



Australian Government

Australian Institute of Health and Welfare



Data
Governance—
in-brief



What is data governance?

Data governance is the system of decision rights and accountabilities surrounding data and the use of data. It can involve legislation, organisational structures, legal contracts, and various agreements, policies, and guidelines.

Data governance arrangements at AIHW help us to achieve our mission of providing authoritative information and statistics about Australians while complying with our legal, regulatory and governance obligations in acquiring, handling and releasing data.

The public has the right to expect that AIHW will manage data professionally, with due respect for its sensitivity, and with privacy and confidentiality assured.

As an information agency, we rely on strong data governance to retain the trust of our many data providers, data recipients and other stakeholders.

AIHW Data Governance Framework

The AIHW's Data Governance Framework is a 24-page document that explains general data governance concepts, and details the AIHW's robust data governance arrangements. A copy of the full Framework is available from the AIHW (see 'Contact' section).

This brochure provides a brief summary of the Framework.

Key features of the Framework

Legislation

The AIHW Act

The *Australian Institute of Health and Welfare Act 1987* (the AIHW Act) establishes the AIHW as a Commonwealth corporate entity and sets out the Institute's functions, powers and governance arrangements. The main functions of the AIHW are to collect, analyse and disseminate health- and welfare-related information and statistics.

The AIHW Act enables the release of information for public benefit while protecting the identity of individuals and ensuring that data providers can be confident that the AIHW will adhere to data supply terms and conditions.

Section 29 of the AIHW Act contains a confidentiality provision which prohibits the release of information 'concerning a person' held by the AIHW unless one of three specific exceptions applies. These are:

- express written permission to release the information to a specific party has been given by the relevant data provider(s)
- release has been approved by the AIHW Ethics Committee, and such release is consistent with the terms set by the data provider when supplying data to the Institute
- release is in the form of publications containing de-identified statistics, information and conclusions.

The confidentiality requirements in section 29 protect a broader range of information than the Privacy Act, including information about deceased persons.

Privacy Act

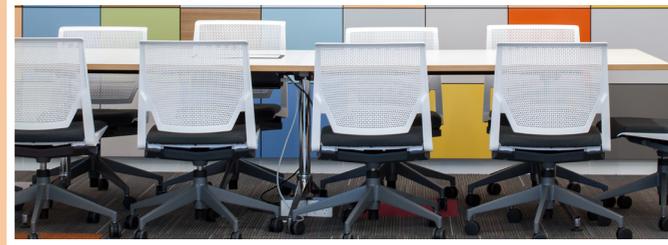
The *Privacy Act 1988* creates obligations on Commonwealth agencies and private sector organisations in relation to collecting, using or disclosing personal information. The AIHW is therefore bound by two sets of confidentiality and privacy requirements—those contained in the Privacy Act and those contained in section 29 of the AIHW Act.

Freedom of Information Act

Under the *Freedom of Information Act 1982* (FOI Act), 'documents' held by agencies (which includes information in databases) are subject to access by members of the public unless a legislative exception applies. Section 32 of the FOI Act provides that data protected by the confidentiality provisions of section 29 of the AIHW Act are exempted from release under FOI.

Decisions on whether AIHW documents can be released under the FOI Act are made by the AIHW's Freedom of Information Officer in the first instance.





Structures and roles

Board

The AIHW is governed by a Board established under the AIHW Act. The Board has 15 members who have knowledge or experience relevant to the work of the AIHW and who come from a wide range of Commonwealth, State and other organisations. The Board has approved the Data Governance Framework.

Ethics Committee

The AIHW Act establishes an AIHW Ethics Committee whose main functions are to form an opinion on ethical grounds of the acceptability of any activities being conducted by the AIHW, or the release of identifiable data for research purposes. It may impose any conditions it thinks appropriate in performing its functions.

Significantly, the Ethics Committee may authorise:

- the release of personal information for medical research that would otherwise be a breach of a privacy principle in the Privacy Act; and/or
- the release of health-related or welfare-related information as provided for in section 29 of the AIHW Act.

Further information about the AIHW Ethics Committee and its processes, including a list of approved projects is available at www.aihw.gov.au/ethics/.

Audit and Finance Committee

The AIHW Audit and Finance Committee comprises three members of the Board and one independent Committee member. It reports to the Board on strategic, financial and data audit matters, including fraud control, security, and the results of regular audits of sensitive data collections required by the Ethics Committee as part of the AIHW's overall internal audit program.

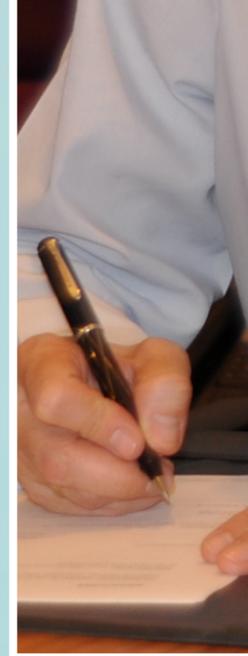
Director

The Director is the chief executive officer of the organisation and manages the Institute subject to the direction of the Board and consistent with Board policies. The Director approves the release of AIHW publications and important internal policies covering all aspects of data management.

The Director has delegated the management of specific data collections to AIHW data custodians (see section below).

Executive Committee

The Executive Committee comprises the AIHW Director and Group Heads (Senior Executives). In making decisions on data governance policies and procedures the Director considers advice provided by the Executive Committee.



Data Governance Committee

The Data Governance Committee, comprising 7 senior staff of the Institute, makes recommendations on data governance and data-related matters to the Executive Committee.

Data custodians

A data custodian is a staff member with delegation from the Director to exercise overall responsibility for a specific data collection, in accordance with legislation, policies, guidelines and any specific conditions for use applicable to that data collection. Subject to these requirements, a data custodian has the power to release data to other bodies or persons.

Prescribed security roles

Effective security risk management is required of *all* AIHW personnel and contractors. More specifically, the Australian Government's Protective Security Policy Framework (PSPF) prescribes key security roles for agencies. In AIHW, the Head of the Business and Governance Group is the Security Executive, responsible for agency protective security policy and practices, while the AIHW Facilities Manager is the Agency Security Adviser, responsible for day to day protective security functions. The Unit Head, ICT Operations, is the AIHW's Information Technology Security Adviser responsible for co-ordinating information technology security.



Data linkage

The AIHW is accredited to integrate Commonwealth data for high-risk research projects. The AIHW performs data linkage through its 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.

Policies, guidelines and procedures

The AIHW's internal data policies, guidelines and procedures are designed to ensure that all staff, and especially those with delegated authority to make data-related decisions, have clear sources of information to guide them in performing their roles effectively and appropriately. These documents cover the acquisition, management, linkage, security, confidentiality, quality, publication and retention of data.



Systems and tools

ICT systems

The AIHW's ICT systems support secure and auditable data governance processes. In particular, access to data is separately restricted at the network, data server and database level, requiring individual authorisation.

AIHW data catalogue

The AIHW's Data Catalogue is the official listing of all AIHW data collections. It:

- identifies past and present data custodians for each AIHW data collection; and
- describes 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 related datasets (if any).

A limited public version of the *Data catalogue* is available on the AIHW website.

METeOR

METeOR, which is managed by the AIHW, is Australia's registry of national metadata standards for the health, community services and housing assistance sectors. Through METeOR users can find, view and download over 2,600 data standards.

These standards provide a structured description of the characteristics of data. METeOR allows free online access to a wide range of nationally endorsed data definitions, and tools for creating new definitions based on existing already-endorsed components.

Validata™

The AIHW works with its data providers to maximise the currency and quality of 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. It enables data providers to quickly check and validate the quality of their data submissions against a set of validation rules.



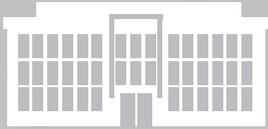
Compliance

The Ethics Committee requires regular monitoring of the progress of projects it has approved and audits of particularly sensitive data collections. The audits occur as part of the internal audit program, with outcomes reported to the Board through the Audit and Finance Committee.

Data collections held by AIHW may also be subject to audit by data providers (for example, under conditions specified in data supply agreements) and by statutory office holders such as the Auditor-General and the Privacy Commissioner.

The AIHW Act and Australian Public Service Code of Conduct require staff to be diligent in preventing breaches of information security. A breach of the confidentiality requirements of section 29 of the AIHW Act constitutes an offence punishable by law, including imprisonment.

Contact



For questions and comments on the AIHW Data Governance Framework or any related complaints please contact the AIHW via email



info@aihw.gov.au

or visit the AIHW website



www.aihw.gov.au

Printed 2014.

Photos of building interior by Ben Wrigley.

