQuade	Major amendment to update Purpose Test to align to *Health Services Act 2016* amendments. Synthetic Data as a risk mitigation strategy has also been included in the Risk Mitigation section. A section for the *Data Availability and Transparency Act 2022* and Privacy and Responsible Information Sharing Legislation has also been included.

Contents

1 Purpose

The *Information Access, Use and Disclosure Policy Resource Compendium* is a supporting document in the Information Access, Use and Disclosure Policy. The purpose of the compendium is to provide context, background information and resources to assist stakeholders comply with the mandated requirements in the *Information Access, Use and Disclosure Policy*. The compendium is not mandatory unless the requirement is mandated in the policy.

2 Introduction

Information in the WA health system is collected, accessed, stored, used and disclosed to support the realisation of WA health system's vision to have a sustainable health system that delivers safe, high quality health care to all Western Australians.

The Information Management Policy Framework specifies the information management requirements to ensure the effective and consistent management of health, personal and business information across the WA health system. The *Information Access, Use and Disclosure Policy* has been updated to align to the Information Management Policy Framework.

The aim of the *Information Access, Use and Disclosure Policy* is to facilitate lawful and appropriate information access, use and disclosure by staff members of the WA health system and enable information sharing. This resource compendium explains key elements of the *Information Access, Use and Disclosure Policy* and provides context and background information to support an understanding of the mandated requirements.

3 Policy drivers

The key policy drivers for the *Information Access, Use and Disclosure* Policy are outlined in Figure 1. The legislative and policy framework as well as the State and National health agendas inform the *Information Access, Use and Disclosure Policy*.

Figure 1: Key Policy drivers

3.1 Information Management Legislative and Policy Framework

The *Information Management Policy Framework* and mandated policies align to the legislation to support effective information management within the WA health system.

A range of legislative requirements govern information in the WA health system. Although the list below is not exhaustive, key legislation includes:

- *Children and Community Services Act 2004*
- *Commonwealth Privacy Act 1988 (Australian Privacy Principles)*
- *Coroners Act 1996*
- *Corruption, Crime and Misconduct Act 2003*
- *Criminal Code Act Compilation Act 1913*
- *Data Availability and Transparency Act 2022*
- *Electronic Transactions Act 2011*
- *Evidence Act 1906, Acts Amendment (Evidence) Act 2000*
- *Freedom of Information Act 1992*
- *Freedom of Information Regulations 1993*
- *Health (Miscellaneous Provisions) Act 1911*
- *Health and Disability Services (Complaints) Act 1995*
- *Human Reproductive Technology Act 1991*
- *Health Services Act 2016* and *Health Services (Information) Regulations 2017*
- *Medicines and Poisons Act 2014*

- *Mental Health Act 2014*
- *National Health and Medical Research Council Act 1992*
- *Private Hospital and Health Services Act 1927*
- *Public Health Act 2016*
- *State Records Act 2000*

The applicable policy frameworks are listed below:

- *Information Management Policy Framework*
- *Information and Communications Technology Policy Framework*
- *Research Policy Framework*

It is essential that the collection, storage, use, disclosure and disposal of information within the WA health system is lawful.

3.2 Commonwealth Government agenda

3.2.1 Productivity Commission

The Productivity Commission's *Data Availability and Use Inquiry* recommended national reforms to overcome barriers and issues with Australia's current data system to move from one based on risk avoidance, to one based on value, choice, transparency and confidence.[1]

3.2.2 Data Sharing

In 2018, the Office of the National Data Commissioner released an issues paper for consultation for the New Australian Government Data Sharing and Release Legislation.[2] The Office of the National Data Commissioner held a series of roundtables across the country to further explore an appropriate data sharing and release legislative framework. The *Data Availability and Transparency Act 2022* was enacted in April 2022. The Act enables sharing of Commonwealth held data to support improved service delivery outcomes.

3.2.3 National Health Reform

The Commonwealth and the States have signed an addendum to the National Health Reform Agreement. A significant inclusion in the addendum is the shift from purchasing for activity to purchasing for value and outcomes. A key part of the reform agenda is improved access and reporting of safety and quality information.

3.3 State Government agenda

3.3.1 Privacy and Responsible Information Sharing

In 2019, the State Government announced plans to develop legislation to strengthen the protection of privacy and enable safe information sharing within the public sector and with authorised third parties.

The Privacy and Responsible Information Sharing (PRIS) legislation aims to respond to community concerns about privacy and contribute to the trust and social licence necessary to share information responsibly for the benefit of the community.

Figure 2: Benefits of Legislation

Source: Department of the Premier and Cabinet PRIS Public Information Session Presentation

More broadly, the legislation introduces reforms that provide[3]:

- guiding principles and a framework to govern the collection, protection, use and disclosure of personal information across the public sector;
- a mandatory data breach notification scheme, requiring agencies to notify the Privacy Commissioner and affected individuals of serious data breaches involving personal information; and
- a mechanism that supports Aboriginal data sovereignty and governance in WA, by requiring that Aboriginal people and communities are involved or consulted with, when data about them is shared[1].

Further information can be found on the Privacy and Responsible Information Sharing intranet page.

[1] Refers to the collection, access, use, and disclosure.

3.3.2 Open Data Policy

The *Whole of Government Open Data Policy* aims to improve the management and use of the public sector's data assets in WA in order to deliver value and benefits for all Western Australians.[4] A key focus of the policy is to facilitate greater release of appropriate and high value data to the public in ways that are easily discoverable and usable.[4]

3.4 Sustainable Health Review

The *Sustainable Health Review*[5] was released in April 2019. The review identifies eight 'Enduring Strategies' to promote the short, medium and long term sustainability of the health system in WA.

The 'Enduring Strategies' are supported by 30 recommendations. The recommendations place a strong community-centred focus on equity, prevention and providing seamless access to the right services in the right settings. The recommendations also foster innovative solutions to deliver effective and efficient services that are safe, high quality and patient centred.

Information access and sharing was identified as a key area to support a sustainable health system. Many of the review recommendations require better access and sharing of information. The key information access and sharing related recommendations in the Sustainable Health Review include:

- *"Recommendation 6(b) - Immediate transparent public reporting of patient outcomes and experience.*
- *Recommendation 16 - Establish a systemwide high value health care partnership with consumers, clinicians and researchers to reduce clinical variation and ensure only treatments with a strong evidence base and value are funded.*
- *Recommendation 17 - Implement a new funding and commissioning model for the WA health system from July 2021 focused on quality and value for the patient and community, supporting new models of care and joint commissioning.*
- *Recommendation 21 - Invest in analytical capability and transparent, real-time reporting across the system to ensure timely and targeted information to drive safety and quality, to support decision making for high value healthcare and innovation, and to support patient choice.*
- *Recommendation 22 - Invest in a phased 10-year digitisation of the WA health system to empower citizens with greater health information, to enable access to innovative, safe and efficient services and to improve, promote and protect the health of Western Australians.*
- *Recommendation 23 - Build a systemwide culture of courage, innovation and accountability that builds on the existing pride, compassion and professionalism of staff to support collaboration for change.*

- *Recommendation 24 - Drive capability and behaviour to act as a cohesive, outward-looking system that works in partnership across sectors, with a strong focus on system integrity, transparency and public accountability.*
- *Recommendation 28 - Establish a systemwide network of innovation units in partnership with clinicians, consumers and a wide range of partners to quickly develop, test and spread initiatives delivering better patient care and value."* [5]

3.5 Health-related coronial inquests

The 'From Death We Learn' reports place a spotlight on the health-related coronial inquests that show the consequences to service delivery and the impact on patients when information is withheld and not shared in the best interests of patients.[6,7] The 2017 report highlighted the legal provisions that were put into place after crucial information was not shared.[7]

4 Information

The *Information Access, Use and Disclosure Policy* applies to all information generated, collected, accessed, used, managed, stored and disclosed by the WA health system including, but not limited to, information collected under the *Health Services Act 2016*, *Mental Health Act 2014*, *Private Hospital and Health Services Act 1927*, *Health (Miscellaneous Provisions) Act 1911* and *Public Health Act 2016*.

4.1 Types and Forms of Information

Information refers to data that has been processed in such a way as to be meaningful to the person who receives it. Data generally refers to unprocessed information. The terms 'data' and 'information' may be used interchangeably and should be taken to mean both data and information. Types and forms of information may include:

- information assets within the WA health system (refer to the WA health system Information Register)
- patient health and personal information
- business/corporate information
- email and other correspondence
- digital files and systems, printed materials, video or sound recordings
- biological samples, physical samples or images
- statistics and graphs
- reports and briefing notes.

4.2 Information Classification

Information classification refers to a business-level process whereby the sensitivity of a piece of information (or collection of information) is evaluated such that the sensitivity will be clear to those who access it subsequently. Information may be classified as either unofficial, official or official: sensitive.

Unofficial information is information that does not relate to official work duties or functions and therefore does not need to be captured or recorded in WA health system information assets or record management systems.

Official information is information created or processed in the WA health system as part of the business of Government including Department of State, System Manager and Health Service Provider functions.

Official: sensitive information is information that could result in damage to individuals, organisations or the government if released. Information at this level commonly includes 'sensitive' material created, used or handled by agencies. This may include content that has limitations restricting its access, use and disclosure.

When accessing, using or disclosing information the information classification and subsequent handling requirements should be considered. Additional information on these classifications can be found in the *Information Classification Policy*.

4.3 Health Information

All references to health information in the *Information Access, Use and Disclosure Policy* refers to the meaning prescribed in the *Health Services Act 2016*.

Health information as defined in the *Health Services Act 2016,* section 213 means personal information, whether collected before, on or after the *Health Services Amendment Act 2023* section 78 comes into operation that:

(a) information, or an opinion, about:

(i) the health (at any time) of an individual; or

(ii) a disability (at any time) of an individual; or

(iii) an individual's expressed wishes about the future provision of health services to the individual; or

(iv) a health service provided, or to be provided, to an individual; or

(b) other personal information collected to provide, or in providing, a health service to an individual.

4.4 Personal Information

The definition of personal information in the *Health Services Act 2016* refers to the meaning given in the *Freedom of Information Act 1992* which is information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead:

(a) whose identity is apparent or can be reasonably ascertained from the information or opinion; or

(b) who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample"[2]

If information is personal, consideration should be given as to whether the information can be collected, accessed, used and/or disclosed lawfully.

5 Access, Use and Disclosure

The terms 'access', 'use' and 'disclosure' are interrelated concepts, however the distinction between these terms is important to understand.

5.1 Information access

An individual, role or group has access to information if they have the right or opportunity to use or view information. An individual enacts this access when they use, view or access the environment in which this information is held.

Note that an individual, role or group must only access information for the purpose for which it has been granted. For example, if a user is granted access to BOSSnet they should only access information relevant to their duties. Where information needs to be accessed, it can be made available in alternative formats if required.

5.2 Information use

An individual, role or group uses information if they employ the information for some purpose, put the information into service, turn the information to account, avail themselves of the information or apply the information for their own purposes.

Within the WA health system, information use refers to the authorised or lawful communication or handling of information by the Department, Health Service Providers and Contracted Health Entities. This includes using information to perform the functions listed in section 20 and 34 of the *Health Services Act 2016*. More specifically, this may include using information to perform functions such as service delivery, policy development, service planning, evaluating health system performance, and identifying emerging risks.

[2] *Freedom of Information Act 1992*

5.3 Disclosure

An individual, role or group discloses information if they cause the information to appear, allow the information to be seen, make the information known, reveal the information or lay the information open to view. Information sharing is considered a disclosure if a person allows information to become available to another person who would not normally have access to it.

5.4 Disclosure models

Detailed information disclosure models can be developed for individual information assets however these models must not contradict any requirements specified in the Information Access, Use and Disclosure Policy. For example, a detailed Information Disclosure Model may specify specific positions that must be consulted before the position with authority to disclose information will approve the disclosure of information from the information asset.

An Access and Disclosure Model could require all users to adopt a Five Safes Framework. At a local level this would be the adoption of the responsible sharing principles. Pre-determined shared controls within a framework could also form part of an Access and Disclosure Model. An Access and Disclosure Model example is provided in Appendix 1.

5.4.1 Disclosure register

Disclosure registers can be developed for individual information assets to assist Custodians and Stewards record and monitor disclosure activity. Typically registers would include:

- recipient details
- request details
- legal purpose
- disclosed data details.

The establishment of a disclosure register also offers Custodians and Stewards a tool to audit and validate disclosure practices. A disclosure register could also include access details if it is considered fit for purpose and appropriate to the specific circumstance of the information asset. A disclosure register example is provided in Appendix 2.

5.5 Multiple users

Access, use and disclosure can be granted for multiple users. Multiple users can include all staff members within the WA health system or a subset of staff members such as a Health Service Provider or a specific group.

5.6 Information requirements in other policies

Health Service Providers and the Department of Health are required to comply with information disclosure requirements mandated in other policies such as the *Clinical Incident Management Policy* and the *Clinical Handover Policy* in the *Clinical Governance, Safety and Quality Policy Framework.*

5.7 Information Sharing Guidelines (*Public Health Act 2016*)

The *Public Health Act 2016* enables the collection of information about the incidence and prevalence of diseases and other public health risks.

Section 300 of the *Public Health Act 2016,* requires the Chief Health Officer to issue guidelines for the disclosure of information prescribed in section 299(3) and (4) of the Act and the request of information prescribed in section 299(5) of the Act.

Under section 299(3) and (4) of the *Public Health Act 2016*, a public health official or an officer of an enforcement agency may, in accordance with the guidelines, disclose relevant information to another public health official, to an officer of an enforcement agency (other than the Chief Health Officer), or to an officer of an information sharing agency.

Under section 299(5) of the *Public Health Act 2016*, a designated officer may, in accordance with the guidelines, request an enforcement agency, a public authority or a department or agency of the government of the Commonwealth, of another State, of a Territory or of another country to disclose relevant information to the designated officer.

The *Information Sharing Guidelines*[8] are a statutory requirement and support the general sharing of 'public health' information. The guidelines do not limit and are separate to the information sharing requirements outlined in Parts 9, 11 and 12 of the *Public Health Act 2016*. More information on the *Public Health Act 2016* is available on the *About the Public Health Act 2016 website*[9].

5.8 Confidentiality

This section should be read in conjunction with:

- the *WA Health Code of Conduct*[11]
- the *Patient Confidentiality Factsheet*[10]
- the *Health Services Act 2016* and any other relevant legislation.

In the WA health system, the privacy of patients is protected through legislation such as section 219 of the *Health Services Act 2016* and the *WA Health Code of Conduct*. There are a number of exceptions to the duty of patient confidentiality, including where:

- express or implied consent has been given for the disclosure by the patient or an authorised representative
- the law either requires or permits the disclosure
- the disclosure is deemed to be in the public interest (authorisation must be sought in this instance)
- the collection, use or disclosure is of a statistical nature or other information that is not personal information
- the collection, use or disclosure of the information is authorised under section 220(1) of the *Health Services Act 2016*.

When using or disclosing information, consideration must be given to the risk of identifying personal information.

5.9 Assurance checks and annual audits

In addition to the policy requirement for Information Management Maturity Assessments, it is a mandated requirement in the *Information Access, Use and Disclosure Standards* to undertake quality assurance checks and annual audits. The aim of the assurance checks and annual audits is to ensure local policies, processes and procedures do not restrict the access, use and disclosure of information to perform legal purposes stipulated in the *Health Services Act 2016*, the *Health Services (Information) Regulations 2017* or other written laws.

The assurance checks and annual audits require a review of existing policies, processes and procedures and an assessment of their impact on information access, use and disclosure when it is permitted or required by law. If a local policy, process, or procedure is inhibiting the lawful access, use and/or disclosure of information it should be reviewed and amended to enable the information to be available to perform the lawful purpose. An assurance check template example is provided in Appendix 3 and an audit template example is provided in Appendix 4.

5.10 Contracted Health Entities

To the extent that requirements in the *Information Access, Use and Disclosure Policy* are applicable to the services purchased from contracted health entities, Health Service Providers must ensure these requirements are accurately reflected in the relevant contract and managed accordingly. In accordance with the *Procurement and Contract Management Policy* it is a mandated requirement for Health Service Providers to manage all contracts and contractors to ensure ongoing compliance with the *Procurement Policy Framework* and government practices and processes. The Procurement and Contract Management Policy also mandates that Health Service Providers must consider whether any policies under the Policy Frameworks are relevant to the delivery of those healthcare services.

5.11 Culture of Information Sharing

A culture of information sharing is a key enabler to maximise information sharing to achieve the System Manager and Health Service Provider functions in accordance with the *Health Services Act 2016* and other written laws. It is a mandated requirement in the *Information Access, Use and Disclosure Standards* to create strategies and mechanisms, such as training and education programs that support a culture of information sharing. The aim of this mandated requirement is to require stakeholders to develop initiatives and resources that promote the access, use and disclosure of information when it is permitted or required by law.

5.12 Commercialisation of Information

Pursuant to section 35(1) of the *Health Services Act 2016* a health service provider may earn revenue by engaging in commercial activities that are not inconsistent with, and do not have an adverse effect on, the performance of its other functions.

The information may be used or disclosed for commercial gain if it is permitted by law. Legal advice should be sought if the identified legal provisions that permit the information to be used for commercial gain are not clear.

The use or disclosure of information for commercial gain for research related projects must comply with *Research Governance Procedures* which includes relevant ethics approvals.

For the protection, management and commercialisation of Intellectual Property generated with State Government resources, compliance with *the Intellectual Property Policy* is also required.

6 Legal Purposes

6.1 Lawful use and disclosure

Disclosure of official and official: sensitive information may be lawful if legislation either requires or permits the use and/or disclosure. In these situations, use and/or disclosure can be made in the absence of an individual's consent without incurring a criminal or civil liability and is not considered a breach of confidentiality or of the code of conduct. Refer to the *Patient Confidentiality Factsheet*[10] for further information.

It should be noted that the applicable legislation can vary depending on the type of information accessed, used, or disclosed. It is the custodian's responsibility to ensure they comply with the relevant legislations associated with their information asset. Therefore, requests to access, use or disclose information should be directed to the relevant custodian who will be able to advise of

any applicable legislative requirements or restrictions. For a list of current custodians refer to the WA health system Information Register.

6.1.1 Required by law

Some legislation requires that certain information must be disclosed. In these circumstances it is lawful to access, use or disclose information in accordance with the legislation. Examples include:

- to comply with the *Health Services Act 2016*, information must be supplied if under an order of a court
- to comply with the *Public Health Act 2016*, medical and nurse practitioners are required to inform the Department of Health about incidences of notifiable infectious diseases.

6.1.2 Permitted by law

There are circumstances where access, use or disclosure of information is permitted and there is no requirement to seek or attain an individual's consent. The *Health Services Act 2016* authorises collection, use or disclosure of information for circumstances such as to perform a function under the Act, including functions in sections 20 and 34, or in another written law. An exhaustive list of circumstances in which information can be collected, used or disclosed can be found in section 220(1) of the *Health Services Act 2016* and in the *Health Services (Information) Regulations 2017*.

6.2 Establishing the Legal Purpose

It is required that the legal purpose for information to be collected, used and/or disclosed is established and any legal caveats or regulations are complied with.

A Purpose Test is a tool to quickly establish the legal purpose for which information can be collected, accessed, used and/or disclosed. This streamlines the process to establish the legal purpose and any legal caveats or regulations. The adoption of a Purpose Test shifts the focus from an assessment based on the operational need to the legal purpose. A Purpose Test also ensures recipients clearly understand the legal purposes for which the information can be accessed, used or disclosed.

An example of a Purpose Test related to the *Health Services Act* is provided in Appendix 5 and examples of the Purpose Test application are provided in Appendix 6.

7 Risk Mitigation

7.1 Misuse, interference, loss, unauthorised access, unauthorised modification

The *WA Health Code of Conduct*[11] requires that employees maintain the confidentiality of any personal or other information that becomes available to them in the course of their employment and to only use the information in connection with their position. An employee accessing, using or disclosing confidential and/or sensitive information must ensure it is protected from misuse, interference, loss, unauthorised access or modification. This includes ensuring that information remains secure while in transit.

Refer to the *Information Security Policy*[12] found within the *Information Communications Technology Policy Framework, and the Information Retention and Disposal Policy*[13] and *Information Storage Policy*[14] in the *Information Management Policy Framework* for more information.

An example of a risk mitigation strategy could include adding the below text to your email signatures:

> *"The contents of this email or its attachments are intended only for the use of the addressee(s). If you are not the intended recipient of this email any use, interference with, disclosure, distribution or copying of this material is unauthorised and prohibited. If you receive this in error, please notify the sender by return e-mail, delete the email and attachments from your system and destroy any copies you have taken of the email and attachments".*

7.2 Risk assessment

As a custodian when using or disclosing information it is important to include safeguards to ensure confidentiality is not breached and that personal information is handled appropriately. Consequences of breaches are damaging to both patients and the WA health system. The likelihood of inappropriate use or disclosure occurring should be assessed by both user and discloser. A risk assessment ensures that the operational purpose and function do not compromise the integrity of information or the organisation.

7.2.1 Five Safes Frameworks

Although many different types of risk mitigation strategies have been developed to manage information sharing, a growing consensus internationally is the adoption of a Five Safes Framework.[15,16] The framework promotes information sharing by allowing users to effectively

manage sensitive and/or confidential information. On a national level the Australian Bureau of Statistics has also adopted a Five Safes Framework approach.

The Productivity Commission recommended the development of a *Commonwealth Data Sharing and Release Bill* to unlock the potential of data. A key element of the proposed legislation is to ensure appropriate best practice risk management which includes the implementation of a Five Safes Framework.[17] The Five Safes Framework allows information users to assess, identify and implement controls and risk mitigation strategies. It shifts the ownership of risk management to all stakeholders. Research suggests that stakeholders typically consider risks from their work-related perspective.[15]

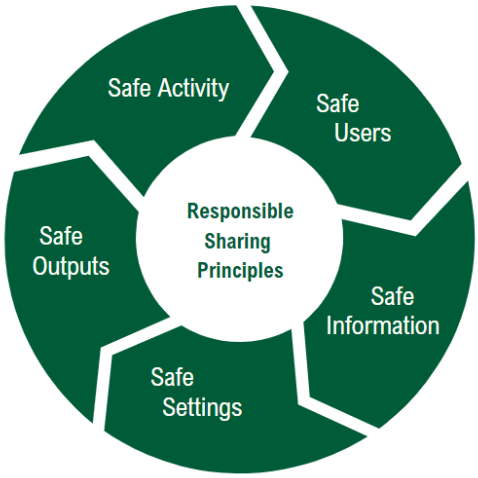
7.2.1.1 Responsible Sharing Principles

At a local level, the Responsible Sharing Principles mandated in the Information Access, Use and Disclosure Standards are based on a Five Safes Framework.

As illustrated in

Figure below, the Responsible Sharing Principles broadens the information users' focus on managing and controlling risks in five key areas.

Figure 3: Responsible Sharing Principles



Source: Modified from Privacy and Responsible Information Sharing for the Western Australian public sector: Discussion paper

Table 1 provides information users a checklist to ensure risk mitigation strategies are considered for each of the risk areas in the Responsible Sharing Principles when accessing, using and disclosing information. The degree of controls in place is dependent on the sensitivity and confidentiality of information. This approach shares the risk burden between custodians and information users within the WA health system. It also lessens the risk of information breaches. For more information refer to the *Information Breach Policy*. A template and working example are provided in Appendix 7.

If a custodian has made an assessment using the Responsible Sharing Principles, it can be shared with other custodians to improve the timeliness of access to information and reduce duplication.

Table 1: Responsible Sharing Principles Risk Mitigation Strategy Checklist

User Checklist	
Safe Activity	• Is the activity for which information is to be shared and used appropriate? • Is it for the public good and will it provide value? • Are there unreasonable risks or detriments if the sharing does not occur?
Safe Users	• Is the organisation receiving the information an appropriate recipient? • Do their staff have the right level of skills and experience? • Will they restrict the information to the right people?
Safe Settings	• Is the setting in which the information will be stored, accessed and used appropriate? • Does it have the right level of security? • What is the likelihood of deliberate or accidental disclosure?
Safe Information	• Is the information to be shared appropriate for the proposed purpose? • If the data is to be de-identified, how will this occur?
Safe Outputs	• Is the proposed publication or disclosure of the information appropriate? • What is the risk of identifying individuals?

Source: Modified from Privacy and Responsible Information Sharing for the Western Australian public sector: Discussion paper

7.3 Identification of Risk Treatments

The Australian Bureau of Statistics have developed guidance on how to assess and treat identification risks in microdata and aggregated datasets. Information users when disclosing

information may assess these risks as part of applying the 'Safe Information' and 'Safe Outputs' elements of the Responsible Sharing Principles.

The information on the adoption of appropriate risk management practices for microdata and aggregate datasets is available from the Australian Bureau of Statistics' *Managing the Risk of Disclosure: Treating Microdata* and *Managing the Risk of Disclosure: Treating Aggregate Data* webpages.

7.4 Synthetic vs. Masked data

A risk mitigation strategy to avoid legal restrictions and to address privacy concerns is to use synthetic data. Synthetic data is artificially manufactured and generally has similar statistical properties to the original data. The data is not real and only uses statistical and machine learning methodologies to mimic the original data.

Stakeholders sometimes use masked data as an alternative to synthetic data. Masked data is when the original data is amended, modified or transformed. Masked data is not synthetic data as it is a modified version of the original data. A key disadvantage of masked data is that there is a risk the masked data could be transformed back into the original data and/or be re-identified. Another disadvantage of masked data is that it does not negate the legal restrictions. It is important to note that data that has been de-identified is masked data.

Synthetic data instead of masked data should be considered as an alternative to the original data when there are legal restrictions or privacy concerns. For further information on synthetic data refer to *Research Paper – Synthetic Business Microdata – A Possible Dissemination Tool, Australian Bureau of Statistics and ANU*.

Synthetic data can be used by stakeholders to better understand the data elements and parameters. Stakeholders such as researchers and external parties are sometimes able to use synthetic data to meet their needs without requiring access to the original data.

The quality of the synthetic data is sometimes a potential weakness. The quality depends on the original data set parameters as well as the methodology employed to create the synthetic data set. There are several methodologies employed to produce synthetic data. The distribution-based model is generally the most common method adopted to generate synthetic data. Other common models typically use machine learning techniques and data algorithms to mimic the relationship between the original data variables.

8 Information Management Governance

The State of Western Australia is the statutory owner of all assets including information assets. Section 29(1)c of the *Public Sector Management Act 1994* requires that CEOs and chief employees undertake and plan for information management. Further to this, section 214(3) of the *Health Services Act 2016* states that "Information in a health information management system is held on behalf of the State".

Information access, use and disclosure authorisations at a system-wide level are described in legislation, instruments of delegation and mandatory policies. These mandatory requirements should be supported by local policies, procedures and guidelines that promote information management governance through detailed authorisations, roles and responsibilities.

The *Information Management Governance Policy* is a key policy in the *Information Management Policy Framework*. The policy mandates the governance model for the management of information contained within information management systems. This includes delegated authorities, roles and responsibilities for access, use and disclosure of the information within the information management governance model.

8.1 WA health system Information Register

Information assets from across the WA health system are collectively listed in the *WA health system Information Register*. Details listed in this register include the information asset name, information asset description, and the delegated officers responsible for the information asset. The document is dynamic and may not necessarily be exhaustive at any given time.

The WA health system Information Register is maintained by the Information and Performance Governance Unit within Information and System Performance Directorate at the Department of Health.

8.2 Information Management delegation schedule

The Director General has delegated their powers relating to the collection, use and disclosure of health information under Part 17 of the *Health Services Act 2016* to employees of the Department and staff members of each health service provider as specified in the Department CEO Instrument of Delegation Health Information made under section 24 of the *Health Services Act.*

8.3 Requesting and authorising information disclosure

It is a mandated requirement to maintain information request and disclosure policies, processes and/or procedures that support the access, use and disclosure of information for legal purposes in the *Health Services Act 2016*, the *Health Services (Information) Regulations 2017* or in other written laws, excluding the FOI Act. An information request form, an information disclosure form,

an information disclosure contract and/or a memorandum of understanding could be adopted to achieve this mandated requirement.

It is, however, at the discretion of the authorising authority to determine, for their circumstance, what local policies, processes and/or procedures best support the access, use and disclosure of information. If forms are adopted, they can be generic or fit for purpose to address a specific need or circumstance. The sections below provide generic examples of information request and disclosure forms, and an information disclosure contract. An example is also available of an information request form and disclosure checklist that has been designed to meet the specific circumstances relating to the disclosure of health information for the planning provision, monitoring and evaluation of public services and health related research.

8.3.1 Information request form

The primary aim of an information request form is to ensure information users have access to information that allows them to undertake legal purposes that they are authorised to perform by law. The form should accommodate information requests for ongoing open access to part or all of the information held when it is required or permitted for legal purposes that are authorised in the *Health Services Act 2016*, the *Health Services (Information) Regulations 2017* or in any other written laws.

The key aim of an information request form is to:

- ensure that health information requested is required or authorised by law
- provide details of information recipients and the purpose for which the information is requested
- ensure that appropriate authorisations have been sought by the requestor
- provide sufficient detail to ensure that the information disclosed is timely and fit for purpose.

An Information Request Form could include:

- the information requester's details (i.e., name, position, work location and contact details)
- the information recipient's details (if not the same as the requester)
- the information asset(s) from which the health information will be sourced (if known)
- the legal purpose(s) for which the health information is required
- acknowledgement of compliance with any disclosure and confidentiality provisions and conditions required by law for the legal purpose(s) being undertaken
- parameters of information required
- list of persons, roles or groups who will access the information (the form should accommodate requests made on behalf of groups for ongoing legal purposes)
- details of the risk controls which will be adopted to safely secure and protect sensitive, confidential and appropriately classified information

- details of how the health information will be stored securely
- details of how the health information will be disseminated to others and to who the information will be disseminated, if any
- health information retention period and intended/required means of disposal (refer to the Information Retention and Disposal Policy for further information).

Ongoing authorisations must be renewed on an annual basis as prescribed in the Information Access, Use and Disclosure Policy.

An example of the information request form is provided in Appendix 8.

8.3.2 Information disclosure form

The key purpose of an information disclosure form is to ensure the information recipients are provided with:

- details about the information such as any caveats associated with the information
- details regarding where the information is sourced
- contact details of a subject matter expert that may be contacted for further details.

The disclosure of information could consider the following:

- compliance with the *Information Access, Use and Disclosure Policy*
- compliance with the *Information Access, Use and Disclosure Standards*
- consideration of the sensitivity and risk classification of information (refer to the *Information Classification Policy*).

An Information Disclosure Form could include:

- person, role or group who supplied the information
- person, role or group who are granted access and use of the disclosed information
- contact details of a subject matter expert for enquiries in relation to the information
- the legal purpose(s) for which the information is being supplied
- information system(s) from which the information was extracted, including data warehouses if applicable
- health information specifications, limitations and caveats
- evidence of HREC approval where applicable
- evidence of approval in accordance with the relevant statutory or delegated authority.

An example of an information disclosure form is provided in Appendix 9.

8.3.3 Information disclosure contract

The purpose of an information disclosure contract or a memorandum of understanding is to ensure information recipients understand the conditions of information disclosure and the obligations associated with receiving the information. An information disclosure contract or a memorandum of understanding could be completed when confidential and/or sensitive information is being disclosed to third parties outside of the WA health system.

The key aims of an information disclosure contract are to:

- define the conditions for access and use under which the information is provided
- ensure information is accessed, used and stored in a manner which is secure and protected
- ensure there are conditions in place relating to third party disclosure
- support information breach protocols.

An example of an information disclosure contract is provided in Appendix 10. Note that the information disclosure contract example does not apply to research as a Data Transfer Agreement Form is used for this purpose.

8.4 Access, Use and Disclosure of Information for Research Purposes

Research, as defined in the *Research Governance Procedures* is the original investigation undertaken to gain knowledge, understanding and insight as described in the National Health and Medical Research Council's "*Australian Code for the Responsible Conduct for Research*" 2018.

Access, use and disclosure of information for research purposes require specific governance processes. These processes may be specific to local collections, and local policies, procedures and guidelines.

One such governance process is ethical review of research projects. Research projects must undergo ethical review and approval through a Human Research Ethics Committee (HREC) in accordance with the *Research Governance Procedures*. Reviews are based on the *National Statement on Ethical Conduct in Human Research (2023)* which was developed in accordance with the *National Health and Medical Research Council Act 1992*.[18] Projects that require approval from a WA health system HREC for research purposes include:

- requests for information by individual's external to the WA health system
- research projects involving the use and disclosure of information from information assets held by the WA health system
- requests deemed by the custodian to be sensitive or requiring ethics approval.

Other governance processes may include approvals by Stewards through a governance policy or by a research governance officer.

Requests for information to undertake research must be approved in accordance with the *Research Policy Framework*[19] requirements.

Glossary

Term	Meaning
Access	Refers to the right or opportunity to use or view information. An individual enacts this access when they use, view or enter the environment in which this information is held.
Aggregated information	Is summed and/or categorised information that is analysed and placed in a format (for example, in tables or graphs) that prevents the chance of revealing an individual's identity (individual records cannot be reconstructed).
Approved governance model	Refers to a model that has been approved by the relevant authorising authority to govern the access, use, disclosure and sharing of information when it is lawful. The governance model must comply with other mandated policies and the relevant authorisation and delegations schedule.
Custodian	Implements Policy on behalf of the Steward and has the delegated authority for granting access, use and disclosure of information from information assets in line with legislation and policy.
Data	The term 'data' generally refers to unprocessed numbers, facts or statistics, while the term 'information' refers to data that has been processed in such a way as to be meaningful to the person who receives it. The terms 'data' and 'information' are often used interchangeably and should be taken to mean both data and information.
Disclosure	A person discloses information if they cause the information to appear, allow the information to be seen, make the information known, reveal the information or lay the information open to view.
De-identified	Personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonable identifiable.
Duty of confidentiality	Obligation imposed on persons by common law, statute and /or equity which requires that information of a certain character (e.g. personal or otherwise sensitive information) be treated in confidence by those to whom it is made known or becomes known.

Term	Meaning
Health information	As defined in the *Health Services Act 2016,* section 213 means personal information, whether collected before, on or after the *Health Services Amendment Act 2023* section 78 comes into operation that: (a) information, or an opinion, about: (i) the health (at any time) of an individual; or (ii) a disability (at any time) of an individual; or (iii) an individual's expressed wishes about the future provision of health services to the individual; or (iv) a health service provided, or to be provided, to an individual; or (b) other personal information collected to provide, or in providing, a health service to an individual.
Information	The term 'information' generally refers to data that has been processed in such a way as to be meaningful to the person who receives it. Information can be personal or non-personal in nature. The terms 'data' and 'information' are often used interchangeably and should be taken to mean both data and information in this Policy.
Information Asset	A collection of information that is recognised as having value for the purpose of enabling the WA health system to perform its clinical and business functions, which include supporting processes, information flows, reporting and analytics.
Legal purpose	Refers to the purpose that is authorised by the *Health Services Act 2016,* the *Health Services (Information) Regulations 2017* or any other written laws. It does not refer to the operational purpose or an operational fit-for-purpose assessment.
Masked data	A modified version of the original data that has been amended, modified or transformed.
Non-personal information	Information from which a person's identity is not apparent, and cannot be reasonably ascertained. Whether information is truly non-personal will depend on the context, including the nature of the information, the number of people to whom it could potentially relate and the amount of information proposed to be disclosed. Although a series of individual pieces of information may not, on their own, enable the identity of an individual to be ascertained, identification may occur when all the pieces of information are combined together.
Operational purpose	Refers to the purpose that an operational activity, action or procedure is undertaken. It does not refer to the legal purpose that an activity, action or procedure is undertaken.

Term	Meaning
Personal information	Has the meaning given in the Freedom of Information Act 1992 in the Glossary clause 1: Means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead — (a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or (b) who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.
Reasonably identifiable	Reasonably identifiable information is personal information. It includes information such as an individual's name, image, date of birth or address; information that contains a unique personal identifier when the holder of the information also has the master list linking the identifiers to individuals; and information that the holder can merge or link to other information they already hold, enabling them to identify individuals.
Research	Original investigation undertaken to gain knowledge, understanding and insight as described in the National Health and Medical Research Council "Australian Code for the Responsible Conduct for Research" 2018. The concept of research is broad and includes the creation of new knowledge and/or the use of existing knowledge in a new and creative way so as to generate new concepts, methodologies, inventions and understandings. This could include synthesis and analysis of previous research to the extent that it is new and creative.[3]
Sensitive Information	Refers to information that might result in an adverse impact on an individual, the WA health system, the government and/or other third parties.
Sponsor	Assists the Steward in operation of managing allocated Information Assets outlined in the relevant delegation schedule.
Steward	The delegated authority for the information assets outlined within the associated delegation schedule.
Synthetic data	Artificially manufactured data that mimics the statistical properties of the original data.

[3] Source: Australian Code for the Responsible Conduct for Research 2018

Term	Meaning
Use	A person ‘uses’ information if they utilise, handle, collect or communicate information within the WA health system or employ information for a purpose.

References

1 Australian Government. (2017). *Data Availability and Use – Inquiry Report.* Productivity Commission, Australian Government, Canberra. Available from: https://www.pc.gov.au/inquiries/completed/data-access/report (accessed 17 June 2019).

2 Australian Government. (2018). *New Australian Government Data Sharing and Release Legislation: Issues paper for consultation.* Department of the Prime Minister and Cabinet, Australian Government, Canberra. Available from: New Australian Government Data Sharing and Release Legislation — submission to Department of Prime Minister and Cabinet | OAIC (accessed 17 June 2019).

3 Western Australian Government. (2022). *Privacy and Responsible Information Sharing.* Department of Premier and Cabinet, WA Government, Perth. Available from: https://www.wa.gov.au/government/privacy-and-responsible-information-sharing (accessed 15 June 2023)

4 Western Australian Government. (2015). *Whole of Government Open Data Policy.* Department of Premier and Cabinet, WA Government, Perth. Available from: Open Data Policy (accessed 17 June 2019).

6 Western Australian Government. (2017). *From Death We Learn 2016 (2017 Edition).* Department of Health, Perth. Available from: From Death We Learn (health.wa.gov.au) (Accessed 18 June 2019).

7 Western Australian Government. (2018). *From Death We Learn 2017 (2018 Edition).* Department of Health, Perth. Available from: https://ww2.health.wa.gov.au/~/media/Files/Corporate/Reports%20and%20publications/PDF/From-Death-We-Learn-2017.pdf (Accessed 18 June 2019).

8 Western Australian Government. (2017). *Chief Health Officer Information Sharing Guidelines: For the purposes of sections 299 and 300 of the Public Health Act 2016.* Department of Health, Perth. Available from: https://ww2.health.wa.gov.au/~/media/Files/Corporate/general%20documents/Public%20Health%20Act/CHO-Information-Sharing-Guidelines.pdf (Accessed 20 August 2019).

9 Western Australian Government. (2017). *About the Public Health Act 2016 webpage.* Department of Health, Perth. Available from: https://ww2.health.wa.gov.au/Improving-WA-Health/Public-health/Public-Health-Act (Accessed 20 August 2019).

10 Western Australian Government. (2021). *Patient Confidentiality Factsheet.* Department of Health, Perth. Available from: https://doh-healthpoint.hdwa.health.wa.gov.au/directory/Governance%20and%20System%20Support/GovernanceandSystemSupport/Legal-and-Legislative-Services/Documents/Patient-Confidentiality.pdf (Accessed 8 December 2021).

[11] Western Australian Government. (2017). *Code of Conduct.* Department of Health, Perth. Available from: Code of Conduct Policy (health.wa.gov.au) (Accessed 18 June 2019).

[12] Western Australian Government. (2017). *Information Security Policy,* Department of Health, Perth. Available from: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-and-Communications-Technology/Mandatory-requirements/Information-Security-Policy (Accessed 18 June 2019).

[13] Western Australian Government. (2020). *Information Retention and Disposal Policy,* Department of Health, Perth. Available from: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-Management/Mandatory-requirements/Storage-and-Disposal/Information-Retention-and-Disposal-Policy (Accessed 14 February 2022).

[14] Western Australian Government. (2014). *Information Storage Policy,* Department of Health, Perth. Available from: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-Management/Mandatory-requirements/Storage-and-Disposal/Information-Storage-Policy (Accessed 18 June 2019).

[15] Desai T. Ritchie F. and Welpton R. (2014). *The Five Safes: working paper*, University of the West of England, UK.

[16] Desai T. Ritchie F. and Welpton R. (2015). *The Five Safes: designing data access for research*, University of the West of England, UK.

[17] Australian Government. (2018). *New Data Sharing Release Legislation: Premier and Cabinet Roundtable Presentation*, Office of the National Data Commissioner, Australian Government, Canberra, Australia.

[18] Australian Government. (2007). *National Statement on Ethical Conduct in Human Research (updated 2018).* National Health and Medical Research Council, Australian Government, Canberra. Available from: https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018 (accessed 17 June 2019).

[19] Western Australian Government. (2017). *Research Policy Framework,* Department of Health, Perth. Available from: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Research (Accessed 18 June 2019).

Appendix 1: Access and Disclosure Model Example

	Information Classification		
	Unofficial	**Official**	**Official: Sensitive**
Purpose for which the information is accessed and/or disclosed	**Information not related to official work duties or functions (the information is not part of the business of Government including Department of State, System Manager and Health Service Provider functions)**	**Information created or processed in the WA health system as part of the business of Government including Department of State, System Manager and Health Service Provider functions**	**Official information that could result in damage to individuals, organisations or government if released**
For a legal purpose authorised in the *Health Services Act 2016*	Not applicable	Approved by Custodian in accordance with the *Information Access, Use and Disclosure Policy – MP 0015/16* or any other relevant policies	Approved by Custodian, Sponsor and/or Steward in accordance with the *Information Access, Use and Disclosure Policy – MP 0015/16* or any other relevant policies
For a legal purpose authorised by other written laws	Not applicable	Approval by the Custodian or the relevant authorising authority in accordance with the applicable legislation and policies	Approval by the Custodian, Sponsor and/or Steward or the relevant authorising authority in accordance with the applicable legislation and policies
Freedom of Information	Not applicable	Approved by the Custodian or the relevant authorising authority in accordance with the *Freedom of Information Act 1992*	Approved by the Custodian, Sponsor and/or Steward or the relevant authorising authority in accordance with the *Freedom of Information Act 1992*
Research	Not applicable	Approved by Custodian and the relevant authorising authorities in accordance with the *Research Governance Policy – MP 0162/21* or any other applicable policy or procedure	Approved by Custodian, Sponsor and/or Steward and relevant authorising authorities in accordance with the *Research Governance Policy – MP 0162/21* or any other applicable policy or procedure
Other (e.g. media inquiries, Ministerials, PQs or other external queries)	Approval by the relevant authorising authority in the *Department of Health Authorisations and Delegations Schedule* or in accordance with any other applicable instrument, policy or procedure	Approval by the Custodian or the relevant authorising authority in the *Department of Health Authorisations and Delegations Schedule* or in accordance with any other applicable instrument, policy or procedure	Approval by the Custodian, Sponsor and/or Steward or the relevant authorising authority in the *Department of Health Authorisations and Delegations Schedule* or in accordance with any other applicable instrument, policy or procedure

Note: An Access and Disclosure Model could require all users to adopt a Five Safes Framework. Pre-determined shared controls within a framework could also form part of an Access and Disclosure Model. Note: The Custodian and Steward are listed in the WA health system Information Register.

Appendix 2: Disclosure Registry Example

Disclosure Date	Authorising Officer	Recipient(s) details	Information Description (type and form	Information Classification	Legal Purpose	Disclosure checklist completed
7 Aug 23	John Smith	Detective Johnston	Information Patient Client Records	Official: Sensitive	Disclosed under section 220(f) under an order of a court or other person or body acting judicially	Completed

Appendix 3: Assurance Check Template Example

Quality Assuror name:

Quality Assurance date:

Policy/Process/Procedure title:

	Quality Assurance Questions	Quality Assurance Response Yes/No/NA	Issues and/or gaps identified	Actions required	Officer Responsible	Scheduled Action Completion Date
	1. Is the policy/process/procedure aligned to the Information Management Policy Framework principles?					
	2. Does the policy/process/procedure support the realisation of the WA health system's vision to deliver a safe, high quality, sustainable health system for all Western Australians?					
	3. Does the policy/process/procedure support the System Manager and Health Service Provider functions in accordance with the *Health Services Act 2016* and other written laws?					
	4. Does the policy/process/procedure facilitate improvements in effectiveness and efficiency of service delivery such as in safety and quality					
	5. Does the policy/process/procedure improve transparency and accountability?					
	6. Does the policy/process/procedure allow better and more informed decision making?					
	7. Does the policy/process/procedure enable stakeholders to understand when information is authorised to be accessed, used or disclosed?					

	Quality Assurance Questions	Quality Assurance Response Yes/No/NA	Issues and/or gaps identified	Actions required	Officer Responsible	Scheduled Action Completion Date
	8. Does the policy/process/procedure enable stakeholders to access, use, disclose and share information when it is lawful to do so and through an approved governance model?					
	9. Does the policy/process/procedure enable stakeholders to access, use, disclose and share information in a manner that protects the privacy of patients including sensitive and appropriately classified information?					
	10. Does the policy/process/procedure promote a culture that encourages information sharing when permitted by law?					
	11. Does the policy/process/procedure enable stakeholders to protect information from misuse and inappropriate access and disclosure?					
	12. Does the policy/process/procedure enable stakeholders to ensure volunteers comply with any mandated requirements?					
	13. Does the policy/process/procedure enable stakeholders manage contracted health entities to ensure compliance with any mandated requirements?					
	Other questions as deemed appropriate for the policy/process/procedure.					

Appendix 4: Audit Template Example

Audit: Health Service Provider/Hospital

Auditor's name:

Audit date:

Policy/Process/Procedure(s) Name and Details	Quality Assured? Yes/No	Issues and/or gaps identified	Audit actions and/or recommendations

Appendix 5: Purpose Test

Section 34 – HSA 2016
Functions of Health Service Provider
(1) A health service provider's main function is to provide —
(a) health services stated in the service agreements for the health service provider; and
(b) teaching, training and research that supports the provision of health services as agreed with the Department CEO; and
(c) any other services agreed with the Department CEO.
(2) A health service provider also has the following functions —
(a) to ensure the operations of the health service provider are carried out efficiently, effectively and economically;
(b) to enter into, and comply with, service agreements with the Department CEO and, if appropriate, with the Commission CEO;
(ba) to do any or all of the following under a service agreement for the purposes of section 20A —
(ii) commission and deliver capital works or maintenance works;
(ii) carry out clinical commissioning of facilities
(c) to comply with the policy frameworks and Department CEO directions that apply or relate to the health service provider;
(d) to contribute to the development of, and implement, WA health system wide plans that apply to the health service provider and undertake further service planning that aligns with the WA health system wide plans;
(e) to prepare and keep under review strategies —
(i) for the provision of health services by the health service provider; and
(ii) to promote consultation with health professionals working in the health service provider; and
(iii) to promote consultation with health consumers and community members about the provision of health services by the health service provider;
(f) to establish an efficient and effective procedure for dealing with complaints about the provision of health services by the health service provider;
(g) to report to the Department CEO on the provision of health services by the health service provider;
(h) to monitor and improve the quality of health services provided by the health service provider;
(i) to develop and implement corporate and clinical governance arrangements for the health service provider;
(j) to maintain land, buildings and other assets controlled and managed by the health service provider;
(k) to cooperate with other providers of health services, including providers of primary health care, in planning for, and providing, health services;
(l) subject to any Department CEO direction and the State Supply Commission Act 1991, to arrange for the provision of health services by contracted health entities;
(m) to manage the performance of the health service provider against the performance measures and operational targets stated in the service agreements;
(n) to provide performance data, other data and any other information the Department CEO may require to the Department CEO;
(o) other functions imposed under this Act or another written law;
(p) other functions necessary or incidental to the functions mentioned in paragraphs (a) to (o).
(3) In subsection (2)(i) -
clinical governance arrangements means policies, processes and systems for maintaining and improving —
(a) patient safety, quality and care; and
(b) the effectiveness and dependability of services provided by a health service provider.

Section 20 – HSA 2016
Functions of Department CEO
(1) The functions of the Department CEO include:
(a) advising and assisting the Minister in the development and implementation of WA health system wide planning;
(b) providing strategic leadership and direction for the provision of public health services in the State;
[(c) deleted]
(d) promoting the effective and efficient use of available resources in the provision of public health services in the State;
(e) carrying out certain functions of health service providers as specified in service agreements pursuant to section 51;
(f) managing WA health system wide industrial relations on behalf of the State, including the negotiation of industrial agreements, and making applications to make or vary awards;
(g) subject to subsection (3), commissioning and delivering capital works and maintenance works for public health service facilities;
[(h) deleted]
(i) establishing the conditions of employment for employees in health service providers in accordance with the requirements of any binding award, order or industrial agreement under the Industrial Relations Act 1979;
(j) arranging for the provision of health services by contracted health entities;
(k) providing support services to health service providers;
(l) overseeing, monitoring and promoting improvements in the safety and quality of health services provided by health service providers;
(m) monitoring the performance of health service providers, and taking remedial action when performance does not meet the expected standard;
(n) receiving and validating performance data and other data provided by service providers;
(na) collecting performance data and other information from health service providers;
(o) other functions given to the Department CEO under this or another Act.

Section 20A – HSA 2016
Works and clinical commissioning

If the legal purpose is to undertake other functions under sections 20(o), 34(o) or 34(p), the functions need to be identified.

If the legal purpose is use and disclosure by consent compliance with the Patient Confidentiality Policy is required.

Purpose Test
(Identify the legal purpose)

Section 220 (1) – HSA 2016
For the purposes of this Act, the collection, use or disclosure of information is authorised if the information is collected, used or disclosed in good faith in any of these circumstances:
(a) for the purpose of, or in connection with, performing a function under this Act or another written law;
(b) for the purposes of section 215 or Division 2;
(c) otherwise under this Act, including in response to a request made under section 61 or 218(2);
(d) under another law;
(e) to a court or other person or body acting judicially in the course of proceedings before the court or other person or body;
(f) under an order of a court or other person or body acting judicially;
(g) for the purposes of the investigation of a suspected offence or disciplinary matter or the conduct of proceedings against a person for an offence or disciplinary matter;
(h) if the information collected, used or disclosed is personal information — with the consent of the individual, or each individual, to whom the personal information relates;
(i) any other circumstances prescribed for this subsection.

If the legal purpose is for another written law the authorised purpose needs to be identified.

Health information as defined in the *Health Services Act 2016,* section 213 means personal information, whether collected before, on or after the *Health Services Amendment Act 2023* section 78 comes into operation that:

Section 216 - HSA 2016 (Part of Division 2)
The Department CEO may, in accordance with the regulations, collect, use and disclose information, including health information, for any of the following purposes —
(a) the administration or enforcement of this Act;
(b) the management of health service providers;
(c) the planning for, provision, monitoring and evaluation of public health services;
(d) health related research, whether that research is conducted by persons who are staff members of a health service provider or persons employed or engaged in the Department or other persons.

Health Services (Information) Regulations 2017
Regulation 3. Disclosure of information by Department CEO (s. 216)
(1) In this regulation:
HREC means a human research ethics committee constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research*, as in force from time to time, issued under the *National Health and Medical Research Council Act 1992* (Commonwealth) section 7(1)(a).
(2) The Department CEO must not disclose health information under section 216 unless —
(a) the individual to whom the information relates consents to the disclosure; or
(b) the Department CEO is satisfied that —
(i) disclosure of the information is reasonably necessary for the purpose for which it is to be disclosed; and
(ii) the purpose for which the information is to be disclosed cannot be achieved by providing information that is not personal information; and
(iii) it is impracticable to obtain the consent of the individual to whom the information relates.
(3) In addition to the requirements of subregulation (2), the Department CEO must not disclose health information under section 216 for the purpose of health related research unless the research has been approved by an HREC.

Section 217 - HSA 2016 (Part of Division 2)
(1) In this section - relevant information means health information that, in the opinion of the chief executive of a health service provider, is or is likely to be relevant to any of the following:
(a) the treatment or care of a patient who has been, is being, or will or may be, provided with a health service by the health service provider;
(b) the health, safety or wellbeing of a patient who has been, is being, or will or may be, provided with a health service by the health service provider.
(2) The chief executive of a health service provider may, in accordance with the regulations, disclose relevant information about a patient of the health service provider to any person who, in the opinion of the chief executive, has a sufficient interest in the treatment, care, health, safety or wellbeing of the patient.

Section 217A – HSA 2016
Disclosure of health information in health information management system under legal process

Health Services (Information) Regulations 2017
Regulation 4. Disclosure of information by health service provider (s. 217)
The chief executive of a health service provider must not disclose health information to a person under section 217(2) if:
(a) the chief executive reasonably believes that disclosure of the information would pose a serious threat to —
(i) the life, health or safety of any individual; or
(ii) public health or safety; or
(b) disclosure of the information would have an unreasonable impact on the privacy of the patient or another person; or
(c) the patient has requested that the information not be disclosed to the person.

Health Services (Information) Regulations 2017
Regulation 5. Circumstances in which collection, use or disclosure of information is authorised (s. 220)
(1) For the purposes of section 220(1), the collection, use or disclosure of information is authorised in the following circumstances —
(a) the collection, use or disclosure is reasonably necessary to lessen or prevent a serious risk to the life, health or safety of any individual;
(b) the collection, use or disclosure is reasonably necessary to lessen or prevent a real or immediate risk of danger to the public;
(c) the collection, use or disclosure is for a purpose specified in a written agreement between the State and the Commonwealth, another State or a Territory entered into by a Minister of the State or the Department CEO;
(d) the collection, use or disclosure is for the purposes of, or in connection with, obtaining legal advice or representation on behalf of —
(i) the Department CEO or the State; or
(ii) a health service provider; or
(iii) an individual who is or was a staff member of a health service provider if the individual is indemnified by the State in respect of liability incurred by the individual as a staff member of the health service provider;
(e) the collection, use or disclosure is for the purposes of, or in connection with, an application to the State Administration Tribunal for a guardianship order or an administration order under the Guardianship and Administration Act 1990.
(2) For the purposes of section 220(1), the disclosure of information is also authorised in the following circumstances —
(a) the disclosure is to an individual who is or was a staff member of a health service provider for the purposes of the individual's compliance with reporting requirements under another law;
(b) the information relates to an individual who is deceased and the disclosure is in response to a written request from —
(i) a coroner, a coroner's registrar, a coroner's investigator or a member of the staff of a coroner's court in connection with an investigation into the death of the individual; or
(ii) a medical practitioner who is performing a post mortem on the body of the individual at the direction of a coroner.

Appendix 6: Purpose Test Application Examples

Example 1

Task:
You work for the Department of Health and want to use financial and workforce information to improve the efficiency of the WA health system.

Purpose Test:
Under Section 220(1)(a) of the *Health Services Act 2016* the collection, use or disclosure of information is authorised if the information is collected, used or disclosed in good faith for the purpose of, or in connection with, performing a function under this Act or another written law. System manager functions under the Act are listed in Section 20 of the *Health Services Act 2016*. The function that you are undertaking is in connection to Section 20(1)(d) to promote the effective and efficient use of available resources in the provision of public health services in the State.

Purpose Test Result:
The legal purpose is to perform the function listed in Section 20(1)(d) of the *Health Services Act 2016.*

Example 2

Task:
You work for a public hospital and want to use inpatient information to assess the effectiveness of a new program.

Purpose Test:
Under Section 220(1)(a) of the *Health Services Act 2016* the collection, use or disclosure of information is authorised if the information is collected, used or disclosed in good faith for the purpose of, or in connection with, performing a function under this Act or another written law. Health service provider functions under the Act are listed in Section 34 of the *Health Services Act 2016*. The function that you are undertaking is in connection to Section 34(2)(a) to ensure the operations of the health service provider are carried out efficiently, effectively and economically.

Purpose Test Result:
The legal purpose is to perform the function listed in Section 34(2)(a) of the *Health Services Act 2016.*

Example 3

Task:
You work for a health service provider and want to use information from the cancer registry to evaluate the effectiveness of services provided to cancer patients.

Purpose Test:
Under Section 220(1)(d) of the *Health Services Act 2016* the collection, use or disclosure of information is authorised if the information is collected, used or disclosed in good faith for another written law. The information in the cancer registry is a statutory collection under the *Health (Miscellaneous Provisions) Act 1911* and *Health (Western Australian Cancer Registry) Regulations 2011*. Regulation 10(4)(a) of the regulations permits information from the cancer registry to be kept for the purposes of planning, monitoring and evaluation of services for the control of cancer and the care of cancer patients in Western Australia.

Purpose Test Result:
The legal purpose is to perform the purpose permitted under regulation 10(4)(a) of the *Health (Western Australian Cancer Registry) Regulations 2011* which is to evaluate services for the care of cancer patients.

Example 4

Task:
You work for the Department of Health and want to benchmark health service provider performance to identity safety and quality improvement opportunities.

Purpose Test:
Under Section 220(1)(a) of the *Health Services Act 2016* the collection, use or disclosure of information is authorised if the information is collected, used or disclosed in good faith for the purpose of, or in connection with, performing a function under this Act or another written law. The System Manager functions under the Act can be identified in the Section 20. The function that you are undertaking is in connection to Section 20(l)) to oversee, monitor and promote improvements in the safety and quality of health services provided by health service providers.

Purpose Test Result:
The legal purpose is to perform the function listed in Section 20(l) of the *Health Services Act 2016.*

Other Examples:
For additional information, including subpoena's and patient confidentiality refer to the factsheet on Legal and Legislative Services Unit (health.wa.gov.au)

Appendix 7: Responsible Sharing Principles

The Responsible Sharing Principles allows users and disclosers to identify risks and implement controls and risk mitigation strategies. It ensures information risk management is a consideration across the organisation when information sharing is occurring.

The column to be completed in the template below is dependent on the information that has been received or being disclosed. It is the responsibility of the information recipient to have the appropriate controls to minimise the risk of unauthorised access, misuse and inappropriate disclosure. It is the responsibility of the discloser to assess requests in line with the five responsible sharing principles.

Table 2: Responsible Sharing Principles Template

	Aggregated Non Personal Data and Non Sensitive Information	Event Level Non Personal Data and Non Sensitive Information	Event Level Personal Data and/or Sensitive Information
Safe Activity	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	List the controls	List the controls	List the controls
Safe Users	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	List the controls	List the controls	List the controls
Safe Settings	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	List the controls	List the controls	List the controls
Safe Information	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	List the controls	List the controls	List the controls
Safe Outputs	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	List the controls	List the controls	List the controls

In Table 3 below, an example is provided for controls that may be put into place if the information was event level data and/or it is sensitive.

Table 3: Responsible Sharing Principles Example

	Aggregated Non Personal Data and Non Sensitive Information	Event Level Non Personal Data and Non Sensitive Information	Event Level Personal Data and/or Sensitive Information
	Example for Aggregated Non Personal Data and Non Sensitive Information	**Example for Event Level Non Personal Data and Non Sensitive Information**	**Example for Event Level Personal Data and/or Sensitive Information**
Safe Activity	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	Purpose Test undertaken and the legal purpose is identified.	Purpose Test undertaken and the legal purpose is identified. The Information Access, Use and Disclosure Policy reviewed.	Purpose Test undertaken and the legal purpose is identified. Disclosure training completed.
Safe Users	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	Trained to use Responsible Sharing Principles to minimise risks.	Trained to use Responsible Sharing Principles to minimise risks and shared controls to other users.	Information management training completed. Trained to use Responsible Sharing Principles and shared controls to other users.
Safe Settings	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	Password required to access system.	Password required accessing system and a separate password required to access file.	File classified as confidential in the title. Restricted directory established. A password is required to access the system and a separate password is required to access the file. Hard copy information kept in secure location. Information in transit is encrypted.
Safe Information	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	Information quality standards identified and understood.	Information quality standards identified and understood. Data reviewed to ensure no patient is likely to be re-identified.	Direct identifiers are removed and the data is further reviewed to remove information not required for the purpose.
Safe Outputs	**No or Limited Controls**	**Moderate Controls**	**High Controls**
	Information quality standards identified and understood.	Information quality standards identified and understood. Outputs reviewed to ensure no patient is likely to be re-identified.	Direct identifiers are removed and the outputs are further reviewed to remove fields and elements from outputs that not required for the legal purpose.

Note: The Responsible Sharing Principles with key pre-determined shared controls could be incorporated into a disclosure model and/or disclosure agreement when applicable.

Appendix 8: Information Request Form Example

For an electronic version of this form click the link: Information request form (Word)

Government of **Western Australia**
Department of **Health**

Reference Number	

Information Request Form

This form is to be completed by individuals/organisations requesting WA health information collected under the *Health Services Act 2016.*

All sections need to be completed to inform a full and proper assessment of this request.

This form should not be used for requests for information for research purposes or for linked data. Such requests should be referred to the Research Governance Unit and/or relevant Research Ethics Committee, or the Data Linkage Branch, for the appropriate application documents.

Part A: Requestor Information	
Name	Click or tap here to enter text.
Position	Click or tap here to enter text.
Institution / Organisation	Please Select
Institution Name	Click or tap here to enter text.
Institution location if outside WA	Please Select
Phone	Click or tap here to enter text.
Email	Click or tap here to enter text.

Part B: Data Request	
ACTIVITY	
Project summary / Purpose	(Please provide context for your request, including why the information is required)
What is the lawful purpose of this request? If unsure, please refer to the Purpose Test in the Information Use & Disclosure Policy Compendium, or relevant Authorising Officer	(Please state the lawful purpose of your request, in relation to the Health Services Act 2016.)
INFORMATION *Please ensure any relevant documentation (e.g. data variable lists, approvals etc.) are attached.*	
Information Source(s) / Data Collection(s)	(Please detail the source(s) of information required)
Details of information required:	
Cohort of interest	(Please detail the cohort required)

Time period of required data	(Please specify the time period of information required)
Inclusions/exclusions to be applied	(Please specify any inclusion/exclusion criteria to be applied to the information)
Other information	(Please detail any other information relevant to this request)
Identifiability of information being requested	☐ Unit (row), record or event level data (most granular) ☐ Aggregated or tabulated data (summarised data)
Participant consent arrangements	☐ Informed consent will be obtained for each participating individual ☐ Informed consent will not be obtained ☐ A 'waiver of consent' will be obtained
USERS	
Who will have access to the information?	(Please list individuals, and their positions, who will have access to the information)
Will the information be provided to any other parties or organisations?	☐ Yes ☐ No
If yes, please provide details	(Please provide details of individuals/organisations who will have access to the information)
Will the information be used or disclosed to parties or organisations outside the WA health system?	☐ Yes ☐ No
If yes, please provide details	(Please detail who and why individuals/organisations outside WA Health will have access to the information)
Will the information be used or disclosed to parties or organisations outside the state of WA?	☐ Yes ☐ No
If yes, please provide details	(Please detail who and why individuals/organisations outside WA will have access to the information)
SETTINGS	
Where and how will the information be stored?	(Please provide details)
What physical security arrangements will be in place?	(Please provide details)
What technological security arrangements will be in place?	(Please provide details)
Will the information be transported?	☐ Yes ☐ No
If yes, how will information be secured during transport?	(Please provide details)

How long will the information be retained for?	(Please provide details)
How will the information be destroyed/disposed of?	(Please provide details)
Will the information be stored by parties outside the WA health system? Please consider physical, technological and virtual (i.e. cloud) storage of the information	☐ Yes ☐ No
If yes, please provide details	(Please provide details)
Will the information be stored outside the state of WA? Please consider physical, technological and virtual (i.e. cloud) storage of the information	☐ Yes ☐ No
If yes, please provide details	(Please provide details)
Other security plan details:	(Please provide details)
OUTPUTS	
What are the intended outputs from this information?	(Please list the outputs expected to arise from the use of this information)
Will the information, or results, be published / made public?	☐ Yes ☐ No
If yes, please provide details of how the information will be disseminated etc.	(Please detail how the outputs will be disseminated)

ADDITIONAL INFORMATION

Additional information relevant to this request	Click or tap here to enter text.

Appendix 9: Information Disclosure Form Example

Note: The information disclosure form example does not apply to research as a Data Transfer Agreement Form is used for this purpose.

For an electronic version of this form click the link: Information disclosure form (Word)

Government of **Western Australia**
Department of **Health**

Reference Number	

Information Disclosure Form

This form is only to be completed by persons authorised to disclose WA health information collected under the Health Services Act 2016.

You must ensure that you have been delegated the relevant functions and powers to disclose information from the relevant information asset, in line with the Department CEO Instrument of Delegation, Health Information, Health Services Act 2016, before authorising the requested disclosure of information.

Please refer to the Information Access, Use & Disclosure Policy, as part of the Information Management Policy Framework, for guidance on the access, use and disclosure of information from the WA Department of Health and Health Service Providers.

This form is to be used in conjunction with the Policy, and is intended as a guide only. Authorising officers should be familiar with the Policy, and seek further legal or other advice as required.

Part 1: Confirmation of Authority to Disclose Information	
I have confirmed that I have been delegated the relevant functions and powers to assess and authorise a disclosure in line with the requirements of the *Health Services Act 2016* and relevant Regulations.	☐ Yes

Part 2: Risk Assessment – Responsible Sharing Principles		
Safe Activity: I am satisfied that the information requested is for a lawful purpose, under the *Health Services Act 2016*	☐ Yes	☐ No
If not, the following measures are to be taken:		

Safe Information: I am satisfied that the information requested is appropriate for the proposed purpose	☐ Yes	☐ No
If not, the following measures are to be taken:		

Safe Users: I am satisfied that the information will be used or disclosed to the appropriate individual(s) and/or organisation	☐ Yes	☐ No
If not, the following measures are to be taken:		

Safe Settings: I am satisfied that the information will be stored and accessed appropriately	☐ Yes ☐ No
If not, the following measures are to be taken:	

Safe Outputs: I am satisfied that outputs arising from the use of the information will be disseminated appropriately	☐ Yes ☐ No
If not, the following measures are to be taken:	

Part 3: Authorising Officer Approval

As the Authorising Officer of the information requested above:
- I am satisfied that the use, access and disclosure of information for the above purpose is lawful under the *Health Services Act 2016.*
- I have assessed the risk of inappropriate use and/or disclosure, and based on the information provided to me, I am satisfied that the information can be disclosed as outlined above.

Name	Click or tap here to enter text.
Position	Click or tap here to enter text.
Signature	
Date	Click or tap to enter a date.

Appendix 10: Information Disclosure Contract Example

Note: The information disclosure contract example does not apply to research as a Data Transfer Agreement Form is used for this purpose.

INFORMATION REQUESTED

- The Department of Health (DoH) agrees to disclose [insert description of applicable information] subject to the terms and conditions of this contract.

INFORMATION CUSTODIAN

Name: xx
Position/title: xx
Telephone: xx
Email: xx

OBLIGATIONS OF THE REQUESTOR

By signing the agreement, the requestor:

- Agrees to maintain the information in a confidential and secure manner in the location to which it was originally disclosed.
- Acknowledges that the information disclosed remains the property of the WA health system.
- Agrees to, under no circumstances, pass on or divulge the disclosed data to a third party without the prior approval of the Information Custodian (see contact details above).
- Agrees not to use the information for any purpose other than that for which it was originally requested.
- Agrees that the source of the information will be properly referenced whenever it is used in publications.
- Agrees not to copy or store parts or the whole of the disclosed dataset in a directory that may be accessible to anyone else.
- Agrees not to leave printouts of datasets in any form in an area accessible to anyone else.
- Agrees to destroy all copies of the information and hard copies at the completion of its use for the purpose intended and inform the Information Custodian of the outcome.
- Agrees to immediately disclose any information or data breach to the Information Custodian and undertake all reasonable steps to:
    a) contain the information breach;
    b) assess the impact of the information breach to determine the extent of the damage and harm caused;
    c) take actions to remediate any risk of further harm;
    d) review the incident and take preventative actions; and
    e) comply with the requirements outlined in the relevant Privacy Impact Assessment(s).

DISCLAIMER

All information/data provided is accurate and up to date at the time of disclosure. WA health system cannot be held liable for the accuracy of the reports based on the analysis of the data.

AGREEMENT

I _____ (please print)

Of _____ department/organisation

Acknowledge that I have read and agree to the above provisions of the contract and indicate the intended use of the information requested as follows:- [insert agreed purpose for using the requested information]

_____

I agree to retain the data in the following location in a secure manner:- [e.g. address]

_____

Signed: _____

Position/Title: _____ Date: _____

Witnessed by _____ *Position:* _____

This document can be made available in alternative formats on request for a person with a disability.