Privacy Code of Practice

August 2022

Version 1.0

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 No	Author	Approved By	Date
1.0	Jane Connor, Data Governance Analyst	Executive Board	19 August 2022 7 September 2022

This document is adapted from the Office of the Australian Information Commissioner – Australian Privacy Principles Guidelines and Privacy Act 1988 (Cth).

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

- Privacy Policy
- Privacy Impact Assessment Threshold Assessment
- Privacy Impact Assessment Template
- Information Management Framework
- Information Management Policy
- 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. Introduction

The purpose of this Privacy Code of Practice is to provide individuals with transparency about how information is handled within WAPHA.[1] WAPHA collects, uses, and stores a variety of personal and de-identified information to assist its daily operational activities, commission services and meet its strategic goals. This document sets out WAPHA's obligations under current legislation, the procedures for safe handling of information.

Western Australia Primary Health Alliance (WAPHA) is a not-for-profit corporate entity operating WA's three Primary Health Networks (PHNs) as part of the Australian Government's national PHN program established in 2015. The program aims to strengthen, improve, and connect the primary care system so people – particularly those at risk of poor health outcomes – can access better care, closer to home. By partnering with local communities, service providers, general practices (GPs) and allied health professionals, WAPHA aims to deliver better health, together.

2. 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.[2]

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.[4]

This Privacy Code of Practice has been developed in keeping with the Guidelines for developing codes issued under Part IIIB of the Act but is not intended to be a registered code and legally binding.[5] This Code is intended to increase openness and transparency about how WAPHA manages personal information under the Act.

The *Freedom of Information Act 1992* (WA) gives the public a right to access government documents, subject to some limitations, in Western Australia, which includes public hospitals and the Department of Health. WAPHA is not currently considered a government 'agency', so this does not apply to WAPHA. Individuals can still request access to personal information under the Act.

An APP entity 'holds' personal information if it has possession or control of a record that contains personal information. Any personal information held by WAPHA in its software or electronic record keeping systems may be considered personal information held by WAPHA, even if the storage of that information is outsourced to a third party. The terms 'use' and 'disclose' are not defined in the Act.[6]

WAPHA provides services to other Primary Health Networks in Australia. The relevant privacy legislation for each jurisdiction should be considered when providing services outside of Western Australia.

[1] OAIC – www.oaic.gov.au/privacy-registers/privacy-codes-register
[2] OAIC – www.oaic.gov.au/privacy
[3] OAIC – www.oaic.gov.au/privacy/privacy-for-health-service-providers.
[4] OAIC APPs B1 – 21 APP Version 1.3
[5] OAIC Guidelines for developing codes – www.oaic.gov.au/privacy
[6] OAIC - Chapter 6: APP 6 — Use or disclosure of personal information

The Privacy Act applies to all private sector health service providers anywhere in Australia. It does not apply to state and territory public sector health service providers, such as public hospitals. In NSW, Victoria, and the Australian Capital Territory (ACT) private sector health service providers must comply with both Australian and state or territory privacy laws when handling health information.

Queensland, the Northern Territory and Tasmania have privacy legislation that applies only to their public sector, including public sector health service providers. Western Australia and South Australia do not have specific privacy legislation.

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

2.1 Personal Information

What is personal information will vary, depending on whether a person can be identified or is reasonably identified in the circumstances. Personal information may include an individual's name, signature, address, phone number or date of birth, location information from a mobile device, IP addresses, photographs, and sensitive information.[7]

Sensitive personal information includes health or genetic information, racial or ethnic origin and some aspects of biometric information. Sensitive information has a higher level of privacy protection that other personal information.[8]

WAPHA also collects personal information on employees, customers, suppliers, and general enquiries. WAPHA also handles health information for quality assurance, planning and commissioning purposes. Whilst most of this information is de-identified before it is collected or supplied to WAPHA, some personal information may remain or, when matched with other external data, be able to be re-identified.

2.2 Health Information

Under the Act, if an entity holds health information, it is considered a health service provider, even if that is not its primary activity.[9] State and territory public hospitals and health services

[7] OAIC - What is personal information?
[8] OIAC - What is sensitive information?
[9] OAIC - Privacy for health service providers

are not covered by the Act but are subject to relevant state legislation.
WAPHA has a Data Disclosure Agreement with the Department of Health to optimise the value and quality of information and minimise misuse and inappropriate disclosure of information.

'Health information' is any personal information about a person's health or disability including information or opinion about the illness, injury or disability, genetic information, and pharmaceutical purchases.[10]

Health information about a patient can be disclosed for the primary purpose it was collected (such as personal information provided to a GP (general practices) for use during a consultation), or for a secondary purpose, in certain circumstances.

Any purpose other than the primary purpose is a secondary purpose. A health service provider can use or disclose health information for a secondary purpose with the patient's consent. This includes if a patient would reasonably expect the health information to be disclosed for that purpose or the purpose is directly related to the primary purpose of collection.[11]

WAPHA cannot collect health information about individuals for one of the research or public health or safety purposes permitted under s 16B(2) of the Privacy Act if de-identified information would serve the same purpose (s 16B(2)(b)).

Activities or processes necessary for the functioning of the health sector may also be directly related purposes (including quality assurance and clinical audit activities) and only the minimum amount of information necessary to achieve the purpose should be disclosed.[12]

A patient's health information may be used or disclosed if necessary for research or the compilation or analysis of statistics, relevant to public health or public safety, and certain conditions are met[13] (such as the patient's capacity to give consent, a child's capacity to consent and that only necessary information is disclosed).[14]

Health information may be collected without consent where it is necessary for health management activities, and:

- the particular purpose cannot be served by collecting de-identified information
- it is impracticable to obtain the individual's consent, and
- the collection is either:
    - required by or under an Australian law (other than the Privacy Act)
    - in accordance with rules established by a competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or
    - in accordance with guidelines issued by the CEO of the National Health and Medical Research Council and approved by the Commissioner under Section 95A of the Act (see below).[15]

WAPHA collects, uses, and stores de-identified information wherever possible, however some information or data collections may include 'necessary' personal information where the health management activity cannot be carried out without it. If any information or data collection contains personal health information, it will be handled according to the processes outlined in

[10] OAIC - What is health information?
[11] OAIC - Chapter 6: APP 6 — Use or disclosure of personal information
[12] OAIC - Chapter 6: APP 6 — Use or disclosure of personal information
[13] OAIC Guide to Health Privacy – Chapter 3: Using or disclosing health information
[14] OAIC Guide to Health Privacy – Chapter 7: Disclosing information without patients with impaired capacity.
[15] OAIC - Chapter D: Permitted health situations

this Code.

2.3 My Health Records

A healthcare provider organisation registered to use the My Health Record system is authorised to collect, use, and disclose health information to provide health care to a patient.

The *My Health Records Act 2012* covers the authorised collection, use or disclosure of health information on the My Health Records system. These authorised actions will not breach the *Privacy Act 1988*. However, once the information is downloaded to a local computer system, most of the rules in the *My Health Records Act 2012* no longer apply to its collection, use or disclosure. Instead the *Privacy Act 1988*, local state or territory health information and privacy laws and professional obligations apply, the same as other health information that is handled by a healthcare service provider.[16]

Any unauthorised collection, use or disclosure of health information from a patient's My Health Record in a way that is not authorised by the *My Health Records Act 2012* will breach the Act and may be liable for a civil or criminal penalty.

The My Health Record System Operator is the Australian Digital Health Agency. In the event of a data breach, WAPHA staff should follow the Notifiable Data Breaches procedure in the Information Management Manual.

2.4 Section 95A Guidelines

The Guidelines issued by the National Health and Medical Research Council (NHMRC) approved under Section 95A of the Act provide a framework for human research ethics committees to assess proposals to handle health information without the consent of the subject. The NHMRC's '*Determining whether the S95A Guidelines Apply*' Flowchart can be used by WAPHA to determine whether the guidelines apply to any information or data collections.

Section 95A does not apply if the proposed relevant collected personal information is de-identified when used for the handling of proposed research or the compilation or analysis of statistics and it is impractical to seek consent. Therefore, de-identified information received by WAPHA from third parties which is used internally and further shared with third parties does not fall under the Section 95A guidelines.[17]

2.5 Employee Records

The handling of employee records by a private sector employer is exempt from the Act if directly related to current or former employment. The Act will apply if the personal information is used for another purpose and for any other personal information collected, such as contact information acquired during the recruitment process or general enquiries.

The *Fair Work Act 2009* (Cth) and *Fair Work Regulations 2009* sets out the range of information which must be made and kept for each employee including general employment, pay, hours of work, leave, superannuation and termination records.[18]

WAPHA's Oracle Cloud based Enterprise Resource Planning (ERP) software incorporates human resources, finance, and contracts in a centralised system. The system is designed to minimise duplication of information across business streams and improve information access and accuracy. The system will keep employee records and personal information about individuals involved in the recruitment process.

[16] OAIC – Handling information in a My Health Record
[17] NHMRC Guidelines - https://www.nhmrc.gov.au
[18] Fair Work Ombudsman - Record-keeping & pay slips - Fair Work Ombudsman

The Privacy (Tax File Number) Rule 2015 issued under section 17 of the Act regulates the collection, storage, use, disclosure, security, and disposal of an individuals' Tax File Number (TFN) information and is legally binding.[19] As an employer, WAPHA is a TFN recipient under this Rule and must not record, collect, use, or disclose TFN information unless this is permitted under taxation, personal assistance, or superannuation law. In addition, WAPHA must abide by the *Taxation Administration Act 1953* which creates offences for unauthorised use of an individual's TFN.

2.6 De-identified information

Personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable and is therefore not 'personal information.'[20] De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so. Generally, de-identification includes two steps:

- removing personal identifiers, such as an individual's name, address, date of birth or other identifying information, and
- removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

The risk of re-identification must be actively assessed and managed to mitigate the risk of the data set being able to be used with other information which would recreate personal information. Relevant factors to consider when determining whether information has been effectively de-identified could include the cost, difficulty, practicality, and likelihood of re-identification.[21]

WAPHA uses de-identified information or data collections as far as practicable for all commissioning, monitoring, reporting, and planning purposes.

3. Consent

Consent[22] means 'express consent or implied consent':

- **Express consent** is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.
- **Implied consent** arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and WAPHA.

WAPHA must ensure that individuals are properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent in plain English, without legal or industry jargon. Capacity to consent should be considered where an individual is a child or young person, has English as a second language or has intellectual capacity issues.[23]

WAPHA must not assume that an individual has consented to a collection, use or disclosure that appears to be advantageous to that person. Nor can WAPHA establish implied consent by asserting that if the individual knew about the benefits of the collection, use or disclosure, they would probably consent to it. An individual's silence should not be taken as implied consent. Consent may not be

[19] OAIC - The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information
[20] APP Guidelines – Chapter B: Key concepts
[21] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 60
[22] *Privacy Act 1988* (Cth) s 6(1)
[23] APP Guidelines – Chapter B: Key concepts

implied if an individual's intent is ambiguous or there is reasonable doubt to about the individual's intention.

The four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower the person's will.

WAPHA should not bundle together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

Use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances and WAPHA will be in a better position to establish implied consent if the following factors are taken into consideration:

- the opt out option was clearly and prominently presented
- it is likely that the individual received and read the information about the proposed collection, use or disclosure and the option to opt out
- the individual was given information on the implications of not opting out
- the opt out option was freely available and not bundled with other purposes
- it was easy for the individual to exercise the option to opt out, for example, there was little or no financial cost or effort required by the individual
- the consequences of failing to opt out are not serious
- an individual who opts out later will, as far as practicable, be placed in the position as if they had opted out earlier.

WAPHA should generally seek consent from an individual for collection and proposed uses and disclosures of personal information at the time the information is collected or ensure that the organisation collecting the personal information has done so and agreed for the information to be shared with WAPHA. Alternatively, if consent was not sought at the time of collection, or that consent did not cover a proposed use or disclosure, WAPHA should seek the individual's consent at the time of the use or disclosure.

WAPHA should generally seek express consent from an individual before handling the individual's sensitive personal information, given the greater privacy impact this could have. WAPHA will record consent on the Information Management Register – Request for Access where consent for the handling of sensitive personal information was obtained and whether express or implied consent was given.

4. Australian Privacy Principles

The APP Guidelines issued under Section 28(1) of the Act are not legally binding however to improve information and data governance, openness and transparency, this Code has been developed in keeping with the thirteen principles set out in Schedule 1 of the Act.

Part 1 – Consideration of Personal Information (APP1 and 2)

4.1 APP1 – Open and transparent management of personal information

WAPHA has developed policies and procedures to manage personal information in an open

and transparent way. This Code is in addition to the Privacy Policy, Information Management Policy, Information Management Manual and Website Privacy Policy and related documents and processes.

WAPHA meets the three separate obligations imposed on an APP entity through the (WAPHA Privacy Code of Practice, Privacy Policy, Information Management Policy, Information Manual) which outline that it has:

- taken reasonable steps to implement practices, procedures, and systems to deal with public information and is able to deal with related inquiries and complaints
- a clearly expressed and up to date APP Privacy Policy about how the entity manages personal information
- taken reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form (available to download from the WAPHA website)
- a commitment to conducting a Privacy Impact Assessment for new projects in which personal information will be handled, or when a change is proposed to information handling practices
- governance mechanisms to ensure compliance and
- regular staff training and information bulletins on how the APPs apply to WAPHA, its practices and processes.[24]

4.2 APP2 – Anonymity and Pseudonymity

'Anonymity' requires that an individual may deal with WAPHA without providing any personal information or identifiers. WAPHA should not be able to identify the individual at the time of the dealing or subsequently. Most information used by WAPHA for planning, commissioning and quality assurance health services is anonymized or de-identified at source and does not come under the Act.

'Pseudonymity' does not necessarily mean that an individual cannot be identified, just that they are using a different name or code to protect their real identity, e.g. WAPHA may use contract numbers or codes in published information to protect personal information.

In circumstances where WAPHA would not be able to offer anonymity or pseudonymity to an individual, such as during a procurement or recruitment process, the Act will apply and WAPHA will ensure there are sufficient measures to protect any personal information as far as practicable.

Part 2 – Collection of personal information (APP3, 4 and 5)

4.3 APP3 – Collection of solicited personal information

WAPHA may only solicit or collect personal information that is reasonably necessary for one or more of its functions or activities. This means any personal information directly obtained from individuals who have consented to their sensitive information being collected by lawful and fair means unless an exception applies.

Examples of solicited information include:

- personal information provided by an individual in response to a request, direction, or order
- any personal information about an individual provided by another entity in response to a request, direction, order, or arrangement for sharing or transferring information
- an employment application sent in response to a job advertisement or expression of interest

[24] OAIC - Chapter 1: APP 1 — Open and transparent management of personal information

- record of credit card payment.

WAPHA may collect sensitive information if a 'permitted health situation' exists (see also section 2.2) in relation to the connection.[25] Research, compilation or analysis of statistics, management, funding or monitoring of health service providers are permitted exceptions under the Act.[26]

'Lawful' collection is not defined in the Privacy Act. The destruction or de-identification of unsolicited personal information may be unlawful if it is obtained by non-lawful means, such as computer hacking; surveillance or used for discrimination.

'Fair means' of collecting information is based on the circumstances. Unfair collection includes personal information collected:

- by deception
- from a printed or electronic document lost or disposed of by accident
- where the purpose of collection has been misrepresented or
- in a way that disrespects cultural differences.

APP 3.6 allows the collection of personal information by exception where it is unreasonable or impractical for the entity to collect personal information only from the individual. For example, WAPHA collects information for individuals accessing commissioned mental health services and it would be impractical or intrusive to contact individuals directly. In culturally specific services, collecting individual personal information in a centralized way may disrespect local cultural differences.[27]

Section 13B(1)(a) of the Act provides that the collection of personal information about an individual (other than sensitive information) by a body corporate from a related body corporate is generally not 'an interference with the privacy of an individual'. This provision applies to the collection of information from related bodies corporate and not to other corporate relationships such as a franchise or joint-venture relationship. WAPHA may obtain legal advice before collecting personal information on a regular basis from new related body corporates to ensure any information sharing conforms with the Act.

4.4 APP4 – Dealing with unsolicited personal information

Unsolicited personal information is personal information received by WAPHA that has not been requested. For example, a commissioned service may provide personal information (such as surnames instead of codes) not required by WAPHA as part of its reporting requirements.

If WAPHA receives unsolicited personal information that is not reasonably necessary or directly related to one or more of its functions or activities then it has an obligation to destroy or de-identify the personal information as soon as practicable, unless it is unlawful or unreasonable to do so.

WAPHA may retain unsolicited personal information if it determines that it could have been collected as solicited personal information under APP3 or if it is not reasonable for WAPHA to destroy or de-identify it (such as complex information received from a third party where personal information is intrinsic to its use). WAPHA may only use the personal information for the primary purpose it was collected unless an exception applies (see also APP6).

[25] Australian Privacy Principles 3.4(c)
[26] Australian Privacy Principles 3.4(c)
[27] Australian Privacy Principles 3.6

If personal information is contained in a 'Commonwealth record' the WAPHA should comply with the provisions of s 24 of the *Archives Act 1983* (Cth), with permission from the National Archives of Australia (as set out in the records disposal authority).[28]

4.5 APP5 – Notification of the collection of personal information

WAPHA must take reasonable steps either to notify an individual of the collection of personal information or to ensure that the individual is aware of those matters. More rigorous steps may be required when collecting 'sensitive information' or information of a sensitive nature. This must also consider any special needs of the individual and if English is not their first language.

WAPHA's website privacy policy notifies individuals about any personal information that might be collected during their interaction with the WAPHA website – www.wapha.org.au.

WAPHA may need to prepare a specific statement in relation to a project if it collects sensitive personal information directly or indirectly from individuals with special needs to ensure awareness of the facts and circumstances of collection. This requirement applies where the personal information has been collected from a third party or the individual may not be aware that WAPHA has collected their personal information.[29]

If the collection is required or authorized by or under an Australian law, then any notice should include the details of the law, regulation or other instrument or a generic description of the laws if there are many (e.g. federal health legislation).

WAPHA may disclose information on a regular basis to third parties for the purpose of software development, planning of services and during the recruitment process. WAPHA does not disclose personal information to third parties unless it is necessary to the third party to use for the provision of health services.

Individuals may access and seek correction of their personal information held by WAPHA under the Complaints and Appeals Management Policy.[30]

It is not usual practice for WAPHA to disclose personal information to an overseas recipient. WAPHA stores all its electronic information and data in Australia in accordance with its cybersecurity policies and procedures. If WAPHA had to disclose personal information overseas, it will notify the individuals of the location of those recipients and the intended use of the information.[31]

Part 3 – Dealing with personal information (APP6, 7, 8 and 9)

4.6 APP6 – Use or disclosure of personal information

APP6 does not apply where WAPHA collects health information under an exception (see 2.2 above) to APP3 Collection of solicited information. Section 16B(2) of the Act allows WAPHA to collect health information about an individual if the collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to

[28] OAIC – Chapter 4: APP 4 — Dealing with unsolicited personal information
[29] OAIC – Chapter 5: APP 5 — Notification of the collection of personal information
[30] Australian Privacy Principles 5.2(g) and (h)
[31] Australian Privacy Principles 1.4(f) and (g)

public health or safety, or the management, funding or monitoring of a health service and certain other criteria are satisfied (see 2.2 above).
WAPHA takes all reasonable steps to ensure information is de-identified before it discloses information in accordance with APP 6.1 or 6.2.[32] For all other personal information, the following applies:

Holding personal information
WAPHA 'holds' personal information in electronic or paper records and information stored by third parties on its behalf. For example, an APP entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information.

WAPHA may hold and store information on behalf of third parties who retain the right to deal with that information. WAPHA may extract de-identified information from personal information stored on behalf of third parties for reporting, management, quality assurance and commissioning purposes. De-identified information is not subject to the Act.

Using personal information
WAPHA 'uses' information where it handles or undertakes an activity with the information within its control. This includes:
- accessing and reading the personal information
- searching records for the personal information
- making a decision based on the personal information
- passing the personal information from one part of WAPHA to another
- unauthorized access by an WAPHA employee (or authorized contractor or supplier).

Disclosing personal information
WAPHA discloses information when it makes accessible to others outside WAPHA and releases the subsequent handling of the information from its effective control. WAPHA will only disclose necessary personal information when it is essential for its activities.[33]

Any requests and disclosure of personal information to third parties outside is recorded on WAPHA's Information Management Register. The Register records:
- the date of use or disclosure
- details of the personal information that was used or disclosed
- how the personal information was / is to be used and
- to whom the personal information was disclosed.

4.7 APP7 - Direct Marketing

Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services. WAPHA must, on request, provide its source for an individual's personal information, unless it is impracticable or unreasonable to do so.

Examples of direct marketing include displaying an advert on a social media site that an individual is logged into, using personal information, including data collected by cookies relating to websites the individual has viewed. Marketing is not direct if personal information is not used or disclosed to identify or target particular recipients, such as sending 'To the householder,' or promotional flyers to local residents or adverts on a website which do not use personal information to select which adverts are displayed.

If WAPHA conducts direct marketing it must provide an option for individuals to 'opt out' which is free or at a nominal cost, such as a telephone call or postage stamp. If an individual has

[32] OAIC - Chapter 6: APP 6 — Use or disclosure of personal information
[33] OAIC - Chapter 6: APP 6 — Use or disclosure of personal information

opted out, WAPHA must not use or disclose their personal information in direct marketing.[34]

Before any direct marketing campaign, WAPHA Communications Team will review the guidance under APP7, *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth) to ensure that no personal information is used incorrectly and that an 'opt out' option is clearly identified.

4.8 APP8 - Cross-border disclosure of personal information (overseas)

WAPHA must take reasonable steps to ensure that any overseas recipient does not breach the Australian Privacy Principles in relation to the information as it is accountable for any acts or practices of the overseas recipient.[35]

'Overseas recipient' is a person who receives personal information and is not in Australia or an external Territory and not the individual to whom the personal information relates. This includes if WAPHA staff disclose information to an international conference or publishes it personal information on the internet, whether intentionally or not, and it is accessible to an overseas recipient.

If WAPHA provides personal information to an overseas contractor to perform services on its behalf and does not release the subsequent handling of personal information from its effective control, then APP8 would not apply.[36] Any contract with a third-party overseas supplier should include a clause requiring them to adhere to the Australian Privacy Principles and *Privacy Act 1988* (Cth) to ensure any personal and sensitive information is protected.[37]

4.9 APP9 - Adoption, use or disclosure of government related identifiers

A government related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract. Medibank, Centrelink Reference, driver license and Australian Passport numbers are examples of government related identifiers.[38]

WAPHA may hold government related identifiers for prospective employees or as part of information provided from a health service which has not been de-identified at source. WAPHA must not organise personal information it holds about that individual with reference to that identifier.[39]

WAPHA may only use a government related identifier to confirm a person's identity with them but otherwise will not disclose identifiers to anyone other than that individual.[40] WAPHA may also disclose a government related identifier in the event of an investigation into fraud or otherwise ordered by an enforcement body for enforcement related activities (e.g. tax fraud).[41]

Part 4 – Integrity of personal information (APP10 and 11)

[34] OAIC - Chapter 7: APP 7 — Direct marketing

[35] *Privacy Act 1988* s 16C, s 2A(f) and APP8
[36] OAIC - Chapter 8: APP 8 — Cross-border disclosure of personal information
[37] *Privacy Act 1998* s 95B and APP8.1
[38] *Privacy Act 1988* (Cth) s 6(1) – an 'identifier' is a number, letter, symbol, or combination used to identify or verify the identity of an individual.
[39] OAIC - Chapter 9: APP 9 — Adoption, use or disclosure of government related identifiers
[40] Australian Privacy Principles 9.2(a)
[41] *Privacy Act 1988* (Cth) s 6(1) – enforcement bodies include Police, Immigration Department and ASIC.

4.10 APP10 – Quality of personal information

WAPHA must take reasonable steps to ensure that the personal information it collects, uses, and discloses is accurate, up-to-date, and complete (see also APP13).[42] Whether personal information is out of date will depend on the purpose for which it is collected, used, or disclosed. Personal information held by WAPHA that is no longer needed for any purpose will be destroyed or de-identified (see also APP11).

The terms 'accurate,' 'up-to-date', 'complete' and 'relevant' are not defined in the Act and retain their original dictionary meanings.
WAPHA has taken the following reasonable steps to ensure any personal information it collects, uses, and discloses is up-to-date and complete by:

- implementing internal practices, procedures, and systems to audit, monitor, identify and correct poor quality personal information (including training staff in these practices, procedures, and systems)
- implementing protocols that ensure personal information is collected and recorded in a consistent format
- ensuring updated or new personal information is promptly added to relevant existing records
- providing individuals with a simple means to review and update their personal information on an on-going basis, for example through an online portal
- contacting the individual to verify the quality of personal information when it is used or disclosed, particularly if there has been a lengthy period since collection
- checking that a third party, from whom personal information is collected, has implemented appropriate practices, procedures, and systems to ensure the quality of personal information. Depending on the circumstances, this could include:
    - making an enforceable contractual arrangement to ensure that the third party implements appropriate measures to ensure the quality of personal information the entity collects from the third party
    - undertaking due diligence in relation to the third party's quality practices prior to the collection
- if personal information is to be used or disclosed for a new purpose that is not the primary purpose of collection, assessing the quality of the personal information having regard to that new purpose before the use or disclosure.

Information and data quality is a key part of WAPHA's information management and data governance strategy and is overseen by the Digital and Data Strategic Advisory Group. Information and data collections are regularly checked for accuracy, up-to-date, completeness and relevance on a regular basis as part of the Data Governance and Data Quality Manager's audit plan.

4.11 APP11 – Security of personal information

WAPHA must take active steps to ensure the security of personal information and to actively consider whether it is permitted to retain the personal information.

WAPHA takes reasonable steps to protect personal information it holds from misuse, interference, and loss, as well as unauthorised access, modification, or disclosure as part of its Data Governance and Data Quality management including:

- governance, culture, and training

[42] OAIC - Chapter 10: APP 10 — Quality of personal information

- internal practices, procedures, and systems
- ICT (Information and Communications Technology) and access security
- Third party providers (including cloud computing)
- Data breaches – recorded on the Information Management Register
- Physical security at the Subiaco office
- Destruction and de-identification
- Privacy Policy, Information Management Policy standards.

WAPHA adheres to the Office of the Australian Information Commissioner's *Guide to Securing Personal Information*.

WAPHA minimises the use of personal information as far as practicable in the day-to-day business of the organisation and carries out regular audits of its electronic record keeping systems to destroy any information no longer required. The processes for de-identification and destruction of information are detailed in the Information Management manual.

WAPHA will complete a Threshold Assessment for all information and/or data collection which will consider whether a full Privacy Impact Assessment is required. The Privacy Impact Assessment will detail any additional security measures required to protect personal information within the data set.

WAPHA's Risk Register lists identified security of personal information risks. Security measures and procedures are detailed in WAPHA's Information Management Manual.

Part 5 – Access to, and connection of, personal information (APP12 and 13)

4.12 APP12 – Access to personal information

WAPHA is required to provide personal information to an individual on request unless it can be refused under the *Freedom of Information Act 1992* (WA), due to legal privilege or other lawful exception under APP 12.2(b)(ii).[43]

APP12.3 lists ten grounds on which refusal for access to personal information can be given:

- Where WAPHA believes that giving access would pose a serious threat to the life, health, or safety of any individual, or to public health or public safety.
- Giving access would have an unreasonable impact on the privacy of other individuals.
- The request for access is frivolous or vexatious.
- The information relates to existing or anticipated legal proceedings between the organisation and the individual and would not be accessible by the process of discovery in those proceedings.
- Giving access would reveal the intentions of WAPHA in relation to negotiations with the individual in such a way as to prejudice those negotiations.
- Giving access would be unlawful.
- Denying access is required or authorized under an Australian law or a court/tribunal order
- The organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, which relates to WAPHA's functions or activities has been, is being or may be engaged in giving access would be likely to prejudice the taking of appropriate action in relation to the matter.

[43] OAIC – Chapter 12 – Access to personal information

- Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.
- Giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process.[44]

The process for requesting access to personal information and any information outside of normal or contracted use is detailed in the Information Management Manual and requests are recorded on the Information Management Register – Request for Access.

WAPHA must respond to requests for information within 30 calendar days, commencing on the day after the date WAPHA receives the request.

WAPHA may provide access to personal information through a suitably qualified intermediary. This may be useful when health personal information is held by WAPHA on behalf of a third party, e.g. an individual's qualified health service provider. WAPHA may request the general practitioner to provide the personal information to the individual on WAPHA's behalf, to further limit the exposure of the personal information in question.

WAPHA is not permitted to charge for providing access to personal information, including the costs of using an intermediary. However WAPHA may charge for staff costs for giving access to personal information, provided the charge is not excessive.[45]

If WAPHA refuse access to personal information, it will provide a written notice setting out:

- the reasons for the refusal, except to the extent that it would be unreasonable to do so, having regards to the grounds for refusal
- the internal and external complaint mechanisms available to the individual; and
- any other matters prescribed by regulations made under the Privacy Act
- any steps that could be taken by the individual to reframe or narrow the scope of the request so that approval can be given.

4.13 APP13 – Correction of personal information

WAPHA must take reasonable steps to correct personal information it holds to ensure that it is accurate, up-to-date, complete, relevant, and not misleading, having regard to the purpose for which it is held. WAPHA can correct personal information on its own initiative or by request from the individual to whom the personal information relates.[46]

For example, an individual may apply for a role within WAPHA as part of a recruitment process and later request WAPHA to update their contact details which contain personal information. WAPHA must take reasonable steps to update this information, even though the person is not an employee yet.

APP 13 overlaps with the requirements of other Principles, including APP10 and APP 11 above.

WAPHA has developed centralised electronic record keeping systems to minimise the amount of personal information kept on separate systems and improve quality and efficiency.

WAPHA may refuse to correct personal information because:

- WAPHA does not hold the personal information that the individual wishes to correct

[44] OAIC – Chapter 12 – Access to personal information
[45] OAIC – Chapter 12 – Access to personal information – Access charges under APP12 – organisations.
[46] OAIC – Chapter 13 – Correction of personal information

- WAPHA is satisfied that the personal information is accurate, up-to-date, complete, relevant, and not misleading having regard to the purposes for which it is held, or
- that the steps necessary to correct the personal information as requested are not reasonable in the circumstances.

WAPHA should provide a notice in the terms set out in APP12 if a request to correct personal information is refused. If a refusal to correct personal information is given, an individual can request that a statement be added to the personal information to advise readers that the personal information is inaccurate, out-of-date, incomplete, irrelevant, or misleading.

WAPHA cannot charge individuals for requesting the correction of information or for making a correction or for associating a statement with the personal information.[47]

5. Data Analytics and Privacy-by-design

WAPHA carries out a range of data analytics processes, including:
- collating data from a wide variety of different sources, including from third parties
- generate new information through 'collection via creation'
- use data insights for a range of different purposes, including new purposes that may not have been anticipated, and
- retain data for a longer period of time than usual in case it may be useful in future for an unspecified purpose.

Privacy-by-design is a holistic approach to where privacy is integrated and embedded in an entity's culture, practices and processes, systems, and initiatives from the design stage onwards. WAPHA uses practice-by-design as part of its risk management approach to identifying and mitigating privacy risks. The key principles are:

- managing privacy proactively, rather than retrospectively after any privacy issues come to light
- recognising it is possible to have both 'good privacy' and effective, innovative use of data
- keeping the activity user-centric by offering strong privacy defaults, appropriate notifications systems, and empowering user-friendly options, and
- end–to–end security throughout the full lifecycle of the project, ensuring that all personal information is kept securely from collection through to destruction.[48]

6. De-identified information

'De-identified' information is information which has undergone a process of de-identification by WAPHA and no longer falls within the definition of 'personal information' under the Act. WAPHA may also receive information which is already de-identified and does not need any further processing.

De-identification involves the removal or alternation of information that identifies a person or is reasonably likely to identify them, as well as the application of any additional protections required to prevent identification. To de-identify effectively, WAPHA must consider not only the information and/or data collection itself, but also the environment the data will be released into. De-identification does not eliminate all risks, however the risk of re-identification in the data access environment must be very low (no reasonable likelihood of re-identification). The removal of name, address or other direct identifiers alone may not result in de-identification for the purposes of the Act.

[47] Australian Privacy Principles 13.5(b)
[48] OAIC – Guide to data analytics and the Australian Privacy Principles

De-identification is carried out in two steps:

- removing or altering other information that may allow an individual to be identified and/or
- putting controls and safeguards in place in the data access environment, which will appropriately manage the risk of de-identification.

WAPHA use the OAIC and CSIRO Data 61 De-identification Decision Making Framework to assist in the de-identification of personal information, together with OAIC's De-identification and the Privacy Act Guide. De-identification allows WAPHA to share or release information in a way that would not otherwise be permitted under the Australian Privacy Principles. The de-identification process is detailed in the Information Management Manual.

7. Privacy Impact Assessments (PIAs)

A Privacy Impact Assessment (PIA) is a systematic assessment of a project that identifies potential privacy impacts and recommendations to manage, minimise or eliminate them. PIAs should ideally be carried out at the start of a project however can be done at any time and should be regularly reviewed to ensure ongoing compliance and highlight areas for improvement.[49]

PIAs are part of WAPHA's risk management and planning processes and assists WAPHA to:

- describe how personal information flows in a project
- analyse the possible impacts on individuals' privacy
- identify and recommend options for avoiding, minimising, or mitigating negative privacy impacts
- build privacy considerations into the design of a project
- achieve the project's goals while minimising the negative and enhancing the positive privacy impacts.

WAPHA will carry out a PIA Threshold Assessment to determine whether a project requires a full PIA. PIAs will be completed for any new project involving information or any business system that has undergone significant change.

8. Notifiable Data Breaches

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure or is lost. A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.[50]

If WAPHA has reasonable grounds to believe an eligible data breach has occurred, they must promptly notify any individual at risk of serious harm. All private sector health service providers have obligations under the Notifiable Data Breaches scheme, which came into effect on 22 February 2018.

WAPHA must also notify OAIC if the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by WAPHA (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- WAPHA has been unable to prevent the likely risk of serious harm with remedial action.[51]

[49] OAIC - 10 steps to undertaking a privacy impact assessment
[50] OAIC - Part 1: Data breaches and the Australian Privacy Act
[51] OAIC - Notifiable data breaches

Data breaches involving My Health Records are reported to OAIC under a different system. Under s 75 of the *My Health Records Act 2012*, there are three types of data breaches:

- a person has or may have contravened the My Health Records Act in a manner involving an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record
- any event that has, or may have, occurred (whether or not involving a contravention of the My Health Records Act) that compromises, may compromise, has compromised, or may have compromised the security or integrity of the My Health Record system or
- any circumstances that have or may have arisen (whether or not involving a contravention of the My Health Records Act), that compromise, may compromise, have compromised, or may have compromised the security or integrity of the My Health Record system.[52]

WAPHA staff should follow the Notifiable Data Breaches procedure in the Information Management Manual.

The OAIC Notifiable Data Breach Form is available online at www.oaic.gov.au. A training version of the Notifiable Data breach form is also available. The OAIC Data Breach preparation and response guide provides assists organisations to prepare for and respond to data breaches.

9. Agencies

The Office of the Australian Information Commissioner (OAIC) is an independent agency whose primary functions are privacy, freedom of information and government information policy and whose responsibilities include conducting investigations, reviewing decisions, handling complaints, and providing guidance and advice. The Information Commissioner has powers to investigate possible interferences with privacy, either following a complaint by the individual concerned or on the Commissioner's own initiative.

Western Australia does not currently have any specific privacy legislation.[53] The Office of the Information Commissioner (WA) administers the *Freedom of Information Act 1992* (WA) which includes some privacy principles related to the disclosure and amendment of personal information held by Western Australian State and local government agencies (including Department of Health).

The Health and Disability Services Complaints Office (WA) is an independent statutory authority that also handles complaints relating to health and disability services in Western Australia, which includes data breaches from private and public health services.

[52] OAIC - Guide to mandatory data breach notification in the My Health Record system
[53] OAIC – Privacy in Your State – www.oaic.gov.au/privacy/privacy-in-your-state