Information Management Policy

August 2022
Version 2

WA Primary Health Alliance
Better health, together

phn
PERTH NORTH, PERTH SOUTH, COUNTRY WA
An Australian Government Initiative

Document Control

Document Owner

Custodian	Next Review Date
Data Governance and Data Quality Manager	August 2024

Version	Author	Approved By	Date
2	Jane Connor, Data Governance Analyst	Executive Board	19 August 2022 7 September 2022
1	Giles Nunis, Chair, Digital and Data Strategic Alignment Group	Learne Durrington, CEO	16 July 2021

This document is based on the National Archives of Australia – Developing an information management policy template.

This document is part of the suite of Data Governance processes and links to the following WAPHA (Western Australia Primary Health Alliance) documents:

- Privacy Policy
- Privacy Code of Practice
- Privacy Impact Assessment Threshold Assessment
- Privacy Impact Assessment Template
- Information Management Framework
- Information Management Manual
- Information Management Registers
- Data Quality Framework
- Risk Management Policy.

The Primary Health Networks (PHN) National Data Governance Framework, Policy and Manual provides additional guidance on the management of data collections and de-identified information.

The following information from the Office of the Australian Information Commissioner can be used with the above policies and procedures:

- OAIC Guide to undertaking privacy impact assessments
- OAIC Guide to Health Privacy
- OAIC Guide to De-identification and the Privacy Act
- OAIC and CSIRO De-identification Decision Making Framework
- OAIC Guide to data analytics and the Australian Privacy Principles.

Further information on current frameworks, policies and procedures are available from the Business Services, Data Governance & Data Quality Manager.

Contents

1. Purpose

The purpose of this policy is to guide and direct the creation and management of information assets (records, information, and data) by staff and contractors, and to clarify roles and responsibilities.

WA Primary Health Alliance (WAPHA) is committed to establishing and maintaining information management practices that meets its business needs, accountability requirements and stakeholder expectations.

The benefit of complying with this policy will be trusted information that is well-described, stored in known endorsed locations and accessible to staff and clients when needed.

This policy is written within the context of WAPHA's Information Management Framework. Complementary policies and additional procedures are available on SharePoint. This policy should be read in conjunction with WAPHA's Privacy Policy which outlines how WAPHA deals with an individual's personal information.

2. Scope

This Policy applies to all WAPHA staff members and contractors and to all information assets (records, information, and data) in any format, created or received, to support WAPHA's business activities.

It covers all business applications used to create, manage, and store information assets, including dedicated information management systems, business information systems, databases, email, voice and instant messaging, websites, and social media applications. This policy covers information created and managed in-house and off-site, including in cloud-based platforms.

WAPHA operates Western Australia's three Primary Health Networks (PHNs), as part of the Australian Government's national PHN program – Perth North, Perth South, and Country WA. As a lead PHN, WAPHA handles information assets on behalf of other PHNs through the Primary Health Insights platform. The PHN Co-operative's National Data Governance Framework and Manual applies to data stored within Primary Health Insights.

3. Policy Statement

WAPHA recognises its information assets as valuable corporate assets and is committed to achieving appropriate and ongoing management of these assets to advance WAPHA's strategic priorities and mission to help those most at risk of poor health by improving health equity and access to services that transform and save lives.

WAPHA is committed to the principles of the *Privacy Act 1988* and Australian Privacy Principles. WAPHA provides services to other PHNs through the Primary Health Insights program and is committed to the PHN Co-operatives National Data Governance Framework.

4. Legislation

The *Privacy Act 1988* (Cth) (the Act) protects and promotes the privacy of individuals and regulates how organisations with an annual turnover of more than $3 million and some other organisations handle personal information. The Act includes thirteen Australian Privacy Principles (APPs). The APP Guidelines outline the mandatory requirements and matters which must be considered when exercising functions and powers under the Act.

WAPHA is defined as an APP entity for the following reasons:

- it is an Australian body corporate that carries out business in Australia and has an annual turnover in excess of $3 million
- it provides a health service and holds health information other than in an employee record[3]
- is a contracted service provider for a Commonwealth contract.

Public health service providers are not subject to the *Privacy Act 1988* and are subject to legislation within their State or Territory. As WAPHA holds information on behalf of other PHNs across Australia, the following Legislation may apply depending on the type of information held:

Jurisdiction	Legislation
Commonwealth	Privacy Act 1988 (Cth)
ACT	Information Privacy Act 2014 (ACT) – does not include health information which comes under the Health Records (Privacy and Access) Act 1997
New South Wales	Privacy and Personal information Protection Act 1998 (PPIP Act) – public sector agencies, including councils and universities Health Records Information Privacy Act 2002 (HRIP Act) – health service providers
Northern Territory	Information Act 2002 – government / public sector
Queensland	Information Privacy Act 2009 – public sector
South Australia	Privacy Act 1988 (Cth) *Health Care Act 2008* - all public health service providers
Tasmania	Personal information Protection Act 2004 – government agencies
Victoria	Privacy and Data Protection Act 2014 – public sector agencies
Western Australia	Privacy Act 1988 (Cth) *Health Services Act 2016* (WA) – all public health service providers

4.1 Australian Privacy Principles

The WAPHA Privacy Code of Practice sets out WAPHA's roles and responsibilities under the 13 Australian Privacy Principles in detail. In summary these are:

1. **Open and transparent management of personal information** – Personal information is managed in a robust and transparent way, through implementation of this policy, supporting documents and procedures.
2. **Anonymity and pseudonyms** – Individuals have the option to not identify themselves, or to use an alternate name when dealing with WAPHA in relation to certain matters, where it is lawful and practicable to do so.
3. **Collection of solicited personal information** – Personal information is collected through lawful and fair means only where it is reasonably necessary for, or directly related to, its functions and activities.
4. **Dealing with unsolicited personal information** – Unsolicited personal information received but not collected through normal processes, will be de-identified or destroyed where lawful and reasonable to do so.
5. **Notification of the collection of personal information** – Individuals are notified when WAPHA is collecting personal information.
6. **Use or disclosure** – Personal information is only collected and used for specified purposes. Personal information is de-identified where possible when it is disclosed.

7. **Direct marketing** – Personal information is not used for direct marketing unless authorised by the individual concerned.
8. **Cross border disclosure of Personal information** – Personal information is not disclosed to overseas recipients.
9. **Use or disclosure of government related identifiers** – Government related identifiers are not used by WAPHA in its use or disclosure of personal information unless necessary to fulfil an Australian Government reporting requirement.
10. **Quality of Personal information** – Reasonable steps are taken to ensure personal information collected is accurate, up to date and complete.
11. **Security of Personal information** – Appropriate steps are taken to ensure personal information is protected from misuse, interference, loss, unauthorised access, modification, and disclosure.
12. **Access to Personal information** – Access is provided to an individual to their personal information held by WAPHA as required by the Privacy Act.
13. **Correction of Personal information** – An individual can request corrections to their personal information held by WAPHA as required by the Privacy Act.

4.2 Personal Information

The Privacy Act defines 'personal information' as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not'.[1]

The term 'personal information' encompasses a broad range of information however some are explicitly recognised as personal information under the Privacy Act. For example:

- **sensitive information** - includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation, or criminal record, provided the information or opinion otherwise meets the definition of personal information.
- **health information** – any personal information about your health or disability (this might include sensitive information).
- **credit information** – credit worthiness of an individual, such as a bank, retailer or businesses that provide credit to suppliers.
- **employee record information** – current and former employee records are exempt from the Privacy Act, however records kept during the recruitment process are personal information.[2]
- **tax file number information** – there are strict rules about the use of individuals tax file numbers.[3]
- **government and healthcare identifiers** – there are additional rules for the adoption, use and disclosure of government related identifiers and healthcare identifiers.[4]

4.3 De-identified Information

The term 'de-identified' is used to describe information that is not (or is no longer) about an identified or reasonably identified individual and does not reveal personal information about such an individual.

[1] OAIC - What is personal information?
[2] OAIC - Employee records exemption
[3] OAIC - The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information
[4] OAIC - Chapter 9: APP 9 — Adoption, use or disclosure of government related identifiers

De-identification involves two steps:

1. removal of direct identifiers
2. taking one or both of the following additional steps:
   - the removal or alteration of other information that could potentially be used to re-identify an individual, and/or
   - the use of controls and safeguards in the data access environment to prevent re-identification.

4.4 Data

Data is measurements and observations, including facts, figures, records, statistics, or opinions, whether true or not, that have been collected directly or obtained as a by-product of a compliance, regulatory or service-delivery process.

Data is raw, unorganised facts that need to be processed. Data can be something simple and seemingly random until it is organised. When data is processed, organised, structured, or presented, in a given context to make it useful, it is called information.

There is no legislation in Australia specifically related to data governance. WAPHA will follow the guidance of the Australian Institute of Health and Welfare, National Archives of Australia, and Data Governance Australia. In addition, WAPHA will adhere to any relevant International Standards for data governance and cybersecurity.

5. Creation and Management of Information Assets

WAPHA creates, captures, and manages a variety of information to support its business objectives and comply with legal requirements. WAPHA has a centralised storage system (SharePoint) for information assets and also uses third party software. WAPHA also uses third party systems to create, collect and share information with stakeholders. WAPHA provides a centralised hosting system for information for third parties through its Primary Health Insights program. Access to information is limited to users with an operational or management business requirements.

WAPHA uses Privacy Impact Assessments (PIA) to ensure 'privacy by design', a process for embedding good privacy practices into the design specifications of technologies, business practices and physical infrastructures, is embedded into new projects and business activities.[5] A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising, or eliminating those impacts. The PIA process allows WAPHA to engage with stakeholders to identify any information creation, management, security, transfer, and disposal issues.

Indigenous Data refers to information or knowledge, in any format or medium, which is about and may affect Indigenous peoples both collectively and individually. Indigenous Data Sovereignty refers to the right of Indigenous people to exercise ownership over Indigenous data. Indigenous data governance refers to the right of Indigenous peoples to autonomously decide what, how and why Indigenous data are collected, accessed, and used. WAPHA adhere to the Australian set of principles developed by Maiam nayri Wingara and uphold the rights of Indigenous peoples by including Indigenous leaders, practitioners and community members in the ownership and governance of Indigenous data collected, used and held by WAPHA.[6]

WAPHA has strict controls to limit the unnecessary transfer of information assets. Any requests to

[5] OAIC - Privacy by design - Home (oaic.gov.au)
[6] KEY PRINCIPLES — Maiam Nayri Wingara

transfer information, records or data is subject to an approval and authorisation process which is detailed in the WAPHA Information Management Manual.

WAPHA has adopted the Australian Institute of Health and Welfare (AIHW) five safes approach – Projects, People, Data, Settings, Outputs - to thinking about, assessing, and managing risk associated with data sharing and release. The framework is an internationally recognised approach to considering strategic, privacy, security, ethical and operational risks as part of a holistic assessment of the risks associated with data sharing or release.[7] The request for information, approval and authorisation process is detailed in the WAPHA Information Management Manual.

WAPHA staff and contractors should only retain information assets as long as they are necessary or as required by legislation and guidelines. The retention and destruction process for information assets and data sets is detailed in the WAPHA Information Management Manual. WAPHA staff, contractors, consultants and third-party software and hardware suppliers must ensure the secure storage and preservation of digital and physical documents according to the relevant legislation and regulations. Commonwealth Records must be stored for at least 15 years.

6. Roles and Responsibilities

WAPHA recognises that the management of personal information and data governance is an organisation wide responsibility, and all staff and contractors are responsible for compliance with this Policy.

Role	Responsible for:
WAPHA Board	The Board will ensure the WAPHA Executive Team effectively manage information and data in accordance with current legislation and guidance.
WAPHA Executive (Data Custodian)	The Executive will keep the Board informed of any information management issues and data breaches. Executives are also responsible for information and data collections relevant to their role as a **Data Custodian**. Data Custodians should ensure that: • information and data collections are in keeping with WAPHA's strategic goals and mission statement, are necessary and fit for purpose • engaging with stakeholders to agree new projects • a privacy impact threshold assessment is carried out for new projects • a privacy impact assessment is developed (where necessary) • the Data Collections Register is updated and audited • personal information is de-identified where possible • controls are put in place to manage access and use • authorising a data sharing agreement (where necessary) • ad-hoc requests for information or access to data collections are appropriately authorised, approved, and disclosed • authorise data to be shared with other PHNs • data breaches or unauthorised access are managed in accordance with current legislation, policies, and procedures • information, data collections, reports and publications are audited and de-identified or destroyed if no longer required.

[7] The Five Safes framework - Australian Institute of Health and Welfare (aihw.gov.au)

	The Executive also ensures that the Digital and Data Strategic Alignment Group carries out its roles and responsibilities, including improving data quality and security. The Executive may also set priorities for Departments and teams within WAPHA to improve information management, including allocating budgets for planning, monitoring, and improving information management and information communication and technology systems. WAPHA also provides services to third parties. The Executive are responsible for ensuring information management systems are in place for all relevant jurisdictions where services are provided.
WAPHA Managers (Data Steward)	All senior staff are responsible for the information and data collections that their team uses. Certain WAPHA staff will also be identified as **Data Stewards** for particular information or data collections and are responsible for: • day to day management of information and data collections in compliance with current legislation, policies, and procedures • mitigating data breaches or unauthorised access (with the Data Governance and Data Quality Manager and Data Custodian) • working with stakeholders to develop new projects or uses of existing information • reviewing access and users (with Digital Services team) • carrying out a privacy impact threshold assessment • developing a full privacy impact assessment (where required) • raising and mitigating any risks on the Risk Register • establishing data standards with the Digital Services team • ensuring information is stored accurately and securely (with Business Services Team) • checking and/or auditing information is accurate, up-to-date, relevant, and fit for purpose • ensuring data and information is de-identified where possible • ensuring information, reports and data collections are archived, deleted and/or destroyed if no longer needed • working with the Data Custodian and keeping them informed of any changes or improvements • working with the Data Quality and Data Governance Manager to improve quality and security and ensure documentation is up to date.
Digital and Data Strategic Alignment Group (DDSAG)	The **Digital and Data Strategic Alignment Group (DDSAG)** is the group which ensures WAPHA's strategic digital and data intentions are commissioned, monitored, and evaluated. The Chief Digital Transformation Officer is the Chair of this group. The Group has oversight of all digital and data activities, and its roles and responsibilities are set out in the Group's Terms of Reference. DDSAG meet on a regular basis to discuss: • the approach to design and delivery of digital and data programs and activities • new digital and data projects or contracts • privacy impact assessments

	• stakeholder engagement • national PHN working groups • risk assessments and risk mitigation measures • software and hardware platforms • data governance and data quality issues and improvements.
Data Governance and Data Quality Manager (Privacy Officer)	The **Data Governance and Data Quality Manager** is responsible for WAPHA's information management, data governance and privacy policies. The Manager works with DDSAG to prioritise areas for improvement, raise awareness and provide training for staff and contractors.
Cyber Security Working Group	The **Cyber Security Working Group** are responsible for data security, user access and data compliance. The Cyber Security Manual details the roles and responsibilities of this group.
Information Systems Manager	The **Information Systems Manager** is responsible for cyber security and information technology systems. The Manager works with DDSAG and the Cyber Security Working Group to plan, monitor and improve WAPHA's Cyber Security Policy and Cyber Security Manual.
WAPHA Staff and contractors **(Data Processors)**	Each WAPHA Department and Team will work with certain information for their day-to-day activities. All staff are responsible for ensuring that the information they work with is kept secure, relevant, accurate and up to date and in keeping with the relevant WAPHA policies and procedures. Staff should review, at least annually, whether the information they work with is accurate, up to date, still required or can be archived or deleted. It is the responsibility of WAPHA staff to: • understand and carry out the information and data management requirements of their role • understand what types of data should not leave the organisation without authorisation from the Data Governance Manager • understand what types of data WAPHA should not receive, due to the risk of re-identification or accidental release from the organisation • document their daily work, and save it in the right location in a way that it can be found again • document decisions, actions, activities, processes, and procedures • ask for assistance from the Data Governance and Data Quality Manager if they have any questions about information management • work together within their team and across WAPHA to consistently manage information and data • model good information and data management practices • ensure projects, tools and technologies developed, implemented, and deployed support effective and compliant information and data governance • record information in ways and in systems that are accessible, useable, and interoperable • follow information management policies, procedures, and training.[8]

[8] Adapted from NAA - Information and data governance framework | naa.gov.au

Third Parties (External Data Owners)	WAPHA may collect and hold information or data which is owned by a third party, for example an Aboriginal Health Service Provider, WA Health or Department of Health and Aged Care. The data ownership may remain with the third party but be used by WAPHA for to meet a business objective, e.g., to assist with the improvement of services to a specific community. Through Primary Health Insights, WAPHA provides a platform for third parties, mainly other Primary Health Networks, to store and catalogue information and data collections. The ownership of any information or data on this platform remains with the third-party organisation. WAPHA will enter into Information and/or Data Sharing Agreements with third parties where necessary.

7. Communications and Training

WAPHA will ensure that this policy is communicated to staff through mandatory induction training. WAPHA's People and Culture team co-ordinates training for staff and contractors. In addition to in-house training, WAPHA staff can access online training through LinkedIn and free training on Privacy Impact Assessments from the Office of the Australian Information Commissioner.

The Data Governance and Data Quality Manager will provide training and support for staff and contractors who manage information assets.

8. Monitoring and Review

This policy will be reviewed on an annual basis to ensure that it is up to date with current legislation and reflect any changes or significant developments in WAPHA's business activities.

9. Resources

In addition to WAPHA's Information Management policies and procedures, resources can be found on the following websites:

- Office of the Australian Information Commissioner - https://www.oaic.gov.au/
- National Archives of Australia - https://www.naa.gov.au/
- Australian Institute of Health and Welfare - https://www.aihw.gov.au/
- Australian Government Department of Health – Primary Health Networks - https://www.health.gov.au/initiatives-and-programs/phn
- Indigenous Data Sovereignty - Maiam nayri Wingara

The following documents form part of the WAPHA information management process:
- OAIC Guide to undertaking privacy impact assessments
- OAIC Guide to Health Privacy
- OAIC Guide to data analytics and the Australian Privacy Principles.

Staff and contractors should contact the Data Governance and Data Quality Manager with any queries or requests.

10. Senior Management Endorsement

In endorsing this policy, we note WAPHA's commitment to establish and maintain information management practices that meet its operating model, business objectives, accountability requirements and stakeholder expectations.

The benefit of complying with this policy will be trusted information that is well-described, stored securely, accessible to authorised users, disclosed appropriately and destroyed when no longer necessary.

Learne Durrington **Chief Executive Officer**	**Giles Nunis** **Chair, Digital and Data Strategic Alignment Group**