



Australian Government

Australian Institute of Health and Welfare

# **DATA GOVERNANCE FRAMEWORK**

**2021**

**(Public edition)**

Date of approval: 06 April 2021

# Table of contents

<b>PART 1 – INTRODUCTION</b>	<b>6</b>
1 The Australian Institute of Health and Welfare (AIHW)	6
2 Audience	6
3 Data governance	6
4 The Framework	6
4.1 Key elements of good data governance	7
4.2 Scope	8
4.3 This 2021 edition of the Framework	8
5 Review, feedback and questions	9
<b>PART 2 – DATA GOVERNANCE CONCEPTS</b>	<b>10</b>
6 Data	10
7 Data collections	10
8 Data registry	11
9 The nature of data	11
9.1 Unit record data	11
9.2 Aggregate data	11
9.3 Identified data	11
9.4 Non-identified data	12
9.5 Identifiable data	12
9.6 De-identified data	13
10 Data integration and data linkage	13
11 Secure access environments	14
12 Separation principle	15
13 Metadata and metadata standards	16
14 Data policies, guidelines and procedures	16
15 Tools	16
<b>PART 3 – LEGAL, REGULATORY AND GOVERNANCE ENVIRONMENT</b>	<b>18</b>
16 The AIHW Act – our establishing legislation	18
17 AIHW Ethics Committee Regulations	19
18 Privacy Act	19
18.1 Australian Privacy Principles	19
18.1.1 Waivers	20
18.1.2 Authorised by law exceptions	21
18.2 Privacy Code	21
18.3 Notifiable Data Breaches scheme	21
19 National Health and Medical Research Council Guidelines	21
20 Freedom of information	22

<b>21</b>	<b>Protective Security Policy Framework and Information Security Manual</b>	<b>23</b>
<b>22</b>	<b>Other Commonwealth Legislation</b>	<b>23</b>
<b>23</b>	<b>State and Territory Legislation</b>	<b>23</b>
<b>24</b>	<b>Contracts, Agreements and Memoranda of Understanding (MOUs)</b>	<b>24</b>
<b>PART 4 – AIHW STRUCTURES AND ROLES IN DATA GOVERNANCE</b>		<b>25</b>
<b>25</b>	<b>AIHW Board</b>	<b>25</b>
25.1	Charter of Corporate Governance	25
<b>26</b>	<b>AIHW Ethics Committee</b>	<b>25</b>
26.1	Committee Functions	25
26.2	Ethical standards	26
26.3	Privacy Oversight	26
26.4	Approval of Institute Activities	27
26.4.1	Research with Aboriginal and Torres Strait Islander Peoples	28
<b>27</b>	<b>Risk, Audit and Finance Committee</b>	<b>28</b>
<b>28</b>	<b>All staff and contractors</b>	<b>28</b>
<b>29</b>	<b>AIHW Chief Executive Officer</b>	<b>29</b>
<b>30</b>	<b>AIHW Deputy Chief Executive Officer</b>	<b>29</b>
<b>31</b>	<b>AIHW Governance Committees</b>	<b>29</b>
31.1	Executive Committee	29
31.2	Data Governance Committee	30
31.3	ICT Strategic Committee	30
31.4	AIHW Security Committee	30
31.5	Statistical Leadership Committee	30
<b>32</b>	<b>Group Heads</b>	<b>31</b>
<b>33</b>	<b>Data Custodians</b>	<b>31</b>
<b>34</b>	<b>Authors of AIHW publications and on-line releases</b>	<b>32</b>
<b>35</b>	<b>AIHW’s Data Integration Services Centre</b>	<b>32</b>
<b>36</b>	<b>Privacy roles</b>	<b>32</b>
36.1	Privacy Champion	33
36.2	Privacy Officer	33
<b>37</b>	<b>Security Roles</b>	<b>33</b>
<b>38</b>	<b>Training Roles</b>	<b>34</b>
<b>PART 5 –SYSTEMS AND TOOLS TO SUPPORT DATA GOVERNANCE</b>		<b>36</b>
<b>39</b>	<b>AIHW ICT Framework</b>	<b>36</b>
<b>40</b>	<b>AIHW data catalogue</b>	<b>36</b>
<b>41</b>	<b>METeOR</b>	<b>37</b>
<b>42</b>	<b>Validata™</b>	<b>37</b>
<b>43</b>	<b>EthOS™</b>	<b>37</b>
<b>44</b>	<b>Data on Request Application (Ad hoc request system)</b>	<b>37</b>

<b>45</b>	<b>Institute Projects</b>	<b>38</b>
<b>46</b>	<b>Secure Messaging and file transfer</b>	<b>38</b>
<b>47</b>	<b>Review and approval (R-A) plan</b>	<b>38</b>
<b>PART 6 – AIHW DATA POLICIES, GUIDELINES AND PROCEDURES</b>		<b>39</b>
<b>48</b>	<b>Managing the data life-cycle</b>	<b>39</b>
48.1	Collection establishment	39
48.1.1	Proposals to establish a new collection	39
48.1.2	What constitutes an AIHW data collection?	40
48.1.3	Approval to establish a new collection	40
48.1.4	Data catalogue entry	41
48.1.5	Listing collections on the AIHW Web Site	41
48.1.6	Data Collection Management Principles	42
48.1.7	Quality Framework	42
48.2	Data acquisition	43
48.2.1	Metadata	43
48.2.2	Data validation and data quality	43
48.2.3	Data storage and security	44
48.3	Data access and use within AIHW	44
48.3.1	Access to AIHW ICT systems	44
48.3.2	Access to AIHW Research Only Network	45
48.3.3	Application of the separation principle	45
48.3.4	Data linkage	46
48.4	Data sharing and release for use outside the AIHW	47
48.4.1	Data sharing and release	47
48.4.2	Preconditions for data sharing or release	48
48.4.3	De-identification	49
48.4.4	Approval for data sharing or release	50
48.4.5	Access arrangements for data sharing and release	50
48.4.6	The Five Safes framework	52
48.4.7	Conditions for data sharing	55
48.4.8	Managing Statistical Outputs	56
48.4.9	Register of data shared or released	57
48.5	Data archiving, return, collection retirement and destruction	57
48.5.1	AIHW data collections	57
48.5.2	Project specific datasets	58
<b>PART 7 – COMPLIANCE</b>		<b>59</b>
<b>49</b>	<b>Breaches</b>	<b>59</b>
49.1.1	Data breach	59
49.1.2	Privacy breach	59
49.1.3	Ethics breach	60
49.1.4	Data and privacy breach response plan	60
49.1.5	Data and privacy breach and incident registers	60
<b>50</b>	<b>Sanctions</b>	<b>60</b>
<b>51</b>	<b>Dealing with complaints</b>	<b>61</b>
<b>List of Appendices</b>		<b>61</b>
<b>Appendix 1 – Glossary of terms and acronyms</b>		<b>62</b>

**Appendix 2 – Data collection management principles \_\_\_\_\_ 71**

Principle 1 – Data collections are established and managed effectively, appropriately and consistently, with clear accountability requirements and governance arrangements. \_\_\_\_\_ 71

Principle 2 – Data receipt processes ensure the security and integrity of the data during transfer. \_\_\_\_\_ 71

Principle 3 – Data are stored securely and regularly backed up. \_\_\_\_\_ 71

Principle 4 – Integrity of the data is maintained. \_\_\_\_\_ 71

Principle 5 – Controls for persons/entities having access to the collection exist and are implemented. \_\_\_\_\_ 72

Principle 6 – Data transmission or dissemination from the collection to any source (internal or external) is conducted in a manner which ensures its accuracy, integrity and security. \_\_\_\_\_ 72

Principle 7 – End of data lifecycle/use is appropriately managed \_\_\_\_\_ 72

**Appendix 3 – Alphabetical list of key legislation, policies and guidelines in the Framework \_\_\_\_\_ 73**

---

## PART 1 – INTRODUCTION

### 1 The Australian Institute of Health and Welfare (AIHW)

The AIHW is a major national agency established under the [Australian Institute of Health and Welfare Act 1987](#) (AIHW Act) as an independent statutory body to collect and produce information and statistics on Australia's health and welfare.

The AIHW produces authoritative and accessible information and statistics to inform and support better policy and service delivery decisions, leading to better health and wellbeing for all Australians.

### 2 Audience

This document contains key information for all AIHW staff and contractors, particularly those who have delegated authority to make data-related decisions.

A separate edition of this Data Governance Framework (the Framework) will be produced for external stakeholders to provide information for those many organisations and agencies that provide data to, or receive data from, the AIHW, as well as its partners, stakeholders and end-users of AIHW data and information.

### 3 Data governance

**Data governance** is "... a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions, with what information, and when, under what circumstances, using what methods."<sup>1</sup>

Data governance describes: the source of authority for making decisions about data; the roles/structures authorised to make decisions; and the basis upon which those decisions are made.

### 4 The Framework

The Framework was first developed in 2014 and has been updated periodically since.

As an information agency, AIHW relies upon strong data governance to perform its functions effectively and maintain a trusted reputation amongst its many data suppliers, data users and other stakeholders.

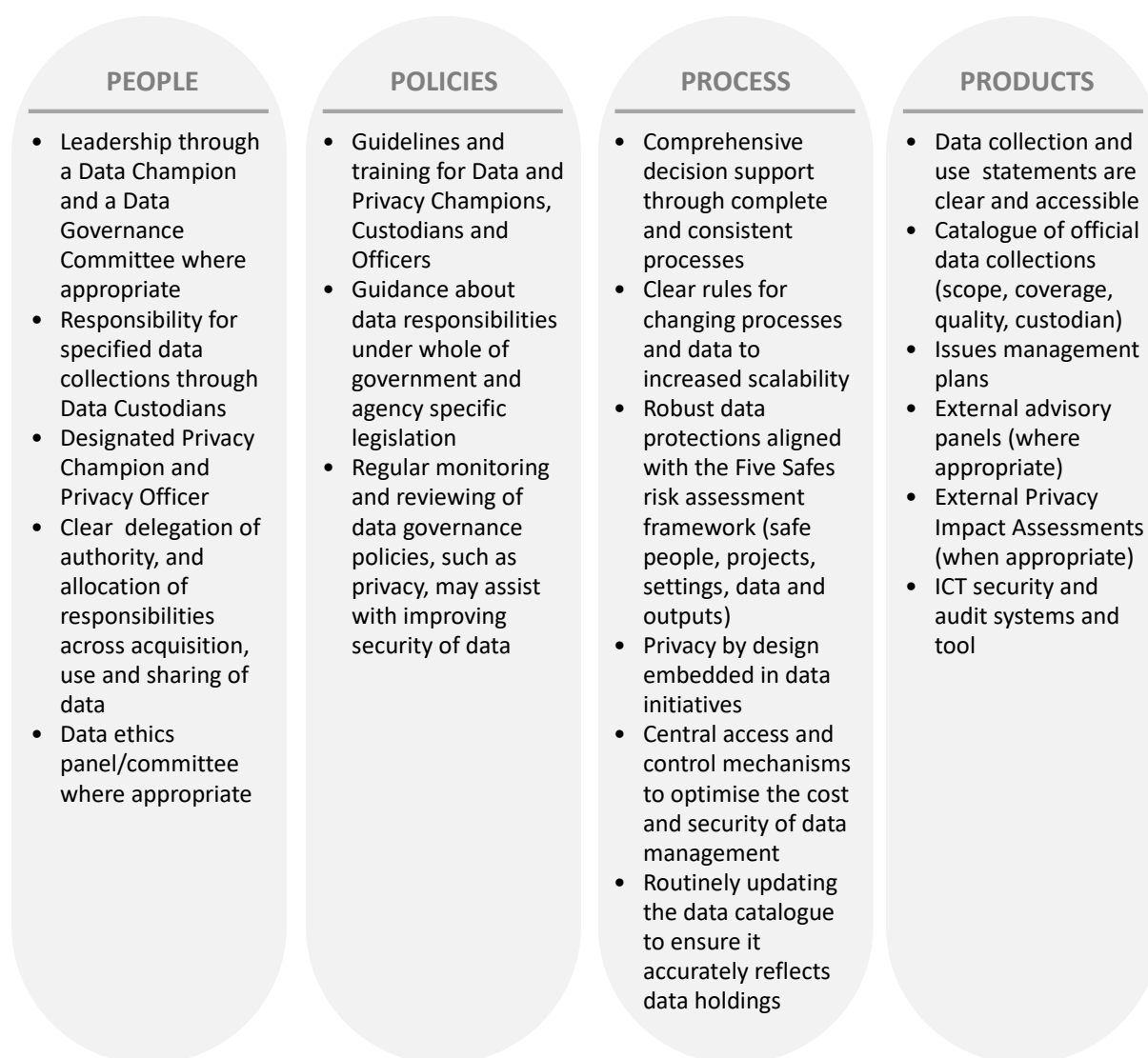
This Framework lists the elements that comprise the AIHW approach to data governance, and describes in detail how they work together to support the legal, ethical and safe management of our data holdings. It recognises that a combination of supporting legislation, roles, policies, practices, standards, tools and technologies is required to deliver effective data governance arrangements at AIHW.

<sup>1</sup> Data Governance Institute, [http://www.datagovernance.com/adg\\_data\\_governance\\_definition/](http://www.datagovernance.com/adg_data_governance_definition/) accessed 25 March 2020.

## 4.1 Key elements of good data governance

The Department of the Prime Minister and Cabinet, in the 2020 guide [Trust in Government Data Use](#), notes that good data governance is required to ensure safe data practices. The document provides the following description of the key elements of good data governance, each of which are addressed in this Framework.

### KEY ELEMENTS OF GOOD DATA GOVERNANCE



The Framework supports AIHW policy that it *works to understand the drivers of community trust in its management and use of data, and undertakes its work in ways that guard that trust.*

## 4.2 Scope

The Framework identifies and provides links to key internal and external documents that collectively define these arrangements. The Guidelines for the custody of AIHW data is a legally enforceable governance instrument that states many of the key obligations related to custodianship of AIHW data. The two documents support one another: this framework describes the system of governance; the guidelines and other documents referenced in this Framework provide policy.

The data governance arrangements described in the Framework apply to AIHW data collections and other data holdings listed in the data catalogue.

The framework explains a number of key aspects of data governance:

- the key concepts in the AIHW context
- the legal and regulatory environment that shapes AIHW's arrangements
- the various structures, roles and responsibilities
- the AIHW ICT systems and tools
- the policies, guidelines and procedures
- compliance regimes, and
- how these elements work together to support the AIHW in executing its functions and meet its data-related obligations.

The Framework has been developed to be sufficiently flexible to apply to new and emerging areas of AIHW data management arrangements such as cloud storage, Multi-sourced Enduring Linked Data Assets (MELDAs), and potential use of machine learning to analyse large data sets. Where these new approaches require changes to this Framework, they will be included in future editions.

The Framework does not address matters related to corporate information governance, such as: management of personnel and financial records; meeting papers and minutes; correspondence and emails; or intranet content.

## 4.3 This 2021 edition of the Framework

The Framework was comprehensively revised and updated in 2020 to reflect changes in the AIHW operating environment and governance landscape. The 2021 minor update reflects policy changes agreed since the last edition.



## 5 Review, feedback and questions

Data governance needs to be reviewed regularly to ensure that existing arrangements continue to reflect contemporary relationships, practices and available technology. This Framework will be reviewed regularly by the Data Governance Committee, and minor updates may be made at any time following consultation with the Heads of the Data Governance and Data Strategies and Integration Groups.

AIHW staff should direct questions regarding the Framework, or suggestions for inclusions or enhancements, to the AIHW Ethics, Privacy and Legal Unit.

Questions and comments from the AIHW's stakeholders, including members of the public, may be submitted via the [contact page](#) of the AIHW website.

## PART 2 – DATA GOVERNANCE CONCEPTS

This Part introduces terms and concepts commonly used in data governance and data management. It provides context for the AIHW-specific data governance arrangements described later in the Framework.

A comprehensive glossary of terms and acronyms is at **Appendix 1**.

### 6 Data

**Data** are 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 includes information about persons, businesses and other organisations and their characteristics, practices and activities.

Data can be stored in structured formats (e.g. databases), semi-structured formats (e.g. spreadsheets) and non-structured formats (e.g. documents).

### 7 Data collections

Individual sets of data may be called ‘data collections’, ‘data assets’ or ‘data holdings’. The AIHW uses the term ‘data collection’ to identify formally recognised and governed sets of data.

The AIHW defines a **data collection** as a cohesive set of data with measurable value that is designed to address a specific set of business needs. AIHW data collections are listed in the AIHW data catalogue, assigned an AIHW data custodian, and subject to strict governance arrangements detailed in the Guidelines for the custody of AIHW data and other AIHW policies and guidelines.

Section 48.1 of this Framework provides more detail on AIHW data collections.

Data comprising a data collection may come from various *sources*. They may be: collected or created internally by an organisation; gathered through surveys; obtained from, or held on behalf of, single or multiple external organisations or governments; or merged from several other data collections. The source(s) of data can influence conditions and controls placed upon them.

## 8 Data registry

A **data registry** is a log of all data holdings managed by an organisation. A data registry commonly holds a minimum of the following metadata about each holding: the date of commencement; duration of use (ongoing or finite); any caveats, for example restrictions on use of the data and/or notes regarding data quality; users; and the purpose of the data collection.

Ideally, a data registry also contains operational metadata that supports efficient and effective use, re-use, sharing, release and logging/monitoring of data. It is a central platform that enables traceability and accountability of data usage.

The AIHW's data registry is known as the AIHW **Data Catalogue**.

The AIHW Data Catalogue is described in section 40 of this Framework.

## 9 The nature of data

The *nature* of data also impacts controls placed upon them. Data may be unit record data and /or aggregate data, and may contain, identified, non-identified, identifiable or de-identified data.

### 9.1 Unit record data

**Unit record data** are detailed data comprising individual records, where each record contains information about a particular unit of interest.

Units of interest could include persons, organisations, or transactions.

### 9.2 Aggregate data

**Aggregate data** are data that have been created from more detailed data by calculation of summary statistics and/or grouping information into categories.

Aggregated data have less detail than the data from which they are derived. They can be unit record data, where the unit is a 'higher level' than the more detailed data from which they are derived (for example, patient data may be aggregated to the level of hospital), but they are commonly summary statistics presented in tables.

Aggregation of data is a (data reduction) method that can contribute to de-identification.

### 9.3 Identified data

**Identified data** about individuals or organisations that includes identifying information – typically, name, address, and perhaps date of birth – allowing the person or organisation to be known from just a few fields of data.

## 9.4 Non-identified data

**Non-identified data** about individuals or organisations where identifying information are not present but no further de-identification techniques or controls have been applied.

Note that non-identified data may still be identifiable data.

## 9.5 Identifiable data

**Identifiable data** are data that contain sufficient detail that a person(s) or organisation(s) can be re-identified from the data, given the particular circumstances.

The Privacy Act provides a foundation for a minimum standard of identifiability, 'reasonably identifiable', where:

- it is technically possible for re-identification to occur (whether from the data itself, or in combination with other data that may be available), and
- there is a reasonable likelihood of re-identification occurring.

Following legal advice in 2013, the AIHW applies the same minimum standard – 'reasonably identifiable' – to whether data are identifiable under both the Privacy Act and the confidentiality provisions of the AIHW Act.

Determining whether an entity – a person or organisation – is 'reasonably identifiable' requires a consideration of the particular circumstances, including:

- a) the nature and amount of data
- b) who will hold and have access to the data; and
- c) the other data and information that is available, and the practicality of using that data and information to identify an individual.

The determination of whether the likelihood of re-identification is 'reasonable' requires informed judgement.

Both aggregate data and unit record data can contain identifiable data.

Other standards of identifiability may be appropriate.

A data supplier to the AIHW may stipulate a higher threshold than 'reasonably identifiable' as a condition of supply of identified data; they may require that under no circumstances is the AIHW to disclose (release or share) data that could result in any individual or organisation being identified.

All data collections are subject to policies, processes, guidelines and controls. However additional strict constraints regarding collection, storage, use, linkage and disclosure apply to identifiable information.

These constraints include the requirements of the privacy laws of Australian states and territories and of the Commonwealth, and numerous other legislative and internal controls designed to protect individuals from the improper use or release of their information. The key legislative and regulatory controls applicable to the AIHW are further explored in Part 3 of this Framework.

## 9.6 De-identified data

**De-identified data** are data that were previously identifiable but have been treated to remove, obscure, aggregate, alter and/or protect data, with a view to ensuring that there is no reasonable likelihood of identifying individual(s) within the data.

De-identification can be a highly technical process that typically involves the following steps:

1. The removal of direct identifiers, such as the individual's name, address or other directly identifying information, and
2. Removing or altering (data reduction or data modification) other information that may allow an individual to be identified, and/or
3. Putting controls and safeguards in place associated with the data access environment that limit access to tools, opportunities and other information that could allow an individual to be identified.

De-identified data are not (or no longer) about identified or reasonably identifiable individuals or organisations.

Whether data have been de-identified or not depends heavily on the particular circumstances.

For example, data in a secure environment that prevents linking to other data may be de-identified in that context, but be reasonably identifiable if released to the public at large.

De-identified unit record data are frequently called Confidentialised Unit Record Files (CURFs) when made available for open access or provided through delivered access. Because CURFs may be made available in non-secure environments, they are subject to extensive data reduction and modification to reduce the likelihood of re-identification in that context.

From the perspectives of the Privacy Act and the AIHW Act, it is neither realistic nor expected that AIHW remove the risk of re-identification entirely. Rather, we must mitigate the risk until it is very low: until there is **no reasonable risk** of re-identification occurring. There is a balance to be struck between providing data that is useful for research and ensuring that privacy and confidentiality are maintained. The aim is to make useful data available, safely.

As noted earlier, however, data suppliers to the AIHW may impose more stringent requirements on the use of their data than 'no reasonable risk' of re-identification.

## 10 Data integration and data linkage

**Data integration** is a method of bringing together data from different sources, but relating to the same individual, organisation, event or other unit.

**Data linkage** is a technical processes within data integration by which identifying information from different sources is used to identify records relating to the same unit.

Within the AIHW, we tend to use these terms interchangeably.

This methodology typically re-uses existing data and is non-intrusive because it avoids the need to re-contact people whose information has already been collected.

Analysis of linked data sets can enable innovative statistical analysis of interrelated data complex policy questions.

The AIHW's Data Integration Services Centre (DISC) links a range of datasets for research purposes.

**Project specific datasets** are created when the DISC works with internal and external researchers to combine datasets, most commonly with one or more AIHW data collections, for a specific project. This can be relatively straightforward when small researcher-supplied data are linked to a single AIHW data collection. These project specific datasets, however, are becoming increasingly complex as larger datasets are merged with multiple AIHW data collections.

**Multi-sourced Enduring Linked Data Assets (MELDAs)** are new AIHW data collections created through the integration of multiple data collections. The National Integrated Health Services Information Analysis Asset (NIHSI AA) was the first AIHW MELDA. Other MELDAs include the Cancer and Treatment Linked Analysis Asset (CaT-Link AA) and the proposed National Disability Data Asset (NDDA).

## 11 Secure access environments

**Secure Access Environments (SAEs)** are a means of providing researchers with access to highly detailed data in an environment that enables them to carry out their analysis while the data custodian maintains oversight of the data and manages outputs to ensure privacy and confidentiality are protected.

The main features of a SAE are:

- Access to an ICT and analytical empowered environment with very strong user authentication.
- Data are stored centrally on servers housed in a secure data centre. No data is stored on a researcher's local computing environment except where already permitted by the data custodian.
- The only way for a file to enter or leave a SAE is via the Curated Gateway. All inbound and outbound files are subject to review as they are curated through a gateway process before they can be accessed within the SAE or downloaded to a user's local computing environment.

The role of a SAE is to:

- Facilitate secure access to detailed data for researchers
- Provide data custodians with secure facilities to host unit record data with adequate end-to-end controls to manage risk appropriate to their dataset
- Facilitate access to analytical tools and appropriate computing power for research
- Be transparent in operation, providing data custodians and AIHW administrators with appropriate real time reporting and audit logs.

SAEs include both on-site data labs, managed within the physical environment of the data custodian (such as the AIHW Data Laboratory), and remote access SAEs, where data are accessed by the researcher from their workplace via a secure connection into a secure environment hosted on behalf of the data custodian. SAEs with remote access capability

combine many of the advantages of the secure on-site setting with the flexibility of having access to data from one's desktop.

SAEs can include cloud-based environments.

Examples of remote access SAEs include the Sax Institute's Secure Unified Research Environment (SURE) and The Department of Health Enterprise Data Warehouse (EDW), AIHW's Secure Remote Access Environment (SRAE) and AIHW's Research Only Network (RON) – see section 48.4.5 for more detail on these environments.

## 12 Separation principle

The **separation principle** is a mechanism to protect the identities of individuals and organisations and builds on the foundation that access to confidential data should be limited to those who need it.

**The separation principle** ensures that access to identifying information that might be used for data linkage (such as name, address, date of birth) is kept separate from access to the content information used for analysis (such as clinical information, medication, age, height, weight or cause of death). Individuals have access to **either** the linking data **or** the analysis data, **never both** at the same time.

Individuals only have access to the information they need to do their role.

Note that some fields (e.g. month of birth and year of birth) may be useful for both linkage and analysis, so the distinction between linkage and analytical fields is not necessarily mutually exclusive. Content data exclude identifying information (and are therefore non-identified data) and are also treated so that they are de-identified (in the analysis environment). Judgement is required in deciding which information is to be included in the identifying information; adding analysis variables can improve the rate of record linkage but may also result in disclosure of sensitive analysis information to those performing the linkage.

Implementation of the separation principle can be achieved in a variety of ways, including:

- Physical separation and separate storage of identifiers and content information. Physical separation can be undertaken within the AIHW Data Integration Service Centre, through the AIHW Validata™ tool, or data suppliers may provide separate files containing linkage data and content data at separate times. Physical separation and separate storage also requires careful application of ICT access control arrangements.
- Virtual separation by managed views of the data through application of ICT access control arrangements; individuals' access to different views of the dataset is carefully managed through ICT permissions. Under this arrangement, the dataset remains as one, but individual users are given permission to see only the identifiers or the content, never both.

Application of the separation principle may be reinforced by role separation, whereby individuals are assigned roles associated with either the identifiers or the content, never both. For example, when linking datasets, the data linkers work exclusively with the identifying data of each dataset to create the linkage keys. The data mergers use these keys to create the combined (linked) content dataset. Linkers never see the content; mergers never see the identifiers.

Further detail on application of the separation principle at AIHW is included in section 48.3.3 of this Framework.

## 13 Metadata and metadata standards

*Metadata* describes and gives information about data.

Metadata provides meaning and context by describing how data are defined, structured and represented. It can also be used to explain how data can be captured and interpreted.

Metadata is necessary for the effective management and use of data.

*Metadata standards* describe the meaning and representation of data within a defined context. Metadata endorsed for use within an organisation or across a range of organisations are referred to as data standards.

Metadata supports:

- efficiency and reliability of data processing and transmission;
- quality of received and stored data;
- interoperability, or the ability of different information systems to link and share data;
- transparency, or clear rules for how and why data will be collected and used;
- compliance with data standards.

A *metadata registry* is a system which enables the creation, management and dissemination of metadata. AIHW manages [METeOR](#), Australia's registry of national data standards for health, community services and housing assistance. See section 41 for further information about METeOR.

## 14 Data policies, guidelines and procedures

**Data policies** are high-level statements that provide agreed rules for strategic decisions relating to data in an organisation that are consistent with external factors such as legislation and government policy. Policies form the structure of data governance and shape standards, guidelines and procedures.

Guidelines and procedures are specific instructions designed to ensure policy is followed, roles and responsibilities are clear and outcomes are measurable. They provide guidance on how to respond to an event, and may be specific to a data collection. They improve the repeatability of the data governance process and reduce the risk that knowledge critical to the organisation is not properly recorded or managed.

**Appendix 3** provides an alphabetical hyperlinked inventory of legislation, policies and guidelines related to this Framework, which are each discussed in Part 6 of this Framework.

## 15 Tools

Tools are physical, technology and/or procedural instruments that support people in doing their work. Tools can range from checklists to workflow systems designed to automate approval processes. Use of tools can promote a standardised approach to a particular component of data governance. Tools produce records which can be reviewed to assess



compliance with policy. Part 5 describes key systems and tools that support AIHW data governance.

## PART 3 – LEGAL, REGULATORY AND GOVERNANCE ENVIRONMENT

The AIHW's internal data governance is informed by, and designed to ensure compliance with, its external legal, regulatory and governance environment while achieving its purpose to create authoritative and accessible information and statistics that inform decisions and improve the health and welfare of all Australians.

This Part describes the key features of that environment.

### 16 The AIHW Act – our establishing legislation

The AIHW is a Commonwealth statutory authority. Its enabling legislation is the [Australian Institute of Health and Welfare Act 1987](#) (AIHW Act). The AIHW Act establishes the AIHW's functions, powers and its governance structures, including the AIHW Board, Chief Executive Officer and AIHW Ethics Committee.

The main functions of the AIHW, described in section 5 of the AIHW Act, are to collect, analyse and disseminate health- and welfare-related information and statistics.

Section 29 of the AIHW Act establishes strict confidentiality requirements which prohibit the release of documents and/or 'information concerning a person' held by the AIHW unless one of the specific exceptions applies. The exceptions include release of data:

- where express written permission has been provided by the relevant data supplier(s);
- where release has been approved by the AIHW Ethics Committee; and
- in the form of publications containing de-identified statistics, information and conclusions.

A 'person' is defined broadly in the AIHW Act to include a body or association of persons, as well as a body politic and a deceased person.

The confidentiality provisions of the AIHW Act protect both the suppliers of data to the AIHW and subjects of that data.

The Act recognises that the AIHW's many data suppliers may attach such conditions to the use of their data as they deem appropriate, and the latter exceptions listed above are expressly subject to compliance with any written terms and conditions imposed by data suppliers.

The AIHW Ethics Committee can authorise the release of information protected by section 29(1) of the AIHW Act, where the wishes of the data supplier are not clear, provided doing so is not contrary to the written terms and conditions (if any) upon which the information was provided to the Institute.

The AIHW Act therefore facilitates the release of information designed to ultimately benefit the public, protects the identity of individuals, and ensures data suppliers may have confidence in the AIHW's adherence to data supply terms and conditions. It also directly establishes, or provides for the establishment of, numerous AIHW structures and roles in data governance, which are described in Part 4 of the Framework.

## 17 AIHW Ethics Committee Regulations

Section 16 of the AIHW Act prescribes the establishment of an AIHW Ethics Committee. The [Australian Institute of Health and Welfare \(Ethics Committee\) Regulations 2018](#) establish the functions and composition of the Committee.

The Ethics Committee oversees the AIHWs activities from an ethical and privacy perspective. The role of the Committee is described in more detail in section 26 of this Framework.

## 18 Privacy Act

The [Privacy Act 1988](#) (Privacy Act) establishes obligations on private and public sector organisations for collecting, using or disclosing personal information: information about living individuals.

The Privacy Act promotes and protects the privacy of living individuals.

As the AIHW is subject to the Privacy Act, in addition to the AIHW Act, it is bound by two sets of requirements: privacy requirements of the Privacy Act, and confidentiality requirements of section 29 of the AIHW Act.

Importantly, both Acts recognise the importance of data being made available for the purposes of research which benefit the community. Subject to certain requirements and considerations, the AIHW Ethics Committee may authorise pursuant to section 95 of the Privacy Act, the collection, use and disclosure of personal information for medical research that would otherwise be a breach of an Australian Privacy Principle in the Privacy Act.

### 18.1 Australian Privacy Principles

The Australian Privacy Principles (APPs) are the cornerstone of the privacy protection framework in the Privacy Act. They replaced the National Privacy Principles and Information Privacy Principles on 12 March 2014.

There are [13 APPs](#) that govern standards, rights and obligations of agencies, including the AIHW, around:

- The collection, use and disclosure of personal information
- AIHW's governance arrangements
- The integrity and correction of personal information
- The rights of individuals to access their personal information.

**Personal information** is defined in the Privacy Act to mean:

'Any information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.'

While the AIHW must apply all 13 APPs, the following most commonly affecting the core work of the Institute.

### **APP 1 – Open and transparent management of personal information**

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date privacy policy.

### **APP 3 – Collection of solicited personal information**

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information.

This APP places strict obligations on the AIHW regarding our receipt of data for collections and research projects that include identifiable data relating to living individuals.

We may only collect personal information if it is reasonably necessary for, or directly related to, one of the AIHW's functions. Sensitive information may only be collected with the individuals' consent or if the collection is authorised by or under an Australian law or a court/tribunal order. Similarly, personal information must be collected only from the individual unless the individual consents to the collection by other means or the AIHW is required or authorised to collect the information by or under an Australian law or a court/tribunal order.

### **APP 6 – Use or disclosure of personal information**

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

For the AIHW to use (analyse) or disclose (share or release) personal information that we hold, either the individual must have consented to us doing so or the use or disclosure is authorised by or under an Australian law or a court/tribunal order.

### **APP 8 – Cross-border disclosure of personal information**

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

### **APP 11 – Security of personal information**

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

An entity has obligations to destroy or de-identify personal information it no longer needs unless the personal information is part of a Commonwealth record or the entity is required by law or court/tribunal order to retain the personal information.

#### **18.1.1 Waivers**

The AIHW Ethics Committee is authorised to grant a waiver pursuant to s.95 or s.95A of the Privacy Act allowing the collection, use or disclosure of personal information for medical research that would otherwise be in breach of an Australian Privacy Principle.

Waivers can only be granted for medical research.

### 18.1.2 Authorised by law exceptions

In certain situations, the AIHW is required or authorised by or under an Australian law or a court/tribunal order to collect, use or disclose information that would otherwise be in breach of an Australian Privacy Principle.

Authorised by law exceptions can include legislation related to specific topics or data collections. For example, the [Cancer Screening Register Act 2016](#) includes provisions that enable AIHW to hold a copy of that register for research, analysis and reporting purposes.

## 18.2 Privacy Code

The [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (the Privacy Code), developed under s. 26G of the Privacy Act and coming into force on 1 July 2018, establishes obligations on Australian government agencies regarding: compliance with Australian Privacy Principle (APP) 1.2; enhancing privacy capability and accountability; promotion of good privacy governance; and building community trust and confidence in agencies' personal information handling practices.

The Code requires agencies to:

- have a privacy management plan, Privacy Officer and Privacy Champion
- conduct a Privacy Impact Assessment (PIA) for all high privacy risk projects, maintain a register of PIAs it conducts, and publish the register or a version of the register on its website
- provide appropriate privacy education or training annually to all staff who have access to personal information and in any staff induction program it provides
- undertake regular reviews of internal privacy processes.

The roles of the Privacy Officer and Privacy Champion are discussed in more detail in section 36 of this Framework.

## 18.3 Notifiable Data Breaches scheme

The [Privacy Amendment \(Notifiable Data Breaches\) Act 2017](#) established the Notifiable Data Breaches (NDB) scheme in Australia, coming into effect in February 2018. The relevant requirements are now contained in Part IIIC of the Privacy Act. The NDB scheme requires entities to notify individuals and the Australian Information Commissioner (AIC) of 'eligible data breaches'. AIHW processes to deal with suspected and actual breaches are discussed in section 49 of this Framework.

## 19 National Health and Medical Research Council Guidelines

[Australian Institute of Health and Welfare \(Ethics Committee\) Regulations 2018](#) state in s.6(2) 'The Ethics Committee, in performing the functions ... must have regard to any relevant ethical principles and standards formulated or adopted by the [National Health and Medical Research Council](#) (NHMRC)'. The regulations also confer on the Committee 'the functions of a Human Research Ethics Committee under guidelines in force from time to time under section 95 or 95A of the Privacy Act 1998'.

The [NHMRC National Statement on Ethical Conduct in Human Research \(2007\) - Updated 2018](#) (National Statement) promotes ethically good human research, clarifies the responsibilities of institutions and researchers, and ‘sets national standards for use by any individual, institution or organisation conducting human research. This includes human research undertaken by governments, industry, private individuals, organisations and networks of organisations’. Research is not defined in the National Statement but ‘is widely understood to include at least investigation undertaken to gain knowledge and understanding or to train researchers’ (page 6). ‘Human research is conducted with or about people, or their data or tissue’ (page 7). The National Statement must be used to inform design, ethical review and conduct of human research that is funded by, or takes place under the auspices of the NHMRC, the Australia Research Council or Universities Australia. The NHMRC [Australian Code for the Responsible Conduct of Research, 2018](#) (the 2018 Code) establishes a framework for responsible research conduct that provides a foundation for high-quality research, credibility and community trust in the research endeavour.

The Ethics Committee and the AIHW are both required, therefore, to have regard to ethical principles and standards including the National Statement and the 2018 Code in all human research activities.

The National Statement provides guidance on the ethical considerations that are relevant to the way human research is designed, reviewed and conducted. Element 4 of Chapter 3.1 of the National Statement specifically addresses aspects of privacy detailing the ethical issues related to generation, collection, access, use, analysis, disclosure, storage, retention, disposal, sharing and re-use of data and information. There is significant overlap between these aspects of ethical consideration and the core requirements of the Australian Privacy Principles.

Further information regarding the AIHW Ethics Committee can be found in section 26 of this Framework.

## 20 Freedom of information

All documents held by the AIHW are potentially subject to access by members of the public under the [Freedom of Information Act 1982](#) (FOI Act). This includes all data at AIHW, whether held in paper-based or electronic form, unless one or more exemptions apply.

Data protected by the confidentiality provisions of section 29 of the AIHW Act are protected from release by section 32 of the FOI Act, unless the information requested is about the individual who made the FOI request.

Further details about AIHW’s FOI responsibilities and AIHW holdings of identifiable data that are potentially subject to release under the Act may be found on the [FOI page](#) of the AIHW website.

Compliance with [FOI Act requirements](#) is overseen by the Office of the Australian Information Commissioner.

Requests for data and information from the AIHW under the FOI Act should be referred to the AIHW Freedom of Information Officer at [foi@aihw.gov.au](mailto:foi@aihw.gov.au). Decisions on whether AIHW data can be released under the FOI Act in response to an FOI request can only be made by the FOI Officer.

## 21 Protective Security Policy Framework and Information Security Manual

The [Australian Government Protective Security Policy Framework \(PSPF\)](#) was developed to assist Australian Government entities to protect their people, information and assets, at home and overseas. The PSPF articulates government protective security policy. It also provides guidance to entities to support the effective implementation of the policy across the areas of security governance, personnel security, physical security and information security.

The Australian Cyber Security Centre within the Australian Signals Directorate produces the [Australian Government Information Security Manual \(ISM\)](#). The purpose of the ISM is to outline a cyber-security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.

The AIHW ICT Framework, approved by the CEO in May 2019, states that 'AIHW endorses the PSPF and the ISM as a requirement for the secure management and protection of AIHW data and assets.'

Compliance with the PSPF and ISM assists the AIHW in meeting its privacy obligations as specified in APP11 – Security of Personal Information– and can satisfy data suppliers, including those in the private sector, that our practices conform with or exceed industry standards.

Many contracts, MOUs and data sharing agreements that the AIHW enters into to obtain data and information, or to provide data analytical services, especially if made with other Commonwealth government agencies, will typically require the AIHW to be fully compliant with the PSPF and ISM in relation to how data and information is securely handled.

## 22 Other Commonwealth Legislation

The AIHW is subject to a wide range of Commonwealth legislation.

In some instances, there is specific legislation that directly affects the management of some AIHW data collections. For example, the Health Insurance Act governs use of Medical Benefits Scheme (MBS) data, and the National Health Act governs the use of Pharmaceutical Benefits Scheme (PBS) data. Guidance should be sought from the EPLU as to how specific legislative requirements could affect the management of individual data collections and information.

As noted in section 18.1.2 of this Framework, some legislation provides authorised by law exceptions to provisions of the Privacy Act.

## 23 State and Territory Legislation

The AIHW enters into agreements with researchers and data suppliers in each of the Australian States and Territories. Researchers and data suppliers are subject to the legislation and regulations of their respective jurisdictions, the requirements of which often differ to those of the Commonwealth. These agreements must recognise and reflect those requirements.

For example, State and Territory data suppliers must comply with their jurisdiction's privacy and other legislation, which can directly affect the provision of identified data to the AIHW. Guidance should be sought from the EPLU as to how whether specific State and / or

Territory legislative requirements could affect the management of individual data collections and information.

## **24 Contracts, Agreements and Memoranda of Understanding (MOUs)**

Section 4 of the [\*Australian Institute of Health and Welfare Act 1987\*](#) established the AIHW the AIHW as a body corporate, with its own common seal that may sue and be sued in its corporate name. Section 6(a) of the AIHW Act gives the AIHW the power to enter into contracts or arrangements in connection with performance of its functions.

The AIHW can enter into legally binding contracts for data and information sharing with other government agencies and external entities. Subject to the needs of the parties, the AIHW also has the option of entering into non-legally binding arrangements, such as Memoranda of Understanding, Data and Information Sharing Agreements and other intergovernmental agreements. These agreements make clear the expectations, obligations and considerations that have been agreed by the parties, including any data licensing arrangements which can impact on current and future use of the data.

Information on some contracts and memoranda/memorandums of understanding (MOUs) can be found on the Agreements and MOUs page of Bruce. Further guidance can be obtained from EPLU.



## PART 4 – AIHW STRUCTURES AND ROLES IN DATA GOVERNANCE

This Part describes the various AIHW organisational structures and roles that give effect to the AIHW data governance system of decision making and accountabilities for information-related processes.

### 25 AIHW Board

Governance of the AIHW is vested in a Board established under section 8 of the AIHW Act, and subject to the general oversight of the Minister for Health. Membership of the Board is prescribed by section 9 of the AIHW Act.

The Board is the accountable authority of the Institute under the [Public Governance, Performance and Accountability Act 2013](#) (PGPA Act). The Board determines the AIHW's vision, purpose and values, sets the overall policy and strategic direction of the AIHW.

#### 25.1 Charter of Corporate Governance

AIHW corporate governance arrangements are described in the Charter of Corporate Governance which is approved, and updated on a regular basis, by the AIHW Board. The Charter describes in detail the respective roles of the Board, Board Committees and the CEO.

### 26 AIHW Ethics Committee

The AIHW Ethics Committee (the Committee) plays a central role in AIHW's data governance arrangements. The functions and responsibilities of the Committee are described in the AIHW Act and the [Australian Institute of Health and Welfare \(Ethics Committee\) Regulations 2018](#) and the principles and standards established by the [National Health and Medical Research Council](#) (NHMRC) such as the [Australian Code for the Responsible Conduct of Research, 2018](#).

#### 26.1 Committee Functions

The Committee is established under section 16(1) of the AIHW Act. The membership composition and functions of the Committee are prescribed in the [Australian Institute of Health and Welfare \(Ethics Committee\) Regulations 2018](#). The key prescribed functions of the Committee, from a data governance perspective, are to:

- to consider ethical matters relating to Institute activities or Institute assisted activities, including advising the Institute on such matters; or imposing conditions, on ethical grounds, on the Institute engaging in activities
- to advise any body or person on ethical matters relating to the collection and production of health or welfare related information and statistics
- its function under paragraph 29(2)(c) of the AIHW Act, that is specifying person(s) to whom 'information concerning a person' may be released, providing this is consistent with written terms and conditions of the relevant data supplier(s). Committee approval is required for release of any data subject to s 29(2)(c) of the AIHW Act, in circumstances where the data supplier has not been specific as to the identity of the individual or entity to which the AIHW can release that data.

- the functions of a Human Research Ethics Committee (HREC) [under guidelines issued by the National Health and Medical Research Council \(NHMRC\) in force from time to time under s. 95 or 95A of the Privacy Act](#). Only the full Committee can grant any s.95 or s.95A Privacy Act waivers authorising the collection, use or release of personal information for medical research that would otherwise be a breach of an Australian Privacy Principle in the Act.

## 26.2 Ethical standards

The Regulations state in s.6(2) 'The Ethics Committee, in performing the functions ... must have regard to any relevant ethical principles and standards formulated or adopted by the National Health and Medical Research Council'.

The [NHMRC National Statement on Ethical Conduct in Human Research \(2007\) - Updated 2018](#) (National Statement) refers to three degrees of risk and relates them to the required level of ethical review.

1. 'Negligible risk research' describes research in which there is no foreseeable risk of harm or discomfort; and any foreseeable risk is no more than inconvenience. 'Institutions may choose to exempt from ethical review research that (a) is negligible risk research (as defined in paragraph 2.1.7); and (b) involves the use of existing collections of data or records that contain only non-identifiable data about human beings (5.1.22).
2. 'Low risk research' describes research in which the only foreseeable risk is one of discomfort. 'For research that carries only low risk ... institutions may choose to establish other levels of ethical review' (5.1.7), including a subcommittee of the Ethics Committee.
3. Research in which the risk for participants is more serious than discomfort is not low risk and must be 'reviewed and approved by an HREC that is constituted and functioning in accordance with this National Statement' (5.1.24).

## 26.3 Privacy Oversight

The AIHW Strategic Risk Profile of June 2019 notes the systemic privacy oversight role of the Committee in mitigating privacy risk: the 'Ethics Committee ... has a role to oversight AIHW activities including data governance and privacy'.

The Privacy Code states that 'An agency must conduct a Privacy Impact Assessment (PIA) for all high privacy risk projects', where the 'project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals' (page 6).

A PIA is a systematic assessment of an activity that identifies the impact that the activity might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. A PIA addresses all Australian Privacy Principles (APPs).

The Ethics Committee reviews applications for all new or amended data collections, for all projects that require use of identifiable data and projects requiring data linkage. The Committee actively considers potential impact and mitigation strategies for all applicable

APPs for every project and collection application it reviews. This approach meets the requirements of a PIA.

The Ethics Committee also reviews specific proposals for activities that involve new or changed ways of handling personal information, for example development of new data access environments. The AIHW Privacy Officer recommends to the Deputy CEO, as chair of the Data Governance Committee, whether a PIA is required for non-research activities of the Institute.

## 26.4 Approval of Institute Activities

In consideration of its functions, the Privacy Code requirements and the guidelines provided in the National Statement, the Ethics Committee determined in December 2019 that the full Committee, or a subset of the Committee, must approve all AIHW work involving any of the following:

- creation of new data collections and/or the acquisition of data collections from data suppliers
- changing the nature or expanding the scope of existing data collections
- projects requiring the use of identifiable data (including ‘personal information’ under the Privacy Act and/or ‘information concerning a person’ under the AIHW Act)
- project proposals requiring a waiver under s.95 or s.95A of the Privacy Act
- project proposals relating to specific categories of participants, as specified in the NHMRC National Statement, including Aboriginal and Torres Strait Islander Peoples
- proposals associated with My Health Record data
- proposals involving any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals, and therefore require a formal Privacy Impact Assessment
- proposals referred to it by the AIHW Chief Executive Officer for consideration.

The Committee has also determined that new projects that do not meet the above criteria may be exempt from ethical review if one or more of the following apply:

- There is no foreseeable risk of harm or discomfort to participants, their families or groups to which they belong. Any foreseeable risk is no more than inconvenience – e.g. filling in a form or giving up time for an interview.
- The proposal involves the use of existing collections of data that contain only non-identifiable data.

The Secretary to the Ethics Committee can approve project amendment requests for extensions of time and/or changes in researchers, provided:

- the extension period for the project work is no more than 12 months
- the extension period for project completion including data retention is no more than two years
- new researchers, including the Principal Investigator, are from within the approved institution.

In summary, the use and release of any data held by AIHW for internal (i.e. AIHW) projects or external projects must be approved by the Ethics Committee in compliance with the terms of the Privacy Act and section 29 of the AIHW Act.

The AIHW Ethics Committee does not necessarily approve every instance of data sharing or release. In many cases, the project or collection approval states conditions under which sharing and release of the data may take place without further Committee consideration. In these cases, authority to share and release data has been delegated by the CEO to the relevant Group Head. In other cases, the Ethics Committee has determined that it is to approve sharing or releasing data from specific collections, for example Medical Benefits Schedule, Pharmaceutical Benefits Scheme and Cancer Registry unit record data can only be shared or released with the express approval of the Committee.

#### *26.4.1 Research with Aboriginal and Torres Strait Islander Peoples*

The NHMRC National Statement notes specific requirements with regard to ethical research with Aboriginal and Torres Strait Islander Peoples. The AIHW Ethics Committee is required to apply the [Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities: Guidelines for researchers and stakeholders](#) (2018) as the basis for assessing proposals for health research with Aboriginal and Torres Strait Islander participation. These guidelines are based on six core values: spirit and integrity; cultural continuity; equity; reciprocity; respect; and, responsibility. The AIHW and ABS have produced a set of [National Best Practice Guidelines for data linkage activities relating to Aboriginal and Torres Strait Islander people](#).

Further information about the AIHW Ethics Committee process, including Committee members, meeting dates, and detailed criteria for determining which AIHW activities require ethical review may be found at < [www.aihw.gov.au/ethics/](http://www.aihw.gov.au/ethics/) >.

## **27 Risk, Audit and Finance Committee**

Section 16(4) of the AIHW Act provides that the Institute (that is, the Board) may appoint such committees as it sees fit to assist it in performing its functions.

The AIHW Risk, Audit and Finance Committee is one such committee, comprised of three non-executive members of the AIHW Board and one independent member. The Committee provides advice and assurance to the AIHW Board, independent of AIHW management, on the integrity of the AIHW's financial reporting and its systems of risk management and internal control. It authorises and oversees the AIHW's audit program and reports to the Board on strategic, financial and data risks and audit matters including fraud control, security and the results of audits of data collections conducted for the AIHW Ethics Committee in accordance with the AIHW data collection management principles endorsed by the AIHW Ethics Committee (also at **Appendix 2**).

## **28 All staff and contractors**

All AIHW staff, and any contractors with potential exposure or access to AIHW data, share responsibility for maintaining the security of AIHW data holdings. Upon commencement, staff and contractors sign an undertaking of confidentiality that acknowledges their legal obligations in this regard. Sanctions are outlined in section 50 of this framework.

All staff and contractors complete mandatory privacy and security training upon commencement, then annually.

The AIHW Recruitment and Selection Policy and Procedures state that ‘As a condition of employment at the AIHW all new employees (including contract staff) engaged for more than six weeks must complete a National Police Check.’

## 29 AIHW Chief Executive Officer

Section 17A of the AIHW Act provides the AIHW CEO with the power to manage the affairs of the Institute, subject to the directions of, and in accordance, with policies determined by the Board.

In relation to data governance, the CEO’s responsibilities (as outlined in the Charter of Corporate Governance) include, amongst other things:

- providing leadership in policy and statistical issues across the scope of the AIHW’s functions
- managing the affairs of the Institute in accordance with the AIHW Act and the [Public Governance, Performance and Accountability Act 2013](#)
- identifying emerging strategic, operational and financial risks to the AIHW, in the context of the *Risk Management Framework* approved by the Board, and actively implementing strategies to mitigate those risks
- ensuring the security of data provided to and held by the AIHW, and ensuring appropriate confidentiality and privacy arrangements are in place as required by relevant statutory, regulatory and best practice requirements.

The CEO’s powers in relation to a range of data governance responsibilities, have been delegated to data custodians by the *AIHW Data Custodianship Delegations*.

Similarly, the CEO’s powers in relation to sharing and release of data have been delegated to Group Heads by the [Instrument of delegation for sharing and release of AIHW data and release of AIHW products](#).

More information on the operation and exercise of delegations within the Institute is set out in the Delegations page of the intranet.

## 30 AIHW Deputy Chief Executive Officer

As chair of the Data Governance and Statistical Leadership Committees, the Deputy Chief Executive Officer (Deputy CEO), plays a key role in providing leadership to, and management oversight of, the data governance arrangements of the Institute.

## 31 AIHW Governance Committees

Within the AIHW, many committees operate to assist the CEO in leading and managing the Institute. Those related to data governance are described below.

### 31.1 Executive Committee

The [Executive Committee](#) (ExCo), which comprises the CEO, Deputy CEO and AIHW Group Heads, supports the CEO in managing the day-to-day affairs of AIHW. Other than those endorsed by the AIHW Board, responsibility for approving policies and procedures rests with the CEO, who considers advice provided by ExCo.

### 31.2 Data Governance Committee

AIHW's Data Governance Committee (DGC) was established in 2014. The DGC:

- provides oversight for review of all data-related legal instruments and policies, including the:
  - *AIHW data custodianship delegations*
  - *Instrument of delegation for sharing and release of AIHW data and release of AIHW products*
  - *Data collection monitoring report and checklist*
  - *AIHW Data Governance Framework, and*
  - *Guidelines for the custody of AIHW data*
- examines proposed new or changed data-related principles or approaches to data governance
- sponsors the data custodian forum as a vehicle for professional development and consultation
- considers and provides advice and recommendations to ExCo on data-governance related project proposals put forward by the Data Governance Group (DGG) and others requiring cross-Institute collaboration or resourcing.

The DGC meets four times each year and membership comprises a blend of Group Heads and Unit Heads with specialist expertise, as stated in the DGC Terms of Reference. The Chair of the DGC is the Deputy CEO.

### 31.3 ICT Strategic Committee

The ICT Strategic Committee (ICTSC), on behalf of ExCo, directs the operation and development of the Institute's ICT capability and steers implementation of the AIHW ICT Strategic Plan. The ICTSC has an overview of all ICT activities, including business as usual ICT and of ICT decisions stemming from any AIHW Project.

The ICTSC is accountable to ExCo and works alongside the DGC. Membership of the ICTSC includes at least one member who is also a member of the DGC. The ICTSC is chaired by the CEO.

### 31.4 AIHW Security Committee

The Security Committee provides ExCo and the CEO with assurance that security risks to the Institute are being identified and managed effectively in compliance with the requirements of relevant legislation and the Institute's internal policies. The Committee drives organisational commitment to effective information (including data), personnel and protective security. The Security Committee approves the AIHW Security Plan. The Security Committee is chaired by the Group Head, Business and Communications Group.

### 31.5 Statistical Leadership Committee

The Statistical Leadership Committee (SLC) provides leadership on statistical matters, develops and actions statistical priorities and provides advice to the CEO to assist in the

management of and investment in the statistical operations of the Institute. The Committee's Chair is the Deputy CEO of the Institute.

## 32 Group Heads

Each of the AIHW's Group Heads is responsible for ensuring compliance with data security and confidentiality requirements for collections managed by their Group. They are also responsible for ensuring that data custodians within their Group are appropriately skilled and have been advised of their responsibilities and all relevant governance instruments affecting their duties.

The *Instrument of delegation for sharing and release of AIHW data and release of AIHW products* issued by the CEO authorises those AIHW SES officers who occupy a designated Group Head role to approve the sharing and release of AIHW data and the publication of AIHW products. This delegation encompasses:

1. making data publicly available (data release) and making data available to another agency, organisation or person under agreed conditions (data sharing)
2. publication of the results of AIHW work in any form that is labelled, branded or otherwise identifiable as being produced by the AIHW, to the public. Examples include print reports, HTML web reports, web pages, dashboards, newsletters, manuals and dynamic data displays such as SAS VA or Tableau products.

The AIHW Security Plan (2019) states that 'all substantive SES Officers (and their equivalents) are to hold and maintain at least a BASELINE security clearance level.'

## 33 Data Custodians

An AIHW data custodian is a staff member with delegation from the AIHW CEO (AIHW Data Custodianship Delegation) to exercise overall responsibility for a specified data collection, in accordance with policies, guidelines and any specific conditions for use applicable to that data collection. In recognition of the importance of this function, data custodians are Unit Head (EL 2) or Senior Executive Service staff with roles aligned to the subject matter of the data collection.

Group Heads are responsible for advising the Head, Ethics Privacy and Legal Unit (EPLU) when data custodianship is to be transferred to a new delegate. EPLU ensures changes are reflected in the data catalogue.

Data custodians manage collections in accordance with the AIHW Data collection management principles at **Appendix 2**.

The *Guidelines for the custody of AIHW data* are a key source of information on the role of data custodians. The Guidelines are supported by a range of data-related policies and guidelines identified throughout this Framework. The data custodian for each collection is listed in the AIHW Data Catalogue. Data custodianship of Multi-sourced Enduring Linked Data Assets (MELDAs) is discussed in section 48.4.8 of this Framework.

An agency that collects or generates data for any purpose, and is accountable and responsible for the governance of that data, can be known as the data custodian for that data. The AIHW frequently compiles data from state and territory data suppliers into AIHW data collections, for the purposes of producing national statistics and /or supporting research, however, the jurisdictions retain ownership of these data at all times. Researcher access to these data may require approvals from each of the jurisdictional data custodians.



Where collections are undergoing a transfer of custodianship, the departing and newly appointed data custodians will discuss the details of the collections as detailed in the checklist for changes in data custodianship. As noted in the checklist, the newly appointed data custodian is required to update the list of databases and schemas' in the data catalogue, advise the Ethics Secretariat of changes in collection and project responsibilities, and advise the ICT Service desk of the change in order for the Data on Request System to be updated.

### 34 Authors of AIHW publications and on-line releases

From a data governance perspective, authors of AIHW publications and on-line releases are responsible for, among other things:

- obtaining approval from the relevant data custodian(s) for the use of data in the publications and on-line releases, as outlined in the AIHW info sheet Data custodian clearance of data in reports
- ensuring that the relevant data quality statement is included with all releases, in accordance with the Data Quality Statements (DQS) policy and guidelines.

### 35 AIHW's Data Integration Services Centre

The AIHW's Data Integration Services Centre (DISC) integrates datasets for research purposes. The DISC can link datasets held at AIHW, and can arrange to receive datasets from external data custodians which can be linked to datasets held at AIHW.

The DISC also offers help and advice with project design, and negotiating access to relevant datasets.

If a project requires the integration of Australian Government data, the linkage must be undertaken by an Integrating Authority. The AIHW is an accredited [Integrating Authority](#). This means we have met stringent criteria covering project governance, capability and data management. The AIHW abides by the [principles](#) for data integration involving Australian Government data for statistical and research purposes, and the [best practice guidelines](#).

When linking data, the AIHW uses a separate computer network which is not connected to the internet or any other AIHW system. This is called the secure Data Integration Services Centre (DISC) linkage environment.

The *AIHW Recruitment and Selection Policy and Procedures* state that 'employees or contract staff that have not completed a National Police Check cannot be employed in the Data Integration Services Unit under any circumstances.'

The *AIHW Security Plan (2019)* states that 'all substantive members of the Data Linkage Units are to hold and maintain at least a BASELINE security clearance level.'

### 36 Privacy roles

[The Privacy \(Australian Government Agencies - Governance\) APP Code 2017](#) (the Code) commenced on 1 July 2018. The Code seeks to enhance existing privacy capability within agencies and prescribes the key roles of Privacy Officer and Privacy Champion.



### 36.1 Privacy Champion

The Privacy Code requires agencies to have a designated Privacy Champion. The role of Privacy Champion at the AIHW is performed by the Senior Executive, Data Governance Group.

The functions of the Privacy Champion are to:

- promote a culture of privacy that values and protects personal information
- provide leadership on broader strategic privacy issues
- review and/or approve the AIHW Privacy Management Plan (PMP) and documented reviews of AIHW's progress against the PMP, and
- provide regular reports to ExCo, including about any privacy issues arising from AIHW's handling of personal information.

### 36.2 Privacy Officer

The AIHW's Privacy Officer is the first point of contact for advice to staff on privacy matters. The role is performed by the Head, Ethics, Privacy and Legal Unit and involves:

- participating in the development of new initiatives that have a potential privacy impact
- providing advice on the general application of the *Privacy Act 1988* (Privacy Act) to new initiatives or to general operations
- handling, or supervising the handling, of privacy complaints and enquiries
- training staff in aspects of the Privacy Act that apply to their day-to-day activities
- being the primary privacy contact for the Office of the Australian Information Commissioner (OAIC)
- maintaining a register of privacy incidents reported to the AIHW data and privacy breach response team in accordance with AIHW Data and privacy breach response plan.

## 37 Security Roles

The AIHW Security Plan prescribes the following security roles, in accordance with the Australian Government [Protective Security Policy Framework](#) (PSPF) and the [Australian Government Information Security Manual](#) (ISM):

- **Chief Security Officer (CSO)** - a member of the Senior Executive Service, responsible for directing all areas of security to protect the entity's people, information (including ICT) and assets. Performed by the Head of the Business and Communications Group.
- **Chief Information Security Officer (CISO)** - responsible for:
  - providing cyber security leadership and guidance,
  - overseeing the cyber security program, coordinating cyber security,
  - reporting on cyber security, overseeing incident response activities,
  - contributing to business continuity and disaster recovery planning,
  - developing a cyber security communications strategy,

- working with suppliers and service providers,
- managing a dedicated cyber security budget,
- overseeing cyber security personnel, and
- overseeing cyber security awareness raising.

Performed by Head, Information Communications and Technology Group.

- **Information Technology Security Adviser (ITSA)** – responsible for managing and implementing security measures, responding to cyber threats, incorporating security measures into the development of ICT projects, delivering information security awareness and training, and the first point of contact on these issues within the agency and for external agencies. Performed by Team Lead, Security Team, Operations and Security Unit, ICT Group .
- **Agency Security Adviser (ASA)** - responsible ensuring a safe and secure physical environment and for identifying and managing physical security risks. Performed by the Unit Head, People and Facilities.
- **Personnel Security Advisor** – responsible for managing personnel security matters. Performed by the Unit Head, People and Facilities.

The Privacy Officer role is also listed as a designated security role in the security plan.

## 38 Training Roles

The *AIHW Learning and Development Strategy 2017-2021* defines how the AIHW approaches its learning and development needs. The strategy notes the following roles and responsibilities.

- **Senior Executive** are responsible for providing strategic direction for L&D activities across the Institute and ensuring that appropriate people and financial resources are allocated.
- **The Learning and Development Advisory Committee (LDAC)** provides strategic direction for learning and development activities across the Institute reporting to the Executive through its Chair, the Senior Executive, Business and Governance Group.
- **Statistical and Analytical Advisory Committee (SAMAC)** provides advice to LDAC in statistical and analytical learning and development needs.
- **Groups** are responsible for the design, delivery and evaluation of internal seminars and programs.
- **The People and Facilities Unit (PFU)**, Business and Communications Group is responsible for providing specialist advice on L&D to the Senior Executive, SAMAC and LDAC. PFU is responsible for the development, delivery and evaluation of the L&D strategy and funding corporate L&D activities.
- **Unit Heads** are responsible for ensuring that staff possess the knowledge and skills required to meet their Units' work programs and each Unit's budget has a learning component.
- **Managers/Supervisors** are responsible for providing formal and informal learning and development opportunities to staff. They are responsible for supporting individuals to apply newly developed skills in the workplace, and for providing timely and appropriate feedback on job performance.

- **Individual staff members** are responsible for identifying and communicating their learning and development needs to their manager.

In relation to Data Governance, specific roles have already been noted in this Framework.

- **Group Heads** are responsible for ensuring that data custodians within their Group are appropriately skilled and have been advised of their responsibilities and all relevant governance instruments affecting their duties (section 32)
- The **Privacy Officer** is responsible for training staff in aspects of the Privacy Act that apply to their day-to-day activities (section 36.2)
- The **Information Technology Security Advisor** is responsible for delivering information security awareness and training (section 37)

[Learnhub](#) is the AIHWs learning management system (LMS) and is utilised to schedule face-to-face courses and online learning modules. All staff (including contractors) are required to complete a selection of mandatory training modules that include Privacy Awareness and Security Awareness.

Selected privacy presentations are freely available to all staff on the Data Governance page on the intranet.

## **PART 5 –SYSTEMS AND TOOLS TO SUPPORT DATA GOVERNANCE**

### **39 AIHW ICT Framework**

The AIHW ICT Framework outlines how all aspects of digital technologies, referred to as ICT, are developed, accredited, sustained and governed in the AIHW.

Under the ICT Framework, each ICT system, product or service has a System Owner, which is generally the CITO, who has responsibilities defined in the ISM related to the registration, operation and monitoring of that system, product or service.

All ICT products and services are subject to a Security Risk Assessment (SRA) against the PSPF and ISM at the OFFICIAL level. The SRA includes consideration of the business case for the product; detailed technical design; the operational business processes; the product support plan; and any legal aspects including contracts. The SRA generates a Security Risk Management Plan (SRMP) that outlines how the identified risks will be treated and/or accepted.

Before a system is authorised to operate, the CEO or delegate must formally accept the security risks associated with its operation as described in the security assessment. This is formally recorded by the CEO signing an Authority to Operate (ATO). If the ATO is rejected, it cannot be resubmitted until the risks outlined in the ATO are mitigated to the satisfaction of the CEO.

### **40 AIHW data catalogue**

The AIHW Data Catalogue (DCat) is the official listing of AIHW's data collections. The Data Catalogue performs two key functions:

- Identify data custodians for each AIHW data collection. Data custodians listed in the data catalogue are, by virtue of the CEO's AIHW Data Custodianship Delegations, vested with the data custodianship responsibilities listed in the Guidelines for the custody of AIHW data; and
- Describe each AIHW data collection, including its scope, format, period of coverage, sub-collections, availability for research, links to relevant publications, whether the collection contains identifiable data, and identifies related datasets in METeOR.

The DCat also contains 'pointers' to other data holdings or groups of holdings that do not comprise data collections to which AIHW data governance controls for data collections are applied. This is generally because other controls or protocols are applied, for example:

- the outputs of data linkage for projects approved by the Ethics Committee which are registered and managed in the DISC
- data are supplied to the AIHW (by the ABS for example) and the AIHW is subject to an Undertaking regarding management and use of these data
- use of these data requires specialist expertise to ensure consistency of application across the AIHW.

A [public listing](#) of the data collections (not pointers) in the Data Catalogue is available on AIHW's website. The Guidelines for the custody of AIHW data detail criteria for exempting collections from public listing.

## 41 METeOR

AIHW's Metadata Online Registry, [METeOR](#), is Australia's repository for national metadata standards for health, housing and community services. METeOR operates as a metadata registry, which is a system or application where metadata are stored, managed and disseminated. The registry aspects of METeOR are based on the international standard for metadata registries, ISO/IEC 11179.

METeOR provides online access to a wide range of nationally endorsed data standards, which users can find, view and download. The Metadata & METeOR Unit is also available to assist users with the creation and endorsement of quality metadata and data standards.

## 42 Validata™

[Validata™](#) is an AIHW tool developed specifically for the secure receipt of data and for checking incoming data against a set of validation rules to ensure the quality of incoming data is fit for purpose. Validata™ is used wherever possible.

Scenarios where Validata™ may not be suitable for use, include:

- once-off ad hoc data supply,
- data that changes successively between supply periods, or
- data where the number of files and records is too large to be processed by Validata.

Where Validata™ is not suitable, other methods are used assure data quality.

Once data are securely submitted through Validata™, appropriate databases are updated for use by AIHW staff and others who have been granted access rights. The system results in higher quality data in a faster turnaround time, greatly improving data governance across the AIHW and giving data custodians greater confidence in the data.

## 43 EthOS™

[EthOS™](#) is a web-based application through which researchers may apply to the AIHW Ethics Committee for access to AIHW data and for data linkage purposes. It also supports oversight of the use of AIHW's data collections by external researchers, by maintaining an auditable record of past and current authorisations, and providing prompts for annual reviews to ensure appropriate access, storage and transmission is maintained over multi-year projects.

## 44 Data on Request Application (Ad hoc request system)

[AIHW's data on request](#) service helps staff to respond to requests for data in a consistent, appropriate and timely manner and ensures that the requisite approvals are gathered and recorded. This helps the AIHW make information more available to the people who need it, when they need it.

The request application also helps with request management by monitoring and reporting data request activities. This makes these activities more visible and helps to address overall data needs and resource allocation.

The application manages ad hoc data requests – that is, requests for unpublished analysis that are not covered by a specific funding agreement. They include requests from members of the public, researchers, students etc. as well as requests for data from government bodies that do not have an existing project or arrangement with the AIHW.

The system is not used for:

- Established, ongoing data provision cycles – such as data provided to the Productivity Commission for ROGS and National Agreement reporting – are managed through existing arrangements.
- Requests that require Ethics Committee approval (e.g. those involving data linkage) are submitted through EthOS, AIHW's Ethics Online System.
- Requests between AIHW units, which are handled by direct contact with relevant data custodian and/or through the Data shopfront.

Details are available on the Data request page of the intranet and in the AIHW Data Request application User Guide.

## **45 Institute Projects**

Institute Projects is an AIHW ICT system that supports planning, implementation, monitoring, reporting and document management associated with AIHW projects.

## **46 Secure Messaging and file transfer**

AIHW Secure Messaging (ASM) is used to securely and reliably send emails, data and other files to AIHW clients. It can also be used by the AIHW's clients to securely send email, data or other files to the Institute.

The DISC also downloads data from secure portals of some State linkage units e.g. [SHeReL](#).

## **47 Review and approval (R-A) plan**

The R-A plan is the framework to ensure that all AIHW products undergo appropriate quality assurance processes. The R-A plan helps project managers to think through, plan and document the input, reviews and approvals required, which helps to get the balance right between timeliness, compliance, risk management and creating the best possible product.

The R-A plan also helps with product planning, so everyone understands what needs to be done, by whom and when. This includes the communications units, which have a role in the release of every product, and other specialist areas, which may advise on how your product could be enhanced.

The R-A plan also requires data users to confer with the relevant data custodians regarding use and release of data in their collections. The R-A is approved by the relevant Unit head.

Details are available on the Review and approval (R-A) plan page on the intranet.

## PART 6 – AIHW DATA POLICIES, GUIDELINES AND PROCEDURES

The AIHW's internal data policies, guidelines and procedures are designed to ensure:

- compliance with the legal and regulatory environment described earlier in this Framework,
- adherence to relevant Australian and international standards and classifications, and
- compliance with ethical considerations and obligations under contracts, agreements and external governance arrangements.

These policies, guidelines and procedures ensure that all staff, and especially those with delegated authority to make data-related decisions, have clear sources of information to perform their roles effectively and appropriately.

### 48 Managing the data life-cycle

It is useful to consider relevant AIHW policies, guidelines and procedures in terms of the data lifecycle – collection establishment, data acquisition, data use with AIHW (e.g. access, storage, management), sharing and releasing data outside the AIHW, and 'end' (archiving, destruction, return) – although some documents address issues relevant to a number of these stages.

#### 48.1 Collection establishment

This section describes arrangements for establishing a new data collection.

##### 48.1.1 *Proposals to establish a new collection*

The opportunity to establish a new collection can arise in various ways, the most common of which are as follows.

- The AIHW may receive a request from an external organisation or agency to undertake one or more of the following: manage their data, undertake analysis for them, safely release their data to third party researchers, and enhance their data and return it to them.
- States, Territories and the Commonwealth may determine that a new collection is required, with the AIHW participating in developing the collection proposal and being engaged to manage the new collection.
- The AIHW can identify gaps in the coverage of Australian health- and welfare-related data and seek support for the establishment of a new collection.

When a collection is under consideration, a Group within AIHW that will be responsible for the new data collection is identified, and a Unit Head from that group designated to support development of the proposal. Frequently this Unit Head becomes the data custodian of the new collection.

The Group and Unit Heads work together to negotiate and agree key parameters associated with the proposal, including:

- data flows including: sourcing arrangements, metadata and data quality assurance, where the data will be held, with which entities might require access to analyse the data
- roles and responsibilities of the AIHW, data suppliers and other entities
- enabling legislative, regulatory and legal arrangements
- Memoranda of Understanding and/or contracts, including data supplier requirements regarding the use, sharing and/or release of the data
- internal operating arrangements, and
- an AIHW Ethics Committee application to establish the collection.

The Ethics Privacy and Legal, Financial and Commercial Services, and Data Strategies and other AIHW Units provide specialist support as required.

Not all proposals are successful.

Also, there are occasions where the AIHW can gain access to data it needs without the necessity to create an AIHW data collection. For example, the AIHW has an agreement with the ABS for access to a range of datasets; we have committed to abide by particular terms and conditions of use, but establishment of AIHW data collections is neither necessary nor appropriate.

#### *48.1.2 What constitutes an AIHW data collection?*

In determining whether a set of data are to be classified as an AIHW data collection, the following criteria are used. If one or more of the following criteria apply, the set of data is designated a data collection:

1. the holding includes identified unit record (individual or service-level) data or reasonably identifiable or re-identifiable unit record data
2. the AIHW provides access to the set of data by third parties or uses the data for linkage
3. the AIHW Senior Executive determines that the data should be managed by a data custodian appointed by the CEO via the AIHW Data Custodian Delegation, regardless of whether they contain identified or reasonably re-identifiable data. This includes data holdings which need to be managed by a data custodian in compliance with data supplier requirements or where this is public sensitivity about the data.

Data collections, once approved by the AIHW Ethics Committee, are listed as collections in the AIHW data catalogue – with a record of the responsible data custodian for the collection – and subject to the governance arrangements detailed in the Guidelines for the custody of AIHW data and described in this Framework.

#### *48.1.3 Approval to establish a new collection*

The AIHW Ethics Committee must approve all proposals to create or amend an AIHW data collection. This approval must be sought and granted **before** action is taken to collect data for a new collection or changes made to an existing collection.

Applications to establish or amend an AIHW data collection are submitted to the Ethics Committee through the [Ethics On-line system EthOS™](#). The application form for a new



collection seeks information that enables the Ethics Committee to consider the ethical and privacy implications associated with the collection. Considerations include:

- Proposed duration of the collection – ongoing or finite
- Objectives and intended benefits
- Source of the data, data field and temporal coverage
- Source of funding for the collection
- Proposed use of the data, including whether the data will be made available to external parties and under what conditions
- Any requirements of the data supplier in respect to the data and their use
- Privacy: Identifiability of the data, consent arrangements, any authorised by law exceptions to the Privacy Act, and whether a waiver is sought under section 95 of the Privacy Act
- Whether the collection relates to Aboriginal and Torres Strait Islander People or any specific participant groups listed by the NHMRC.

In approving of the collection, the Ethics Committee can impose conditions on the AIHW's management of the collection. The conditions typically relate to: for what purposes the data may be used; with whom they may be shared and under what arrangements; how privacy and confidentiality considerations are to be managed; and how data supplier requirements are to be honoured. These conditions are binding on the AIHW.

Data custodians are required to report annually to the Ethics Committee and certify that the collection continues to be managed in accordance with the stated Committee conditions.

#### ***48.1.4 Data catalogue entry***

The *Guidelines for the custody of AIHW data* require, amongst other things, the relevant data custodian to record the details of each new or amended data collection in the data catalogue. The type of information that must be recorded in the catalogue is described under the data catalogue entry in section 40 of this Framework and specified in the Data Catalogue Wiki on the intranet.

#### ***48.1.5 Listing collections on the AIHW Web Site***

A listing of AIHW data collections is published on the [AIHW website](#) periodically with two purposes in mind:

1. Promoting researchers access to AIHW data.
2. Enhancing transparency with the community about the data holdings of the AIHW.

All AIHW data collections listed in the data catalogue are to be listed on the AIHW website unless particular criteria are met; these are listed in the *Guidelines for the custody of AIHW data*.

For some collections, researchers' access to the data may be restricted: these collections are identified as such on the website. The criteria for determining which collections have restricting access are also listed in the Guidelines and include: conditions imposed by the AIHW Ethics Committee with respect to use of the collection; agreements with the suppliers of data to the AIHW; practicalities in providing access to older collections; and data quality limitations.

#### 48.1.6 Data Collection Management Principles

The Data Collection Management Principles (DCMPs) make explicit the expectations of Ethics Committee regarding how all AIHW data collections are to be managed. The DCMPs are at **Appendix 2**.

The DCMPs were developed in the 2011 as a basis for internal audits of sensitive AIHW data sets. The DCMPs were revised, updated and approved by ExCo and the Ethics Committee towards the end 2012.

At the request of the Audit and Finance Committee in August 2016, the DGC oversaw the development of a data custodian self-assessment checklist based upon the DCMPs. The checklists were to provide data custodians a tool to self-audit data governance controls for the collections for which they had delegated responsibility, and to provide the AIHW with a snapshot of conformance the DCMPs. Use of the checklists commenced in July 2017 with a requirement that a checklist be completed annually for each data collection listed in the AIHW Data Catalogue.

In August 2019, following a review of implementation of the checklist, the DGC proposed that the self-assessment checklist be merged with the Ethics Committee Collection Monitoring Report, and that the new form be submitted every two years rather than annually for some lower risk collections. This was agreed by the Ethics Committee in December 2019.

The *Data Collection Monitoring Report and Checklist* is used to record progress and compliance for data collections approved by the AIHW Ethics Committee and provides:

- the Ethics Committee assurance that the collection continues to meet the terms and conditions of Committee approval as stated in the Committee's approval letter
- data custodians with additional guidance on the DCMPs against which data collections are audited, and enable them to assess their collections' readiness for audit, and
- the AIHW with a summary snapshot of conformance with the DCMPs to aid in identifying key risks and any systemic issues.

Further details of the DCMPs and the Data Custodian Monitoring Report and Checklist are available on the Data Governance page of Bruce.

#### 48.1.7 Quality Framework

The Quality Framework (QMF) supports staff with a role in the work cycle of directing, managing and processing fit-for-purpose data and developing reports for sharing and publishing. It is being improved during 2020 and 2021 as a framework for continuous improvement with a set of quality management and data quality principle-based guides, processes and quality checklists for the following stages in the work process:

- 1 - Define **SCOPE**
- 2 - **MANAGE** work
- 3 - Collect and **VALIDATE** data
- 4 - **CHECK** output
- 5 - **DISTRIBUTE** output
- 6 - Review and **IMPROVE**

## 48.2 Data acquisition

### 48.2.1 Metadata

In accordance with the AIHW Data Collection Management Principles, data are collected and stored with appropriate metadata and associated with appropriate data dictionaries to accurately define and describe them. The *Guidelines for the custody of AIHW data* assign to data custodians the role of maintaining up-to-date documentation, including Data Catalogue entries, for all data collections for which they have responsibility.

[METeOR](#) is used to store metadata for some AIHW data collections. Metadata for other data collections may not be held in METeOR but are maintained by data custodians and are available on request and/or are stored in the Data Catalogue. Some metadata information is also documented in the data quality statements for each collection.

### 48.2.2 Data validation and data quality

The AIHW's approach to data quality is outlined at a high level in the *ICT Strategic Plan 2020-2023* with the strategy of consolidating and implementing a single source of truth for AIHW data collections, analysis and outputs.

There are three aspects to managing data quality:

- working to maximise the currency and quality of the data;
- ensuring the data are used appropriately given their quality; and
- reporting on data quality.

The AIHW works with its data suppliers to maximise the currency and quality of its data collections.

The AIHW's online data receipt and validation product, Validata™, has been designed to improve the quality and timeliness of data supplied by jurisdictions and non-government organisations. Validata™ has data quality checks (edits) built into the data submission process that notify data suppliers of potential errors in the data. Validata™ is discussed in section 42 of this Framework.

Whether through the use of Validata™, the data ingress checking guide, or by other methods, data custodians are responsible for reviewing data as it is acquired to ensure the data are consistent with the descriptions given in the metadata, the data dictionary and approvals given by the AIHW Ethics Committee.

As set out in the *Guidelines for the custody of AIHW data*, one of the roles of data custodians is to provide advice and assistance to users of the data within the AIHW. Among other things, this advice should include any caveats on the use of the data attributable to data quality considerations.

Statistics for the AIHW, the AIHW's statistical handbook, contains information and guidance relating to determining the quality of data and the appropriate use of statistical and analytical methods based on that determination.

The statistical content of publications may be reviewed as per the AIHW Review and Approval plan. One aspect of the review examines whether the analysis and conclusions are commensurate with the quality of the data used.

The quality of AIHW data collections is recorded and reported by way of Data Quality Statements which are made available to the public via METeOR and/or inclusion in publications. The requirement for, and content of, data quality statements is subject to the Data Quality Statements policy and guidelines.

### **48.2.3 Data storage and security**

The AIHW secures all data it holds. To gain access to data held by the AIHW requires multiple levels of approval. A person is provided with approved access to the level necessary. Access is audited and logged and permissions removed from those who no longer require access.

An overview of ICT-based security, including building access, systems access, virus detection and AIHW secure messaging, is provided on the ICT security page of the intranet.

The AIHW Security Plan aims to protect Institute staff in the course of their duties and protect official information from compromise or unauthorised disclosure and protect official assets from compromise, theft, loss and/or damage.

The Security Plan also identifies specific delegations for security-related roles required by Australian Government protective security policies, which were discussed in section 37 of this Framework.

The *Guidelines for the custody of AIHW data* detail a range of requirements relating to:

- compliance with directions from the AIHW management and directives given by the data suppliers and the Ethics Committee;
- compliance with storage and archiving requirements of the National Archives of Australia;
- data custodians' responsibility for ensuring their data collections are protected from unauthorised access, alteration or loss;
- ICT Units' responsibility for providing and maintaining a safe electronic environment for storage of AIHW data collections;
- manipulation and/or changes to data collections and maintaining appropriate records of changes;
- proper use of IT systems *and* in handling classified information;
- secure storage, printing and photocopying of paper-based information;
- additional requirements and/or prohibitions in relation to recording and managing all identifiable data collections; and
- physical security systems and properly enforced measures to protect both staff and its repositories of personal information.

## **48.3 Data access and use within AIHW**

### **48.3.1 Access to AIHW ICT systems**

AIHW procedures regarding ICT security provide the first level of data access management. These procedures are outlined in the AIHW Security Plan and include use of passwords, access to the computer room, and the requirement for a signed confidentiality undertaking to be lodged before staff are given access to any part of the Institute's computer system.

The AIHW Recruitment and Selection Policy and Procedures state that ‘As a condition of employment at the AIHW all new employees (including contract staff) engaged for more than six weeks must complete a National Police Check. Note that employees or contract staff that have not completed a National Police Check cannot be employed in the Data Integration Services Unit under any circumstances.’

Requirements for access to data under data-sharing agreements are specified in those agreements and are at all times subject to the need to know principle and compliance with legislative obligations. [Information regarding access to data collections](#) held by AIHW is published on the AIHW website.

Data Custodians are responsible for approving access to, and use of, the data collections for which they have delegated authority. This responsibility encompasses internal requests for access, based on work requirements, and external requests for access to data held by AIHW. Access by any external persons to identifiable data held by the AIHW, or for linkage with AIHW-held data, for the purpose of research also requires prior approval by the AIHW Ethics Committee. More [information on applications to the Ethics Committee](#) for access to data is available on the AIHW website.

#### *48.3.2 Access to AIHW Research Only Network*

The AIHW Research Only Network (RON) is a secure environment that was approved by the Ethics Committee on 10 December 2019 to host unit record linked data sets for access by AIHW staff in Canberra and Sydney via the analysts' existing desktop computers.

Effectively, RON is a replica of the DISC Data Laboratory environment except that access can be provided to approved AIHW staff from outside the physical DISC area but still completely within AIHW secure offices and computing environment.

User accounts are unique to individuals, and user access are monitored and reportable. Access and data transfer requests are managed through the AIHW internal Service-desk tool. Transfer of files into and out of the environment are not permitted by researchers, and only the Data Custodians can authorise the transfer of files which is performed by approved AIHW ICT System Administrators. Approved/denied data access and transfer requests are recorded via the AIHW Service-desk tool.

The environment is separate from other AIHW computing environments and accessible via a controlled gateway. It is physically stored in the AIHW Data Centre, on location at the AIHW main office. Staff access a virtual desktop containing tools to perform analysis on the data, and can save and share information with other staff working within the same project. As in the DISC Data Laboratory the desktop environment is locked down, such that staff are not able to access any other networks (including the internet), print documents, or send electronic messages from within the environment.

#### *48.3.3 Application of the separation principle*

The separation principle – a mechanism to protect the identities of individuals and organisations – was introduced in section 12 of this Framework.

Implementation of the separation principle is achieved at the AIHW in two ways:

- **Physical separation** and separate storage of identifying and content information is commonly applied across the AIHW, particularly for highly sensitive collections; the DISC holds and manages an ‘identifier collection’ that contains the identifier information separate from that collection’s content information.

- **Virtual separation** by managed views of the data through application of ICT role-based access control arrangements, whereby, individuals are provided access to different views of the dataset. Individual users are given permission to see only the identifying or the content information, never both.

Within the AIHW's Data Integration Services Centre (DISC) the separation principle is reinforced by role separation, whereby individuals are assigned roles as either linkers or mergers. When linking datasets, the data linkers work exclusively with the identifying data of each dataset to create the linkage keys. The data mergers use these keys to create the combined (linked) content dataset. Linkers never see the content, mergers never see the identifiers, and those who analyse the linked dataset only see the content.

The Separation Principle is applied in accordance with the *AIHW Separation Principle Policy*.

#### 48.3.4 Data linkage

The AIHW is one of seven Integrating Authorities in Australia accredited to integrate Commonwealth data for high-risk research projects.

To secure accreditation, AIHW met, and continues to adhere to, stringent criteria covering project governance, capability, data management, privacy and confidentiality. The AIHW abides by the [National Statistical Service \(NSS\) guide for data integration projects involving Commonwealth data for statistical and research purposes](#). Additionally, the AIHW Act, in particular section 29, facilitates the appropriate release of data safely and securely, and statistical linkage projects performed by AIHW must also be approved by the AIHW Ethics Committee in accordance with guidelines provided under '[Lodging an application to the AIHW Ethics Committee](#)'.

As an accredited Integrating Authority, the AIHW applies best standard linkage protocols. A key aspect of best practice data linkage is the separation principle, a set of data management practices that ensures privacy by the separation of identifying data and content data. The AIHW applies a rigorous management approach to each project to ensure appropriate risk mitigation mechanisms are applied. These mechanisms include an integrated set of principles to mitigate the risk of re-identification of data, including de-identification, confidentialisation, user undertakings and secure data access.

These multi-layered arrangements provide the necessary assurance for data suppliers that their data are being appropriately secured, managed and used.

**The Technical Assessment:** A comprehensive Technical Assessment is agreed between the DISC and the researcher prior to a linkage project application being considered by the Ethics Committee. The purposes of the Technical Assessment are to:

- ensure that data requested for linkage will answer the proposed research questions
- ensure that study aims are achievable using the proposed linkage methodology
- serve as a comprehensive record of the project protocol and data specifications
- successfully obtain AIHW Ethics Committee approval for their project
- where applicable, successfully obtain approval from the Department of Health as data custodian.

**The linkage process:** The AIHW performs data linkage through the Data Integration Services Centre (DISC), a physically secure area within AIHW that can be accessed solely by



authorised, specialist staff. Within the DISC, all data integration projects are conducted on a separate secure network and best practice data protection methods are employed.

Once data have been linked, DISC staff confirm the resulting dataset contains only those variables agreed with the data custodian, and confidentiality protection has been applied as agreed with the data custodian. Researchers can then access the linked data:

- via a remote access computing environment called the Secure Unified Research Environment ([SURE](#)), managed by the Sax Institute
- in Canberra via the AIHW's secure data lab – a locked room within DISC that requires authorised entry, or
- other secure access environment approved by the AIHW Ethics Committee and relevant data custodians, which sometimes includes provision of the data by delivered access to the user's secure environment.

Only DISC staff, the systems manager and approved users can use the secure network and the data lab. Each data lab user is assigned a personal virtual computing environment which is securely managed and supervised. Data can be freely manipulated in this area, producing output in required formats. All output is stored in a temporary work area for the duration of the session. When a researcher is confident that they have produced the required output, the data are again vetted to ensure the data are confidentialised and suitable for release.

The AIHW determines and logs all access rights to the data throughout the process. At the end of the project, and as per the data retention date, AIHW uses recognised software to remove all files relating to a project from hard disk. In line with DISC data retention/backup cycle procedures, data are overwritten on a regular cycle. Data are encrypted as part of the archival process.

The '[data linkage](#)' page of the AIHW website contains more information on data linkage, including:

- contact details for the DISC
- current and past data integration projects; and
- information on how to undertake a data linkage project.

## 48.4 Data sharing and release for use outside the AIHW

### 48.4.1 Data sharing and release

AIHW shares and releases data held in our collections for use by researchers, policy makers and the public.

- Data **sharing** is making data available to another agency, organisation or person under agreed conditions.
- Data **release** is making data publicly available with few or no restrictions on who may access the data and what they may do with it.

#### Data release

Consistent with the AIHW's functions as described in the AIHW Act – to collect, analyse and disseminate health- and welfare-related information and statistics – we regularly release data in the form of publications and on-line releases, which can include detailed supplementary tables and data cubes. Furthermore, the AIHW Public Domain Policy reinforces that

aggregate (non-identifiable) AIHW data are to be released publicly. Subject to limited exceptions, data produced under contract with external agencies are also released publicly.

From a data governance perspective, authors of AIHW publications and on-line releases are responsible for, among other things:

- obtaining approval from the relevant data custodian(s) for the use of data in the publications and on-line releases, as outlined in the AIHW info sheet Data custodian clearance of data in reports.
- ensuring that the relevant data quality statement is included with all releases, in accordance with the Data Quality Statements (DQS) policy and guidelines.

### **Data sharing**

Arrangements to share AIHW data externally are generally agreed either through a MOU, agreement or contract, or in response to direct requests from researchers.

Sharing of data under MOUs, agreements or contracts must be managed in accordance with the terms of these arrangements, which must in turn should have been drafted for consistency with legislation, conditions set by data suppliers and any relevant Ethics Committee approval(s).

Information on the processes associated with data requests received via the data request application or through other means can be found on Bruce: data requests, data request application new release, and *Data request application user guide*. For more information on data access see the data access page on Bruce.

Specific arrangements associated with preparing linked data for sharing were discussed in section 48.3.4 of this Framework.

#### ***48.4.2 Preconditions for data sharing or release***

AIHW data custodians are responsible for making recommendations to their Group Heads about the sharing and release of data held in AIHW data collections for which they are accountable. In exercising this function, data custodians must consider a range of factors. Before recommending that data be shared or released, the data custodian will ensure that all necessary pre-conditions have been met.

The AIHW does not publicly release Statistical Linkage Key (SLK) information, and will only share such information in confidence in exceptional circumstances. Written authorisation of the Deputy CEO, and the recommendation of the Group Head Data Governance Group and Group Head Data Strategies and Integration Group is required for this information to be shared.

### **Data Supplier Requirements**

At the time a collection is established, an agreement is documented between the AIHW and the data supplier. That agreement includes a statement of terms and conditions of supply that can place requirements and constraints on:

- AIHW's use of the data,
- how we may develop and release products derived from the data, and to whom these products may be made available, and
- the conditions under which we on-share their data with third parties.



A decision to share or release data must be in accordance with the terms and conditions of supply of the data collection.

### **Section 29 of the AIHW Act**

Section 29 of the AIHW Act imposes strict confidentiality requirements that prohibit the release of documents and/or 'information concerning a person' held by the AIHW unless one of the following apply:

- express written permission has been provided by the relevant data supplier(s);
- release has been approved by the AIHW Ethics Committee;
- the data are in the form of publications containing de-identified statistics, information and conclusions.

In the absence of express approval of the data supplier(s) or the AIHW Ethics Committee, only de-identified data can be shared or released.

A breach of section 29 of the AIHW Act comprises an offence punishable by fines and/or imprisonment.

### **Privacy Act**

The Privacy Act, which incorporates the Australian Privacy Principles, prohibits sharing or release of personal information unless the individual has consented to us doing so, their release is subject to a waiver pursuant to section 95 of the Privacy Act, or the disclosure is authorised by or under an Australian law or a court/tribunal order. Authorised by law exceptions and waivers are very rare for the sharing or release of personal information, which means that unless consent has been obtained, data to be released or shared must nearly always be de-identified.

### **AIHW Ethics Committee Approval**

The sharing or release of any data held by AIHW must be approved by the Ethics Committee in compliance with the terms of the Privacy Act and section 29 of the AIHW Act. While the Ethics Committee can issue a waiver pursuant to s.95 or s.95A of the Privacy Act for the sharing or release of personal information for medical research, this is more commonly done with respect to receipt and use of such data. Waivers for sharing or release of data are rare.

The Ethics committee, in approving a project or collection, states conditions under which sharing and release of the data may take place. Frequently, the approval will clearly reference the terms and conditions of supply, and the requirements of the AIHW Act and Privacy Act as they apply to that project or collection.

#### ***48.4.3 De-identification***

The AIHW De-identification Policy details the AIHW approach to de-identification for all instances of data sharing and release. The policy replaces the previous AIHW Policy 'Guidelines for AIHW publications and on-line releases.

As noted above, in most cases, sharing or release of data will require that the data are de-identified. It is important to establish whether the data require de-identification due to the need to protect personal information regarding living individuals (covered by the Privacy Act), and/or for information concerning a person, living or dead, or organisations (covered by the AIHW Act).

Following legal advice obtained by the AIHW in 2013, the AIHW applies the same ‘reasonably identifiable’ threshold to determining whether data or information are identifiable under both the Privacy Act and the AIHW Act. A person or organisation will be reasonably re-identifiable where:

- it is technically possible for re-identification to occur (whether from the information itself, or in combination with other information that may be available in the data environment), and
- there is a reasonable likelihood of re-identification occurring.

De-identification is context specific. Whether data can be re-identified will depend on factors such as:

1. the access arrangements for data sharing and release (the setting into which the data are placed)
2. the nature of the data itself and other data available to the data users
3. the terms and conditions of use agreed to by the user, and their skills and incentives to apply them

The AIHW de-identification policy outlines how the Five Safes framework is applied to assess and mitigate the risk of re-identification until it is very low: there is no reasonable likelihood of re-identification occurring.

#### *48.4.4 Approval for data sharing or release*

The Group Head, when exercising their delegated responsibility for data sharing and release, will refer to documentation and evidence prepared by the data custodian that confirms the pre-conditions for sharing or release have been met and that the data have been through a rigorous de-identification and risk assessment process as required. The use of the data release checking guide to ensure these conditions have been met is advised.

When a Group Head approves the sharing of data, he or she imposes certain conditions that usually include a requirement that statistical outputs derived from the data meet specific conditions related to privacy and confidentiality before they are released. A data custodian has the authority to review these outputs against the stated conditions and clear them for publication without the need for further approval by the Group Head.

#### *48.4.5 Access arrangements for data sharing and release*

There are four generic modes of access used by the AIHW for data sharing and releasing, which are:

**Open  
access**



Open access

Data are made publicly available with few or no restrictions on who may access the data and what they may do with it. For example, making data available through a publicly accessible website. The data made available through open access is sometimes called open data.

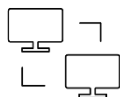
**Delivered access**



Delivered access

Data are made available by direct delivery to the user's custody. The user can be required to agree to specific conditions associated with management and use of the data.

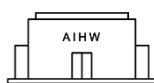
**Secure remote access**



Secure remote access

Data are made available to users via remote access that has a high level of security infrastructure control and where the users' activities can be remotely supervised.

**Secure on-site access**



Secure on-site access

Data are made available to users in a managed physical location that has a high level of security infrastructure control and where the users' activities can be personally supervised.

Data are **released** through open access and **shared** through the other three modes.

**Open Access and Delivered Access**

Identifiable, reasonably identifiable, or otherwise sensitive data is unsuitable for open access release, regardless of the protections offered by the software applications used, for example Tableau.

The default access arrangement for unit record data is via secure mechanisms. Delivered access is also supported, provided the relevant Group Head and Group Head, Data Strategies and Integration Group have approved the confidentialisation approach.

**Secure Remote Access**

For sharing and release of data outside the AIHW, there are currently four secure remote environments available. Each has differing capabilities and constraints, and the choice of the most appropriate secure remote environment will depend on the specific requirements in each case.

**Australian Bureau of Statistics Data Laboratory**

The Australian Bureau of Statistics (ABS) requires that any data linked to ABS unit record data cannot leave the ABS. The ABS Data Laboratory is used, therefore, to provide secure remote access to unit record data that has been linked to ABS data. Furthermore, arrangements with the ABS are such that the ABS Data Laboratory manages data ingress and egress vetting of data on behalf of the data custodian.

**Secure Unified Research Environment (SURE)**

We have had an arrangement with the Sax Institute since 2013 to use the Secure Unified Research Environment (SURE) for researcher access. SURE was developed by the Sax Institute as part of the Population Health Research Network (PHRN) along with the AIHW and state data linkage units. The SURE facility incorporates a range of information security controls relating to the access, storage and transmission of data.

Until recently, SURE was the only secure remote environment through which AIHW could share linked data sets with researchers, and retain full visibility and control over that data.

### **Enterprise Data Warehouse (EDW).**

On 20 February 2018 the Ethics Committee first approved release of linked data into the Department of Health's Enterprise Data Warehouse (EDW). The EDW was built by the Department within its ICT environment to facilitate States and Territories hosting and accessing health data. There are strict eligibility and access conditions that currently prohibit non-government agency use of EDW. Jurisdictions use the EDW, as do AIHW staff.

### **Secure Remote Access Environment (SRAE)**

The AIHW Secure Remote Access Environment (SRAE) was developed by the AIHW and approved by the Ethics Committee on 14 May 2019 'as an alternative to SURE to house AIHW unit record data' to enable researchers to access approved datasets remotely. SRAE provides the same level of security as the Secure Unified Research Environment (SURE), with advanced performance capability and cost flexibility.

The AIHW SRAE is a secure platform for storing and accessing unit record data. The SRAE is configured using the University of New South Wales E-Research Institutional Cloud Architecture (ERICA) platform, which is designed to provide appropriate security for sensitive unit record data. The platform is built on the Amazon Web Services (AWS) secure cloud environment to provide researcher analytics workspaces that are scalable, flexible and cost-effective. AWS is a cloud service accredited by the Australian Signals Directorate for hosting Commonwealth data configured according to the Government's Protective Security Policy Framework. AIHW data is only stored on a facility located in Australia.

Governance and administration arrangements for SRAE are as they are with SURE.

### **Secure On-site Access**

**The DISC Data Laboratory** was developed to provide secure on-site access to sensitive linked datasets at the AIHW offices in Canberra.

The DISC Data Laboratory has similar access and control arrangements to RON (introduced in section 48.3.2 of this Framework), but staff and researchers are restricted to accessing the data in a dedicated, physically secure environment.



Like RON, user accounts are unique to individuals, and user access are monitored and reportable. The environment is separate from other AIHW computing environments and accessible via a controlled gateway. Staff access a virtual desktop containing tools to perform analysis on the data. The desktop environment is locked down, such that staff are not able to access any other networks (including the internet), print documents, or send electronic messages from within the environment.

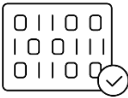


#### **48.4.6 The Five Safes framework**

The Five Safes is an approach to thinking about, assessing and managing risks 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 for data sharing or release.

In November 2018 the AIHW Executive Committee 'agreed that the AIHW use the Five Safes framework to reinforce management of the privacy of data'.

The framework can be used to assess risk across five dimensions associated with a specific data sharing or release proposal. The dimensions and their attendant risks are described below.

Dimension		Meaning	Potential risks to be mitigated
<b>Projects</b>	 <p>Safe projects</p>	<p>Is the use of the data appropriate?</p> <p><i>AIHW Interpretation: Use of the data is legal, ethical and the project is expected to deliver public benefit.</i></p>	<ul style="list-style-type: none"> <li>• Breach of data supplier requirements</li> <li>• Breach of AIHW Ethics Committee collection/project approval conditions</li> <li>• Project is not expected to deliver public benefits commensurate with risk</li> <li>• Project design unlikely to meet stated objectives</li> <li>• Consent arrangements are unlawful</li> <li>• Using AIHW data for this project is outside community expectations.</li> </ul>
<b>People</b>	 <p>Safe people</p>	<p>Can the users be trusted to use it in an appropriate manner?</p> <p><i>AIHW Interpretation: Researchers have the knowledge, skills and incentives to act in accordance with required standards of behaviour.</i></p>	<p>Users of the data:</p> <ul style="list-style-type: none"> <li>• are subject to a conflict of interest</li> <li>• are subject to incentives to breach terms and conditions</li> <li>• are inexpert in the subject matter</li> <li>• have insufficient statistical skills to analyse the data effectively</li> <li>• and/or their organisation are unlikely to be able to manage data breach risks effectively</li> <li>• and/or their organisation have a history of breaching terms and conditions.</li> </ul>

Dimension		Meaning	Potential risks to be mitigated
<b>Data</b>	 <p>Safe data</p>	<p>Is there a disclosure risk in the data itself?</p> <p><i>AIHW Interpretation:</i> Data has been treated appropriately to minimise the potential for identification of individuals or organisations.</p>	<ul style="list-style-type: none"> <li>• Identifiers are not removed</li> <li>• Data include variables not required for the project</li> <li>• Data include records not required for the project</li> <li>• Data treatments are insufficient to prevent disclosure of personal information (Privacy Act)</li> <li>• Data treatments are insufficient to prevent attribute disclosure</li> <li>• Data treatments are insufficient to prevent identification of an information subject (AIHW Act s.29).</li> </ul>
<b>Settings</b>	 <p>Safe settings</p>	<p>Does the access facility prevent unauthorised use?</p> <p><i>AIHW Interpretation:</i> There are practical controls on the way the data is accessed – both from a technology perspective and considering the physical environment.</p>	<p>Data are:</p> <ul style="list-style-type: none"> <li>• lost, intercepted or disclosed during transmission to the setting (data/privacy breach)</li> <li>• subject to unauthorised access at the setting (data/privacy breach)</li> <li>• used for purposes beyond those approved (including linking to other data)</li> <li>• removed from the approved setting</li> <li>• not destroyed on completion of the project.</li> </ul>
<b>Output</b>	 <p>Safe output</p>	<p>Are the statistical results non-disclosive?</p> <p><i>AIHW Interpretation:</i> A final check can be required to minimise risk when releasing the findings of the project.</p>	<ul style="list-style-type: none"> <li>• Outputs do not meet confidentiality requirements</li> <li>• Outputs are released without required data supplier approval</li> <li>• Output treatments are inconsistent with those of data already released.</li> </ul>

The five dimensions are assessed separately, then considered jointly to evaluate whether the overall arrangements are such that the risk have been appropriately managed. Any data access proposal considers all five dimensions (even if simply to note that a particular dimension is not relevant to that solution).

Each dimension of the framework can be considered as an adjustable mechanism offering a range of controls at proportionally higher or lower levels depending on the specific case.

While each dimension can be set independently, all five dimensions need to be considered jointly to evaluate whether a particular instance of data sharing is a safe arrangement. The dimensions interact. More stringent controls in one dimension can allow the controls on other dimensions to be relaxed somewhat, and vice versa. In each situation, we must satisfy ourselves that 'Collectively, these techniques are appropriate and adequate to manage the risk.'

The focus of the framework is compliance with our requirements of the Privacy Act, the AIHW Act and our ethical obligations arising from the AIHW Ethics Committee Regulations. The table above illustrates that the scope of a Five Safes framework extends beyond re-identification to consider and manage a wide range of risks associated with data sharing or release.

#### *48.4.7 Conditions for data sharing*

AIHW strives to provide researchers with the most useful data possible while continuing to meet our privacy, confidentiality and data supplier obligations. Each request for data access is considered on a case-by-case basis with a view to maximising the utility of the data provided for the research. To achieve this, researchers can be asked to do any or all of the following:

- provide a research proposal that: is clearly documented; includes the research objectives; states the expected public benefit; and, details the proposed data analysis methodology
- complete a Technical Assessment of a proposed linkage project
- submit an application for ethical review of the research proposal by the AIHW Ethics Committee
- advise us of other data or information available within the proposed work environment
- satisfy us that:
  - they have expert knowledge in the subject area
  - they have the skills and resources required to undertake the research project and associated analysis
  - they understand and have the capacity to prevent and manage data breach risks
  - they will not attempt to link the data to other data
  - data will always be stored on approved media in an access restricted environment
  - access to the data will be restricted (password controlled or two-factor authentication) to those listed as authorised to access the data
  - physical security of the work environment meets our requirements
  - the data hosting facilities are compliant with the relevant provisions of the Australian Government Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) and are fit for managing AIHW data

- the data will be destroyed – when no longer required, by a date agreed in the terms and conditions, or if the organisation ceases operation – whichever is the sooner
- they are not subject to any conflicts of interests or incentives to breach the terms and conditions of use
- they are supported by their organisation, including the organisation’s preparedness to sign a memorandum of understanding or a legally binding contract for which sanctions can apply in the event of non-compliance.
- sign terms and conditions of use, which may be legally binding. Sanctions can apply for non-compliance with terms and conditions
- permit us to undertake audits of the work environment to ensure compliance with the terms and conditions of use
- ensure that the statistical output of the research complies with AIHW policy and data supplier requirements regarding de-identification. Outputs may be subject to audit or approval by the AIHW.

Our requirements of researchers in these regards will depend on the nature, volume, detail and sensitivity of the data to which they are requesting access. Requests for access to highly aggregated summary data will result in few, if any, of the requirements listed above. Access to highly sensitive or detailed data may call for your response to most or all of the above.

The data custodian is responsible for determining which of the above requirements are to apply for each instance of data sharing.

#### *48.4.8 Managing Statistical Outputs*

The preconditions for sharing and release, and the de-identification requirements, outlined earlier in this subsection, apply also to the release of statistical outputs of data analysis undertaken by researchers. These requirements mean that in most cases the output data must be checked to ensure that they are de-identified consistent with the guidelines in Part 1 of the AIHW De-identification policy.

#### **Output from analysis derived from a single data collection**

In the case of analysis derived from a project specific dataset created by linkage to a single data collection, the data custodian is accountable for ensuring appropriate review is undertaken prior to release. It may be appropriate for the data custodian or member(s) of their team undertake this review. It may also be pragmatic to require researchers to undertake this review as part of the terms and conditions of supply, where the researchers have the requisite skills, experience and motivations to ensure the review is in accordance with AIHW and data supplier requirements.

#### **Output from linkage of researchers’ data with AIHW data collections**

Where data provided by researchers are linked data in one or more AIHW data collections to create a project specific dataset, the data custodians of the respective collections work collaboratively with DISC staff to ensure that appropriate review of the output is undertaken prior to release.



## Output from analysis of MELDAs

Each Multi-sourced Enduring Linked Data Asset (MELDA) has a data custodian appointed to exercise overall responsibility for the MELDA. This includes ensuring that appropriate review of the output is undertaken prior to release.

Managing projects drawing on multi-source linked data collections is becoming more complex as the diversity and volumes of data and the number of stakeholders involved expand rapidly. Arrangements for the governance of these projects, including managing the rapidly expanding array of statistical outputs, will be subject to ongoing review.

### 48.4.9 Register of data shared or released

The AIHW data custodians and the DISC maintain a register of all data shared or released. This register is maintained to:

- provide an audit trail that considers all relevant de-identification activities and processes to demonstrate adherence to correct procedures
- facilitate analysis, as required, of risks of re-identification that may arise from differencing attacks on previously released data, and
- support review and improvement of AIHW de-identification activities and processes.

## 48.5 Data archiving, return, collection retirement and destruction

### 48.5.1 AIHW data collections

Most data collections are approved by the Committee as 'ongoing'. In these cases, there are no return to source or destruction requirements. If at some stage a decision is made that the collection is no longer required, Ethics Committee approval should be sought to destroy the collection or return it to source.

A small number of 'limited life' collections have been approved by the Committee. That is, they must be destroyed or returned to source, at the end of a specified period, unless the Committee grants an extension to the life date of the collection.

The *Guidelines for the custody of AIHW data* specify criteria that must be satisfied before a data collection can be deleted.

The National Archives of Australia ([Retaining, managing and disposing of data and datasets](#)) provides the following information on data destruction: 'Data and datasets should be managed to ensure that they are disposed of in accordance with their minimum retention period in an approved records authority. Disposal may involve arranging secure destruction of the data and datasets or, where applicable, transferring custody and/or ownership of the data and datasets to another entity through machinery of government changes, or to the National Archives.' Keeping, destroying or transferring records to the NAA or out of Australian Government custody or ownership is regulated by section 24 of the [Archives Act 1983](#). Among other things, these guidelines seek to ensure our compliance with requirements of National Archives Australia (NAA) regarding [Notices of Disposal Freeze](#), [Records Retention Notices](#) and the [AIHW NAA Records Authority](#).

### *48.5.2 Project specific datasets*

In relation to projects approved by the Ethics Committee, the Committee determined in November 2013 that, for AIHW data held outside their secured physical and electronic environment:

- the default data retention period will be 7 years calculated from the end of the project approval period originally specified by the Committee
- longer periods could be approved on a case-by-case basis when the first application is considered, and at intervals approved by the Committee from time to time (noting, for example, that NHMRC recommend at 15 year retention period for clinical trials)
- projects would be monitored to completion including certification of data destruction.

The terms and conditions of release for data shared by delivered access should include detailed undertakings or requirements regarding the return or destruction of the data at expiration of the data retention period.

Project data may be destroyed when all of the following apply:

1. The data destruction complies with the project's Ethics Committee approval letter and any subsequent amendments.
2. Data are NOT subject to a Notice of Disposal Freeze or a Records Retention Notice from National Archives of Australia.
3. Destruction of the data is consistent with AIHW' National Archives of Australia Records Authority.

Data custodians need to ensure that all historical project data have been destroyed in line with Ethics Committee approvals. Projects should be reviewed on an ongoing basis to ensure this requirement is met.

Data archiving and destruction methods specific to the AIHW's Data Integration Services Centre (DISC) are described section 48.3.4 of this Framework.

## PART 7 – COMPLIANCE

The AIHW regularly monitors compliance with its data management and security arrangements. As provided in the *Guidelines for the custody of AIHW data*, the Ethics, Privacy and Legal Unit undertakes half-yearly validation of the data catalogue through the Data Custodians, to ensure all holdings are listed and their data custodian is current.

The AIHW Ethics Committee requires regular monitoring of progress of projects it has approved. Monitoring occurs through the submission of [annual \(routine\) monitoring reports](#) and a [final monitoring report](#).

The AIHW Ethics Committee requires the maintenance of a register of data collections approved by the Committee and the regular audit of particularly sensitive registers against the Data Collection Management Principles. The audits occur as part of the AIHW's internal audit program and their outcome are also reported to the Risk, Audit and Finance Committee and, through it, to the Board.

Data collections held by AIHW may not only be subject to internal audit, but may also be subject to audit by data suppliers (for example, under conditions specified in data supply agreements) and by statutory office holders, such as the Australian Information Commissioner.

Data custodians complete and submit a Data Collection Monitoring Report and Checklist for each of their data collections listed in the data catalogue. The report and checklist is completed annually unless the following apply, in which case the submission is required every two years:

- the data are not identified or reasonably identifiable/re-identifiable **and** there are no or limited stakeholder requirements above standard legal and AIHW policy or guideline requirements; and/or
- the data are archived, not accessed or very rarely accessed.

### 49 Breaches

The AIHW has in place rigorous controls and protocols in respect of information security, privacy and confidentiality, with an accompanying strong focus on preventing issues. In the event of any identified risk or occurrence, the AIHW will act swiftly to mitigate risk and/or prevent recurrence and will maintain appropriate transparency throughout this process.

#### 49.1.1 Data breach

A data breach occurs when information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.

#### 49.1.2 Privacy breach

Where a data breach involves 'personal information', as defined in the Privacy Act, the data breach may also be a privacy breach, and may be subject to the [Notifiable Data Breaches \(NDB\) Scheme](#).

### 49.1.3 Ethics breach

Data breaches that involve ‘information concerning a person’, as defined in the AIHW Act, may also be a breach of the AIHW Ethics Committee approval conditions for the collection from which the data originated or a breach of the project approval.

A privacy breach is also a breach of the AIHW Ethics Committee approval conditions.

### 49.1.4 Data and privacy breach response plan

The AIHW *Data and privacy breach response plan* (response plan) outlines AIHW procedures and lines of authority for responding to data breaches, including those involving personal information (whether actual or suspected), in accordance with the Privacy Act, the Notifiable Data Breaches Scheme in Part IIIC of the Privacy Act and Australian Government information security requirements. (**Note:** there are mandatory reporting requirements for some types of data and privacy breaches.) The response plan was approved by the CEO in June 2018 to:

- assist the AIHW to rapidly assess, contain and respond to potential data breaches (including those involving a breach of privacy) and mitigate and remediate potential harm to any affected individuals
- clarify relevant roles and responsibilities in the event of a potential data breach, and
- provide a flowchart to assist the AIHW to respond to a potential data breach.

A key aim of data governance, management and security is **preventing** a breach. However, if a breach has occurred, the key aims become containing the breach to minimise harm, managing the breach and preventing future recurrence. The response plan addresses these aims and is reviewed regularly; it was last updated in November 2019.

### 49.1.5 Data and privacy breach and incident registers

In September 2018, ExCo agreed to the establishment of two registers to record details of privacy and data breaches and incidents:

1. Privacy and data breach register
2. Privacy and data incident register

Any incident that is escalated to the Privacy Officer, as required by the *Data and privacy breach response plan*, is recorded in either the incident or breach register.

Where investigation determines that a breach did **not** occur, the case is classified as an incident and recorded in the incident register. The registers are regularly reviewed to identify trends, root causes and initiate preventive action where required.

A template for reporting a potential breach can be found on the Privacy page on Bruce.

## 50 Sanctions

The *Guidelines for the custody of AIHW data* outline the following reporting processes and possible sanctions for breaches of information security and confidentiality:

- The [AIHW Act](#) and the [Australian Public Service Code of Conduct](#) require staff to be diligent in preventing breaches of information security.
- Breach of the confidentiality requirements of section 29 of the AIHW Act constitutes a criminal offence.

- The CEO may appoint a person to investigate the circumstances of a suspected breach. If a breach is proven, the CEO may initiate disciplinary or legal action under the relevant legislation.

## 51 Dealing with complaints

The [AIHW Privacy Policy](#), published on the AIHW website, provides guidance on dealing with privacy complaints and the role of the AIHW's Privacy Officer. The appropriate management of complaints about breaches of privacy is overseen by the Commonwealth Privacy Commissioner.

Applicants dissatisfied with a refusal by the AIHW of access to data under a freedom of information (FOI) request, may submit a request to the AIHW for review of the decision to review access, or may approach the Commonwealth [Office of the Australian Information Commissioner](#) for a review of decision. [More information on FOI processes](#) is available on the AIHW website, including contact details for the AIHW's FOI Contact Officer.

The [Charter of Corporate Governance](#) provides guidance on the management of complaints about Board members.

Bi-lateral data-sharing agreements entered by the AIHW contain dispute resolution procedures to facilitate the prompt resolution of any issues that arise. In the absence of specific complaints resolution processes (for example, in relation to multilateral agreements) complaints are referred through usual management channels to the AIHW CEO for management/action in or by the appropriate forum.

Complaints about researchers, the conduct of research or the conduct of the AIHW Ethics Committee can be addressed to the Ethics Committee Secretary – a role currently undertaken by the Unit Head, Ethics Privacy and Legal. Complaints will be handled promptly and sensitively, in accordance with Chapter 5.6 of the NHMRC National Statement.

## List of Appendices

1. Acronyms and Definitions
2. AIHW Data collection management principles
3. Alphabetical list of Acts, policies and guidelines contained in this Data Governance Framework

## Appendix 1 – Glossary of terms and acronyms

Acronyms and terms used in this Data Governance Framework have the following meanings.

Access control profile	A defined set of controls applied to each of the dimensions of the five safes – projects, people, data, settings and outputs – that collectively provide a high degree of safety for provision of access to data.
Access mode	The defined mode by which users are provided with access to data. See also <i>delivered access, open access, secure on-site access and secure remote access, disclosure, output and release</i> .
Aggregate data	Data that have been created from more detailed data by calculation of summary statistics and/or grouping information into categories. Aggregated data have less detail than the data from which they are derived and are typically presented in tables. Aggregation can be used to achieve <i>confidentialisation</i> , but this is not guaranteed. See also <i>micro data and unit record data</i> .
AIHW	Australian Institute of Health and Welfare.
AIHW Act	<a href="#">Australian Institute of Health and Welfare Act 1987</a> (Cth).
AIHW Ethics Committee	The committee established under section 16(1) of the <i>Australian Institute of Health and Welfare Act 1987</i> (Cth), with a membership prescribed in the <a href="#">Australian Institute of Health and Welfare (Ethics Committee) Regulations 2018</a> .
Anonymisation	The process of removing identifying information to produce <i>non-identified data</i> . (Note that some other organisations define anonymisation to mean de-identification.) See also <i>de-identification</i> .
Archiving	Transferring appropriately described information to a storage facility with established arrangements for preservation and retrieval of that information on a long-term or permanent basis.
Assets	Resources under the control of a person or entity that have recognised value.
Attribute disclosure	Where information about an individual, group or organisation, which was not already known, is revealed (without necessarily formally re-identifying them). Also known as attribution.

Confidentialisation	<p>Treatments applied to data to reduce the likelihood of <i>re-identification</i> and <i>attribute disclosure</i>.</p> <p>See also <i>statistical disclosure control</i>.</p>
Confidentialised Unit Record File (CURF)	<p>Files that consist of <i>Unit record data</i> that have been modified to protect the confidentiality of information subjects while also maintaining the integrity of the data.</p>
Content information	<p>Information within a dataset that is used for analysis.</p> <p>See also <i>identifying information</i>.</p>
Custody	<p>Assuming responsibility for data, usually under an arrangement pertaining to management and use of the data.</p> <p>See also <i>data custodian</i>.</p>
Data	<p>Data are 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 includes information about persons, businesses and other organisations and their characteristics, practices and activities.</p>
Data analytic risk assessment	<p>A range of techniques from the very simple (counting unique combinations or identifying small cells) to more complex construction of statistical or computational models. These techniques take the dataset in question as an analytic object, treating disclosiveness as a property of the data and attempting to identify the level of that property latent in the data.</p> <p>Sometimes referred to as (statistical) disclosure risk assessment.</p>
Data breach	<p>A data breach occurs when information is subject to unauthorised access, modification, use, <i>disclosure</i>, or other misuse. 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.</p> <p>A data breach that involves information from which a person could reasonably be identified is a <i>privacy breach</i>.</p>
Data catalogue	<p>The official registry of the data holdings of the AIHW data. The data catalogue is the official listing of AIHW's data collections.</p>

Data collection	<p>A cohesive set of data with measurable value that is designed to address a specific set of business needs. AIHW data collections are listed in the AIHW data catalogue, assigned an AIHW data custodian, and subject to strict governance arrangements detailed in the <i>Guidelines for the custody of AIHW data</i>.</p> <p>If one or more of the following apply, the data holding is designated a data collection and listed in the data catalogue:</p> <ol style="list-style-type: none"> <li>1. the holding includes identified unit record (individual or service-level) data or reasonably identifiable or re-identifiable unit record data</li> <li>2. the AIHW Senior Executive determines that the data should be managed by a data custodian appointed by the CEO via the AIHW Data Custodian Delegation, regardless of whether they contain identified or reasonably re-identifiable data. This includes data holdings which need to be managed by a data custodian in compliance with data supplier requirements or where this is public sensitivity about the data</li> <li>3. the AIHW provides access to a set of data by third parties or uses the data for linkage.</li> </ol>
Data custodian	<ol style="list-style-type: none"> <li>1) The agency that collects or generates data for any purpose, and is accountable and responsible for the governance of that data. [DPMC]</li> <li>2) An AIHW staff member with delegation from the AIHW CEO to exercise overall responsibility for a specified data collection in accordance with policies, guidelines and any specific conditions for use applicable to that data collection. [AIHW Data Governance Framework]</li> </ol>
Data provider	<p>An individual, household, business or other entity that supplies data, or has data about them supplied by a third party, to a government agency. [DPMC]</p>
Data subject	<p>The entity to which the data relates. Entities can include persons, organisations, and transactions; data subjects and can be the units in <i>unit record data</i>.</p>
Data supplier	<p>An agency or organisation that supplies data to the AIHW.</p>
Data release	<p>Making data publicly available with few or no restrictions on who may access the data and what they may do with it. [DPMC]</p> <p>See also <i>access mode, data sharing, disclosure, open access and output</i>.</p>
Data sharing	<p>Making data available to another agency, organisation or person under agreed conditions. [DPMC]</p> <p>See also <i>access mode, data release, disclosure, open access and output</i>.</p>



Data sharing agreement	A formal arrangement between a data custodian and another agency, organisation or individual that details conditions under which data is shared and used. [DPMC]
Data situation	<p>A single term to describe all of the arrangements under which access to the data will be provided. This includes contextual considerations relating to:</p> <ul style="list-style-type: none"> <li>the <i>access mode</i>;</li> <li>the <i>setting</i> in which the data are being used;</li> <li>the <i>confidentialisation</i> of the data;</li> <li>the knowledge, skills and motivations of the users; and</li> <li>the use to which the data is being put.</li> </ul> <p>The data situation is particular to each case and can change over time.</p>
Dataset	Any collection of data about a defined set of entities, called population units. The units can be persons, households, businesses or other entities.
De-identification	<p>The process of treating data so that they are no longer <i>reasonably identifiable</i> for the purposes of the Privacy Act or <i>information concerning a person</i> as defined in s 29 of the AIHW Act, having regard to all the circumstances of the particular case.</p> <p>The de-identification process involves treatments (<i>confidentialisation</i>) to remove, obscure, aggregate, alter and/or protect data, with a view to reducing the likelihood of <i>re-identification</i> or <i>attribute disclosure</i>.</p> <p>De-identification requires consideration of the totality of the <i>data situation</i> in the particular case, including the <i>setting</i> into which it will be made available and the data users.</p> <p>Also known as contextual de-identification.</p>
De-identified data	Data which have been through a process of <i>de-identification</i> . There is no reasonable likelihood of <i>re-identification</i> having regard to the <i>data situation</i> , treatments and controls applied in the particular case.
Delivered access	An <i>access mode</i> in which data are made available by direct delivery to the user's <i>custody</i> . The user can be required to agree to specific conditions associated with management and use of the data.
Direct identifier	<p>A single data item that is either the name of a person, or a unique identification code assigned to them. A name identifies a person. An identification code can identify a person, when it is known to have been assigned to them or can be found in another dataset that links the person's name to the identification code. Person, in this definition, refers to an individual, organisation or other entity.</p> <p>See also <i>identifier</i>.</p>

Disclosure	When an entity makes information available to others and relinquishes control of the subsequent handling of the information. See also <i>access mode, data release, data sharing</i> and <i>output</i> .
Disclosure risk	The combination of likelihood and consequence that information about an individual, organisation or other entity is revealed or provided to an unauthorised person or entity. [DPMC] See also <i>re-identification risk</i> .
FOI	Freedom of information
FOI Act	The <a href="#">Freedom of Information Act 1982</a> (Cth)
Identifiable data	Data that are either <i>identified data</i> or <i>de-identified data</i> that contain sufficient detail that a person(s) or organisation(s) can be re-identified within the data, given the particular <i>data situation</i> .
Identified data	Data that include <i>personal information</i> or <i>information concerning a person</i> and includes identifying information allowing them to be known in the current <i>data situation</i> from just a few fields of data.
Identifier	An individual variable within a dataset that is among the dataset's identifying information.
Identifying information	Information which when taken together is sufficient to establish a link between the information and a particular individual, organisation or other entity, thus identifying them within the data. Identifying information can be used for linking data sets. See also <i>content information</i> .
Inferential disclosure	Inferential disclosure occurs when information can be inferred with high confidence from statistical properties of the data.  For example, the data may show a high correlation between income and purchase price of a home. As the purchase price of a home is typically public information, a third party might use this information to infer the income of a data subject.

<p>Information concerning a person</p>	<p>A term defined in s 29 of the <u>AIHW Act</u>:  ‘any information concerning another person ... being acquired ... because of:</p> <ul style="list-style-type: none"> <li>(i) holding an office, engagement or appointment, or being employed, under this Act;</li> <li>(ii) performing a duty or function, or exercising a power, under or in connection with this Act; or</li> <li>(iii) doing any act or thing under an agreement of arrangement entered into by the Institute...’</li> </ul> <p>where</p> <p>‘person includes a body or association of persons, whether incorporated or not, and also includes:</p> <ul style="list-style-type: none"> <li>(1) in the case of an information provider - a body politic; or</li> <li>(2) in the case of an information subject - a deceased person</li> </ul> <p>[AIHW Act]</p>
<p>Intruder</p>	<p>A data user who attempts to access, modify, <i>release</i> or disclose data without appropriate approvals.</p>
<p>MELDA</p>	<p>Multi-sourced Enduring Linked Data Asset</p>
<p>Metadata</p>	<p>A structured description of the characteristics of specified data, including its content, quality and format.</p>
<p>Micro data</p>	<p>The most detailed unit record data available.</p> <p>Micro data may contain <i>unit record data</i> pertaining to more than one item of interest. For example, a single set of micro data could contain data about patient, hospital and jurisdiction.</p> <p>See also <i>unit record data</i> and <i>aggregated data</i>.</p>
<p>NHMRC</p>	<p>National Health and Medical Research Council</p>
<p>Non-identified data</p>	<p>Data that include <i>personal information</i> or <i>information about a person</i> where information that may allow for direct identification are not present but no further <i>de-identification</i> techniques or controls have been applied. Note that <i>non-identified data</i> may still be <i>identifiable data</i>.</p>
<p>Open access</p>	<p>An <i>access mode</i> in which data are made publicly available with few or no restrictions on who may access the data and what they may do with it.</p> <p>For example, making data available through a publicly accessible website. The data made available through open access is sometimes called open data.</p> <p>See also <i>access mode</i>, <i>data release</i>, <i>delivered access</i>, <i>secure remote access</i>, and <i>secure on-site access</i>.</p>

Output	<p>Data leaving a given <i>data situation</i> (and therefore entering another <i>data situation</i>).</p> <p>See also <i>access mode, data sharing, disclosure</i> and <i>release</i>.</p>
Penetration testing	<p>In the context of de-identification, the idea of penetration testing is to replicate what a plausible motivated intruder might do (and the resources they might have) to execute a re-identification attack on a dataset. [OAIC]</p> <p>In the context of ICT systems, a penetration test is designed to exercise real-world targeted cyber intrusion scenarios in an attempt to achieve a specific goal, such as compromising critical systems or information. [ISM]</p> <p>Also known as intruder testing.</p>
Personal information	<p>A term defined in s. 6 of the <u>Privacy Act</u>:                  ‘Any information or an opinion about an identified individual, or an individual who is reasonably identifiable:                  (a) whether the information or opinion is true or not; and                  (b) whether the information or opinion is recorded in a material form or not.’ [Privacy Act]</p>
Privacy Act	The <u>Privacy Act 1988</u> (Cth)
Privacy breach	A <i>data breach</i> that involves <i>personal information</i> and from which a person could reasonably be identified.
Reasonably identifiable	It is technically possible for <i>re-identification</i> to occur and there is a reasonable likelihood that this might occur given the <i>data situation</i> .
Responsible officer	A senior person in an organisation who has the legal authority to agree to conditions of shared data use on behalf of that organisation. [DPMC]
Re-identification	<p>The discovery of the identity of individual(s) or organisation(s) in apparently <i>de-identified data</i> or <i>non-identified data</i>.</p> <p>Also known as identity disclosure.</p>
Re-identification risk	<p>The combination of likelihood and consequence of <i>re-identification</i> occurring given the totality of the <i>data situation</i>.</p> <p>See also <i>disclosure risk</i>.</p>
Secure on-site access	An <i>access mode</i> in which data are made available to users in a managed physical location that has a high level of security infrastructure control and where the users’ activities can be personally supervised. The controls are such that the <i>data custodian</i> can fulfil all their obligations. The AIHW DataLab is an example.

Secure remote access	An <i>access mode</i> in which data are made available to users via remote access that has a high level of security infrastructure control and where the users' activities can be remotely supervised. The controls are such that the <i>data custodian</i> can fulfil all their obligations. The ABS DataLab and SURE are examples.
Sensitive information	<p>A defined category of personal information under the Privacy Act, which is accorded a higher standard of protection under the Australian Privacy Principles as it more likely to cause harm or distress.</p> <p>Defined in section 6 of the Privacy Act to include information or opinion about a person's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, trade union membership or associations, sexual orientation or practices, criminal record and health, genetic and/or biometric information.</p>
Sensitive variables	Distinguishable from sensitive information, which is a legal term, 'sensitive variables' are variables contained in a data record that the data subjects would not want to be disclosed. Sensitive variables are subjective and cannot be exhaustively defined, however they would include sensitive information as described above, and any other type of personal information that a data subject wants to keep confidential. For example, this could include data related to income, wealth, credit record and financial dealings.
Separation principle	<p>Arrangements designed to protect the identity of people, organisations and other entities, whereby individuals have access to either identifying information in a dataset or the content information, never both at the same time.</p> <p>See also <i>identifying information</i>, <i>content information</i>, <i>identifier</i> and <i>direct identifier</i>.</p>
Setting	The physical and technological environment into which data are provided. Settings have variable degrees of physical security, IT security, controls on who can enter the physical environment, and what data can enter and leave the setting.
Spontaneous recognition	An unintentional identification of an individual within a dataset from personal knowledge of a small number of characteristics.
Staff	People working for the AIHW including ongoing APS employees, non-ongoing APS employees, and those engaged by AIHW under labour hire agreements.
Statistical disclosure control	<p>Statistical treatments applied to data to reduce the risk of <i>re-identification</i> and <i>attribute disclosure</i> while maintaining data utility.</p> <p>See also <i>confidentialisation</i>.</p>

<p>Unit record data</p>	<p>Detailed data comprising individual records, where each record contains information about a particular unit of interest.</p> <p>Examples of units include person, organisation, transaction and geographic area. Where the units are people and organisations, the records contain <i>personal information</i> or <i>information about a person</i> respectively.</p> <p>Unit record data can be <i>micro data</i> if the item of interest provides the most detailed data available. Unit record data can also be <i>aggregated data</i> where the unit presents a grouping of more detailed unit records.</p> <p>See also <i>micro data</i> and <i>aggregated data</i>.</p>
-------------------------	--

## Appendix 2 – Data collection management principles

### Principle 1 – Data collections are established and managed effectively, appropriately and consistently, with clear accountability requirements and governance arrangements.

- 1.1 Procedures for the management of the data collection are documented and maintained.
- 1.2 Procedures detail how data are collected, why data are collected, when data are collected, and by whom data are collected.
- 1.3 Procedures address data collection, storage, security, integrity, manipulation and dissemination.
- 1.4 Systems are in place to ensure adherence to documented procedures.
- 1.5 Data are collected and stored with appropriate metadata to accurately define and describe it.
- 1.6 Data comprising ‘personal information’ and/or ‘information concerning a person’ are collected, used and disclosed only in accordance with Privacy Act 1988 and Australian Institute of Health and Welfare Act 1987 requirements.
- 1.7 Data custodians for the collection are clearly identified.
- 1.8 Responsibilities of data custodians are defined, documented and adhered to.

### Principle 2 – Data receipt processes ensure the security and integrity of the data during transfer.

- 2.1 Procedures are in place to ensure that data are transmitted by data suppliers and received without degradation/corruption.
- 2.2 Requests to data suppliers for data include information on transmitting the data in a secure manner.
- 2.3 Received data are assigned to a data custodian.

### Principle 3 – Data are stored securely and regularly backed up.

- 3.1 Operating systems in which databases are installed should be appropriately secured.
- 3.2 Access to the operating system running the database in which the collection is stored should be appropriately restricted.
- 3.3 Each database should be covered by data backup and recovery procedures.
- 3.4 These backup and recovery processes should be regularly undertaken.
- 3.5 Backups should be regularly tested.

### Principle 4 – Integrity of the data is maintained.

- 4.1 Procedures for processing and manipulation of the data are documented and include data storage, migration, editing and protecting the integrity of the data during analysis.

- 4.2 Employees handling data are appropriately trained and qualified and are subject to appropriate confidentiality requirements.

**Principle 5 – Controls for persons/entities having access to the collection exist and are implemented.**

- 5.1 Access to collections is granted on a needs basis. If access is not specifically needed for operational purposes it is not granted.
- 5.2 Individuals granted access to AIHW data collections are only granted a level of access ('permissions') to those data commensurate with their role and level of responsibility.
- 5.3 Database administrative access is restricted to appropriately skilled and authorised database administrators.
- 5.4 All users accessing AIHW collections are uniquely identifiable and authenticated on each occasion that access is granted.
- 5.5 Database access permissions are documented and appropriately granted or revoked for all users. All changes to database access permissions are approved by the data custodian.

**Principle 6 – Data transmission or dissemination from the collection to any source (internal or external) is conducted in a manner which ensures its accuracy, integrity and security.**

- 6.1 Documented procedures for the collection detail to whom the data may be sent, when data are sent, how these data must be sent and why the data are to be sent.
- 6.2 Transmission or dissemination of the data is compliant with any conditions imposed by the AIHW Ethics Committee and also the data supplier(s) of the data being transmitted or disseminated.
- 6.3 Conditions/compliance requirements imposed by Ethics Committee and data supplier(s) are passed on to data recipients.
- 6.4 Documented procedures include measures to ensure the data are sent intact, non-degraded/uncorrupted and securely.
- 6.5 Data are sent securely, consistent with the sensitivity of the data.
- 6.6 A register of requests for unpublished data and associated action taken in response to such requests is maintained.

**Principle 7 – End of data lifecycle/use is appropriately managed**

- 7.1 Documented procedures for the collection include information on what happens to the data at the end of its use.
- 7.2 Data are destroyed, returned to data owner (for example, in compliance with contractual obligations), or de-identified (per Privacy Act requirements) and archived in a secure environment, as appropriate, when no longer needed.



## **Appendix 3 – Alphabetical list of key legislation, policies and guidelines in the Framework**

### **Legislation**

[Archives Act 1983](#)

[Australian Institute of Health and Welfare Act 1987](#)

[Australian Institute of Health and Welfare \(Ethics Committee\) Regulations 2018](#)

[Freedom of Information Act 1982](#)

[Privacy Act 1988](#)

[Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#), (Privacy Code) developed under s. 26G of the Privacy Act

[Privacy Amendment \(Notifiable Data Breaches\) Act 2017](#) from which the relevant requirements are now contained in Part IIIC of the Privacy Act.

[Public Governance, Performance and Accountability Act 2013](#)

### **External policies, guidance and standards**

[Australian Code for the Responsible Conduct of Research, 2018](#) (the NHMRC 2018 Code)

[Australian Government Information Security Manual \(ISM\)](#).

[Australian Government Protective Security Policy Framework \(PSPF\)](#)

[Australian Privacy Principles](#)

[Australian Public Service Code of Conduct](#)

[Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities: Guidelines for researchers and stakeholders](#) (NHMRC 2018)

[Guide for Data integration projects involving Commonwealth data for statistical and research purposes](#) (National Statistical Service)

[Guidelines under Section 95 of the Privacy Act](#) (NHMRC)

[Information Management Standard for Australian Government](#) (National Archives Australia)

[National Statement on Ethical Conduct in Human Research \(2007\) - Updated 2018](#) (NHMRC)

[National Statistical Service \(NSS\) guide for data integration projects involving](#)

[Notifiable Data Breaches \(NDB\) Scheme AOIC](#)

[Retaining, managing and disposing of data and datasets](#) (National Archives Australia)

### **AIHW corporate documents, policies and guidelines**

AIHW Data Transfer Policy 2020

AIHW Strategic Directions 2017-2021

[Charter of Corporate Governance](#)

Data and privacy breach response plan

Data Catalogue

Data Collection Management Principles

Data Collection Monitoring Report and Checklist

Data custodian clearance of data in reports

Data Custodianship Delegations

Data linkage and protecting privacy policy

Data Quality Statements (DQS) policy and guidelines.

De-identification Policy (2020)

Delegations

Guidance to collaborating units on secure use, handling and storage of AIHW data

Guidelines for the custody of AIHW data

ICT Framework

ICT security

ICT Strategic Plan 2017-2020

Information Security and Privacy Policy and Procedures

Instrument of Delegation dated 22 February 2018 (delegates powers of the Board to the Chief Executive Officer)

Instrument of delegation for sharing and release of AIHW data and release of AIHW products

Learning and Development Strategy 2017-2021

National Best Practice Guidelines for data linkage activities relating to Aboriginal and Torres Strait Islander people

Physical security policy

Policy on reporting to manage confidentiality and reliability

Privacy Management Plan (PMP)

[Privacy Policy](#)

Public Domain Policy

Recruitment and Selection Policy and Procedures

Review and approval (R-A) plan

Risk Management Framework

Security Plan (2019)

Security Risk Management Policy

Statistics for the AIHW

Strategic Risk Profile

**AIHW repositories, tools, systems and fact sheets**

AIHW data catalogue

[AIHW data collections \(public version\)](#)

[AIHW data request application](#)

[AIHW Ethics Committee - annual \(routine\) monitoring report](#)

[AIHW Privacy Policy](#)

[EthOS™](#)

Institute Projects

[METeOR](#)

[Validata™](#)