Australian Government

Australian Institute of Health and Welfare

DATA GOVERNANCE FRAMEWORK

2014

Table of contents

PART 1: INTRODUCTION

The 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 provide reliable, regular and relevant information on Australia's health and welfare. Our work informs and supports the development of health and welfare policy and programs and is a valuable source of research data.

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."[1] In simple terms, data governance describes how data-related decisions are made within an organisation or group of organisations.

This Framework

This Data Governance Framework identifies and provides an overview of the AIHW's robust data governance arrangements, including:

- a description of key concepts in data and data governance;
- the legal, regulatory and governance environment in which AIHW operates;
- core data governance structures and roles;
- an overview of AIHW data-related policies, procedures and guidelines;
- systems and tools supporting data governance; and
- compliance regimes.

These data governance arrangements apply to data: collected and/or enhanced by the AIHW; collected on the AIHW's behalf (for example under collaborative or sub-contractual agreements); and data obtained from all external sources.

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

This Framework recognises that a combination of supporting legislation, roles, policies, practices and supporting tools and technologies is required to deliver effective data governance arrangements at AIHW.

Audience

This document contains key information for all AIHW staff and in particular those who have delegated authority to make data-related decisions. It is also an important source of 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.

[1] Data Governance Institute, http://datagovernance.com/adg_data_governance_definition.html , accessed 22 January 2014.

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 contained in Part 3 of the Framework.

Data

Data means 'factual information used as a basis for reasoning, discussion or calculation.'[2] Data can be stored in structured formats (e.g. databases), semi-structured formats (e.g. spreadsheets) and non-structured formats (e.g. documents). This Data Governance Framework applies to data held by AIHW in structured and semi-structured formats.

While money and people have long been considered assets, data and the information created from that data are now also widely recognised as organisational assets or, in respect of the public sector, strategic assets for the nation. High quality data informs decision-making and makes it more effective, and consistent management of quality data improves operational, tactical, and strategic performance. Within a public sector context, the proper use of public monies requires that all assets are appropriately managed, including data and information. Data held by public sector agencies are recognised as a national resource that should be made available for community access and use, unless there are legal reasons certain information should be protected.[3]

Data collections

Individual sets of data may be called 'data collections', 'data assets' or 'data holdings'. As the AIHW has traditionally used the term 'data collections', this is the term used throughout the Framework..

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

The *nature* of data also impacts controls placed upon them. Data collections may contain aggregate data, de-identified data (where information which could identify an individual has been removed) or identifiable information. All data collections are subject to policies, processes and controls, however additional strict constraints regarding collection, storage, use, linkage and disclosure apply to identifiable information. These 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 controls applicable to the AIHW are further explored in Part 3 of this Framework.

Data governance and data management

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*

[2] http://www.merriam-webster.com/dictionary/data , accessed 23 January 2014.

[3] *Principles on Open Public Sector Information,* OAIC, (May 2011), p. 1.

what information, and when, under what circumstances, using what methods."[4] In other words, it 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.

Data Management comprises the 'agreed upon models' in the definition above. It is "*the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets.*"[5]

Data management may be divided into several components, as shown in **Figure 1**.

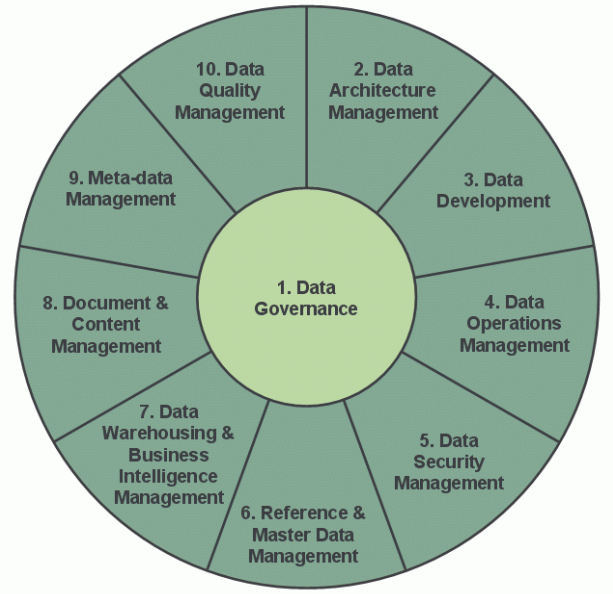

Figure 1: Data management functions[6]

Each of these data management components is described briefly below:

- *Data architecture management* involves defining the blueprint for managing data collections;
- *Data development* comprises analysis, design, implementation, testing, deployment and maintenance;
- *Data operations management* involves the provision of operational and technical support from data acquisition to purging;
- *Data security management* ensures privacy, confidentiality and appropriate access
- *Reference and master data management* involves managing authoritative information about standards and the business of the organisation;
- *Data warehousing and business intelligence management* enables reporting and analysis;
- *Document and content management* relates to managing data held outside of databases;
- *Metadata management* involves integrating, controlling, and providing metadata; and
- *Data quality management* involves defining, monitoring and improving data quality.

[4] Data Governance Institute, http://datagovernance.com/adg_data_governance_definition.html , accessed 22 January 2014.

[5] http://www.dama.org/files/public/DI_DAMA_DMBOK_Guide_Presentation_2007.pdf

[6] Ibid.

Note that Figure 1 does not reflect the full data lifecycle (for example, it does not address data acquisition, dissemination or destruction) but rather provides an overview of data management activities *within* an organisation. AIHW data governance, described in Part 3 of this Framework, covers the full data lifecycle including dissemination, which is a key function of the AIHW.

Data registry

A data registry is a log of all data collections held and managed by an organisation. A data registry commonly holds the following metadata about each data collection: the date of commencement; duration of use of the data collection (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. The AIHW's data registry is known as the 'Data Catalogue' and is described further in Part 3.

Metadata and metadata standards

In order to effectively manage and use data, metadata needs to accompany data collections. Metadata is the structured description of the characteristics of data, including its content, quality and format. It is important for comparability and to ascribe a shared meaning, and makes it easier to retrieve, use and manage information resources.

Metadata supports: enhanced efficiency and reliability of data processing and transmission; improved received and stored data quality; completion of more validation work at source; less staff time spent on routine and duplicated work; better retention of, and access to, corporate knowledge; easier access to, and better compliance with, agreed data standards; and a simpler process to enact widespread data standards changes.

Metadata standards are one type of metadata which describe the meaning and acceptable representation of data for use within a defined context.

A *metadata registry* is a system which enables the creation, management and dissemination of metadata. A *data standards registry* is a metadata registry which contains data standards. An example is METeOR, Australia's registry of national data standards for health, community services and housing assistance, which is managed by the AIHW. METeOR includes useful information about metadata and metadata standards.

Data policies, guidelines and procedures

Data policies are high-level statements that provide context for strategic decisions relating to data in an organisation. 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.

Tools

Tools are pre-prepared objects that support people in carrying out procedures. Tools can range from checklists to workflow systems designed to automate approval processes. In all cases, they promote a standardised approach to a particular component of data governance. Tools produce records which can be reviewed to assess compliance with policy.

PART 3: AIHW DATA GOVERNANCE

The AIHW's internal data governance is informed by, and designed to ensure compliance with, its external legal, regulatory and governance environment whilst delivering on its mission to provide authoritative information and statistics to promote better health and wellbeing for Australia's people.

This Part describes the AIHW's external environment, as well as its internal data governance arrangements, data management policies, guidelines and procedures, and systems and tools that support good data governance and management. While this Part highlights the role played by each of these core elements, it is the combination of these features, policies and functions that best delivers AIHW's dual obligations of maximising health and welfare data availability whilst protecting the confidentiality and privacy of identifiable data. The AIHW's capabilities in this regard are reflected in its status as one of only two accredited Commonwealth Data Integration Authorities.

Legal, regulatory and governance environment

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 Act establishes the AIHW's functions and powers and its governing bodies, including the AIHW Board, Director and 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. Key areas of such information include health, aged care services, child care services, services for people with disabilities, housing assistance, child welfare services and other community services.

Although the AIHW Act requires AIHW to place information in the public domain, it also contains a confidentiality provision. Section 29 of the 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 provider(s);
- where release has been approved by the AIHW Ethics Committee; and
- in the form of publications containing de-identified statistics, information and conclusions.

The Act recognises that the AIHW's many data providers 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 providers.

The AIHW Act therefore facilitates the release of information designed to ultimately benefit the public, protects the identity of individuals and ensures data providers 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. This is described further in each of the component parts of the section 'AIHW structures and roles in data governance'.

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 1989* establish the functions and composition of the Committee. These are described further under the heading 'AIHW Ethics Committee' in the section 'AIHW structures and roles in data governance' below.

Privacy Act 1988

The *Privacy Act 1988* (Privacy Act) establishes obligations on private and public sector organisations for collecting, using or disclosing personal information. As the AIHW is subject to the Privacy Act, in addition to the AIHW Act, it is 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.

Importantly, both Acts recognise the importance of data being made available for the purposes of research which benefit the community. In both cases, subject to certain requirements and considerations, the AIHW Ethics Committee may authorise:

- pursuant to section 95 of the Privacy Act, the release of personal information for medical research that would otherwise be a breach of a privacy principle in the Act; and/or
- the release of health-related or welfare-related information that would otherwise be prohibited by section 29 of the AIHW Act.

Freedom of information

All documents held by the AIHW are potentially subject to access by members of the public under the freedom of information provisions of 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.

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 at http://www.aihw.gov.au/ips/>.

Compliance with FOI Act requirements is overseen by the Freedom of Information Commissioner in the Office of the Australian Information Commissioner. More information on FOI is available here <http://www.oaic.gov.au/freedom-of-information/freedom-of-information>.

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. 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.

Other legislative, contractual and governance obligations

The AIHW has traditionally adopted a strongly collaborative approach to its work, developing relationship networks with Australian, state and territory governments and with the education and private sectors. This is reflected in the AIHW's formal arrangements with other organisations, in national information agreements and the AIHW's active participation in numerous national committees.

The purpose of national information agreements is to support the availability of nationally-consistent, high-quality data and to promote the efficient, confidential and timely use of data shared under them. The agreements set out national information infrastructures, outline processes for data development and data sharing and underpin the development and provision of National Minimum Data Sets to the AIHW. National information agreements current at the time of finalising this Framework include:

- National Health Information Agreement (NHIA) 2013 – through which the Commonwealth, states and territories will develop agreed programs to improve, maintain and share national health information;
- National Housing and Homelessness Information and Infrastructure Agreement (NHHIIA) – which confirms and supports the national infrastructure and processes needed to integrate, plan and coordinate the development of consistent national housing and homelessness information;
- National Community Services Information Infrastructure Agreement – which confirms and supports the national infrastructure and processes needed to integrate, plan and coordinate the development of consistent national community services information; and
- National Information Agreement on Early Childhood Education and Care (NIAECEC) – which aims to ensure the availability of a national information base for early childhood education and care - policy, programs, reporting requirements.

Participating in, and undertaking activities under, bi-lateral and multilateral agreements and committees means that the AIHW must consider the related data and information implications. For example:

- changes or refinement in areas of focus for data collection activities;
- Commonwealth, state and territory legislation applicable to use of specific types of data; and
- conditions and caveats regarding use, disclosure and release of data in contracts and memorandums of understanding.

AIHW structures and roles in data governance

AIHW Board

Governance of the AIHW is vested in a Board established under section 4 of the AIHW Act, and subject to the general oversight of the Minister. Membership of the Board is prescribed by section 8 of the AIHW Act.

The Board's functions are listed in section 5 of the AIHW Act. Its data-related functions include:

- the collection and production (and coordination of the collection and production) of health and welfare-related information and statistics
- the development, in consultation with the Australian Bureau of Statistics, of specialised statistical standards relevant to health and welfare services, and
- (subject to section 29 confidentiality requirements) enabling researchers to access health and welfare-related information and statistics held by the AIHW or associated bodies.

The powers of the Board, specified in section 6 of the Act, include the power to release data to other bodies or persons. The Board has delegated this function to the AIHW Director in its Instrument of Delegation dated 25 March 2010.

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 Director.

Ethics Committee

The AIHW Ethics Committee plays a central role in AIHW's data governance arrangements. The Committee is established under section 16(1) of the AIHW Act. The membership composition and functions of the Committee are prescribed in the *AIHW Ethics Committee Regulations 1989*.

The key prescribed functions of the Ethics Committee, from a data governance perspective, are 'forming an opinion, on ethical grounds, about the acceptability of, and to impose any conditions that it considers appropriate on:

- activities that are being, or are proposed to be engaged in by the AIHW in the performance of its functions;
- activities that are being, or are proposed to be, engaged in by other bodies or persons in association with, or with the assistance of the Institute in the performance of its functions; and
- the release, or proposed release, of identifiable data by the AIHW for research purposes; having regard to any relevant ethical principles and standards formulated or adopted by the National Health and Medical Research Council and to any other matters that the Ethics Committee considers relevant.'

Based on these functions, the Committee has determined that any AIHW work that involves one or more of the following activities must be approved by the Committee:

- any work requiring the use of identifiable data;
- any work requiring data linkage (as linkage of two different data sets may cause the creation of identifiable data);
- new surveys and changes to existing surveys;
- creation of a new data set, provided that critical ongoing collections will be audited from time to time; and
- amending the scope of existing collections.

From a data governance perspective, 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.

Further information about the AIHW Ethics Committee process, including Committee members, meeting dates, on-line application forms for project approval and a list of approved projects may be found here < www.aihw.gov.au/ethics/ >.

AIHW Director

Section 18(1) of the AIHW Act provides the AIHW Director 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 Director'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
- ensuring the security of data provided to the AIHW, and protecting confidentiality and privacy in accordance with legislation and ethical standards.

As indicated above, the Board has delegated a number of powers to the Director, including the power to release data to other bodies or persons. The Director's powers in relation to this, and a range of data governance responsibilities, have been delegated to data custodians by the AIHW Data Custodianship Delegations.

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

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 Audit and Finance Committee is one such committee, comprised of three non-executive members of the AIHW Board and one independent member. The Committee authorises and oversees the AIHW's audit program and reports to the Board on strategic, financial and data 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.

Executive Committee

The Executive Committee, which comprises the Director and AIHW Group Heads, supports the Director 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 Director, who considers advice provided by the Executive Committee.

Data Governance Committee

At the time of finalising this Framework, the Executive Committee has recommended the establishment of a Data Governance Committee (DGC) on the following terms:

- the DGC will report to the Executive Committee and make recommendations in relation to data governance and data-related matters; for example recommending for approval reviewed or new data policies and guidelines, including annual reviews of this Framework;
- for the first 12 months of its operation, the DGC will meet every two months, following which a review/assessment of its operations will be conducted; and
- membership will comprise a maximum of four Senior Executives and three Unit Head level staff.

Data Custodians

An AIHW data custodian is a staff member with delegation from the AIHW Director (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, with the power to release data to other bodies or persons. 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.

Security

The Australian Government Protective Security Policy Framework (PSPF) prescribes several key security roles, including the Security Executive (a member of the Senior Executive Service, responsible for the agency protective security policy and oversight of protective security practices) and an Agency Security Adviser (ASA, responsible for the day-to-day performance of protective security functions). In AIHW, the role of Security Executive is performed by the Head of the Business and Governance Group and the role of ASA is performed by the Facilities Manager.

Another role prescribed by both the PSPF and the Australian Government Information Security Manual, which governs the security of government ICT systems, is the Information Technology Security Adviser (ITSA). The roles of Information Technology Security Manager (ITSM) and Information Technology Security Adviser (ITSA) have been assigned to the Unit Head, ICT Operations. The ITSM is responsible, amongst other things, 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. The ITSA role encompasses ITSM functions and is also the first point of contact on these issues within the agency and for external agencies. Where there is more than one ITSM, the ITSA is also responsible for coordinating ITSM activities.

Importantly, as identified in the AIHW Security Risk Management Policy, effective security risk management is a core requirement of *all* AIHW personnel and contractors.

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 Part, adherence to relevant Australian and international standards and classifications, and compliance with ethical considerations and obligations under contracts, agreements and external governance arrangements. They 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.

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

Data acquisition

The AIHW Information Security and Privacy Policy and Procedures establish requirements regarding information gathering and receipt, including:

- information may only be collected and held for the purpose of AIHW activities (that is, for purposes consistent with the AIHW Act);
- identifiable information may only be collected and held with the approval of the Institute's Ethics Committee;
- any information collected must be limited to that directly relevant to the aims and objectives of an approved project;

- subject to specific exceptions, consent from information subjects for the use of their information should be obtained if identified records are to be held indefinitely on registers for the purpose of contacting those persons for research purposes; and
- all research involving identifiable information must be approved by the Ethics Committee. If consent has not been obtained for use of the information in the context sought, the Committee will consider a range of factors consistent with its functions under the AIHW Ethics Committee regulations and its practice documentation. More information on the Ethics Committee is available on the Ethics Committee page on the AIHW website and in the AIHW Ethics Committee Background and Practice document.

The Guidelines for the custody of AIHW data require, amongst other things, the relevant data custodian to record the details of each new or significantly changed data holding in the data catalogue. The type of information that must be entered into the catalogue are described under the data catalogue entry in the 'AIHW systems and tools to support data governance' section below.

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.

Data management

Access

AIHW procedures regarding secure use of ICT systems provide the first level of data access management. These procedures 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's Information Security and Privacy Policy and Procedures and Guidelines for the custody of AIHW data also detail requirements and processes relating to access to data and information by Institute staff.

Requirements for access to data under data-sharing agreements are specified in those agreements and are at all times subject to compliance with legislative obligations. Information regarding ad hoc requests for data 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.

Storage and security

The AIHW logically and physically 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 Risk Management Policy describes the AIHW's approach to managing security risks. It also identifies specific delegations for security-related roles required by Australian Government protective security policies, including the Security Executive, Agency Security Adviser (ASA) and Information Technology Security Adviser (ITSA).

The AIHW Information Security and Privacy Policy and Procedures and Guidelines for the Custody of AIHW Data impose a range of requirements relating to:

- compliance with directions from the AIHW management and directives given by the data providers 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.

The Data Linkage and Protecting Privacy policy provides additional guidance on access to, and storage of, linked datasets. The protection of data confidentiality is also explicitly recognised as one of the primary objectives of the Institute's physical security policy.

The AIHW Secure Messaging User Guide and procedures provide information and specify requirements for transmitting information securely, including the use of encryption.

Collaborating centres of the AIHW are given specific guidance on the secure use, handling and storage of AIHW data.

Privacy

The Privacy Act 1988 regulates the handling of personal information by Australian Government agencies. A range of AIHW policies, guidelines and procedures contain requirements reflecting obligations under the Act. In particular, the AIHW Privacy Policy, and two brochures *Safeguarding your privacy* and *Privacy at the AIHW* published on the AIHW website <www.aihw.gov.au> outline our approach to privacy matters, provide guidance on complaints, and list contact details for the AIHW's Privacy Officer.

In addition to its Privacy Act obligations, the AIHW is subject to a confidentiality provision in section 29 of the AIHW Act. Further information on confidentiality is provided in the section 'Release' below.

Data linkage

The AIHW is one of only two 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) high level principles for data integration involving Commonwealth data for statistical and research purposes and best practice guidelines. 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 the AIHW Ethics Committee Guidelines for the Preparation of Submissions for Ethical Clearance.

As an accredited Integrating Authority the AIHW applies best standard protocols. A key aspect of best practice data linkage is the separation principle, a set of data management practises that ensures privacy by the separation of identifying data and content data. For high-risk projects involving Commonwealth data, the AIHW ensures privacy and data control are enhanced by only linking data for particular projects (or families of projects). 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 providers that their data are being appropriately secured, managed and used.

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; or
- in Canberra via the AIHW's secure data lab – a locked room within DISC that requires authorised entry.

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 is again vetted to ensure the data is 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 is overwritten on a 4-weekly cycle. Data is encrypted as part of the archival process.

The 'data linking' page of the AIHW website contains more information on data linkage, including:

- contact details for the DISC
- current and past data integration projects
- a video on the data integration process; and
- information on how to link data.

Quality

The AIHW's approach to data quality is outlined in the ICT Strategic Plan 2011–14 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 providers 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 in to the data submission process that notify data providers of potential errors in the data.

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 manual, 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 is reviewed as per the AIHW's Publications Review Policy. 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.

Release

AIHW data custodians bear the responsibility for making decisions about the release to third parties of data held in collections for which they are accountable. In exercising this function, data custodians must take into account a range of considerations.

For example, consistent with the AIHW's functions as described in the AIHW Act and the AIHW Work in the Public Domain Policy Statement, as a general policy all aggregate (non-identifiable) AIHW data are placed in the public domain. Subject to limited exceptions, data produced under contract with external agencies are also made publicly available. The AIHW also has policies and procedures in place regarding processes for confidentialising data that would otherwise be identifiable, so that the identity of individuals is protected whilst maximising the amount of data that may be publicly released. Information on these matters

is contained in the AIHW Policy on Reporting to Manage Confidentiality and Reliability and in *Statistics for the AIHW*.

The release of identifiable data for the purposes of research must be consistent with section 29 of the AIHW Act, a confidentiality provision for which a breach comprises an offence punishable by fines and/or imprisonment. Release of identifiable data must also be approved by the AIHW Ethics Committee, consistent with its functions under the AIHW Act, AIHW Ethics Committee Regulations and the Privacy Act.

Data archiving, return and destruction

In accordance with the AIHW Information Security and Privacy Policy and Procedures, decisions regarding retention of data collections lies with Data Custodians, and must be taken in accordance with the Institute's Guidelines for the Custody of AIHW Data. The Guidelines provide that:

- data collections must normally be retained for a specified period in order to allow later verification of the research and in accordance with undertakings given to data providers. Also, electronic records may need to be retained so that future surveys can undertake comparative analyses. At the time of approving the establishment of data collections, the Ethics Committee either endorses proposed data retention periods or stipulates alternative data retention requirements;
- when a data holding is no longer used, and is being held only to meet retention requirements, data custodians should review the access privileges of all users and mark the data holding as 'inactive'; and
- the destruction of data collections must be in accordance with National Archives of Australia (NAA) policies for managing records. The National Archives of Australia (National Archives on keeping-destroying-transferring data) provides the following information on data destruction: 'Once records are no longer needed for business, you need to decide whether they should be kept, destroyed or transferred. 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*.'

The AIHW Record Keeping and Filing Guidelines provide more information on the retention of records and contains links to NAA information. Data archiving and destruction methods specific to the AIHW's Data Integration Services Centre (DISC) are described in the 'Data linkage' section on page 15 of this Framework.

AIHW systems and tools to support data governance

ICT systems

The AIHW's Secure Use of ICT Systems procedures provide a multi-tiered system of data governance with regard to security and auditability. In particular, access is separately restricted at the network, data server and database level requiring individual authorisation and centralised (through ICT Operations) access management.

The ICT Strategic Plan 2011–14 identifies the need to "consolidate and implement a single source of truth" to better manage data quality through the development and implementation of single repositories of data, metadata, validation rules, SAS codes and reference data.

Streamlined production

The AIHW's updated standard architecture and data access process provides more formal and easily auditable systems of data access and use. In particular, data access expiry is automated, analysis files are stored and managed in a more uniform and transparent

manner, and data custodians have greater visibility of access to their holdings. This updated process addressed a weakness previously identified in the ICT Strategic Plan i.e. that data storage was not centralised.

AIHW data catalogue

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

The Data Catalogue performs two key functions. It:

- identifies past and present data custodians for each AIHW data collection. Data custodians listed in the data catalogue are, by virtue of the Director's AIHW Data Custodianship Delegations, vested with the data custodianship responsibilities listed in the Guidelines for the Custody of AIHW Data; 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 identifies related datasets in METeOR.

A limited public version of the Data Catalogue is available on AIHW's Internet site here.

METeOR

METeOR is Australia's repository for national metadata standards for the health, community services and housing assistance sectors. The system was developed by the AIHW to replace the previous repository, the Knowledgebase. METeOR provides online access to a wide range of nationally endorsed data definitions and tools for creating new definitions based on existing already-endorsed components.

METeOR operates as a metadata registry, that is, a system or application where metadata is stored, managed and disseminated. The registry aspects of METeOR are based on the international standard for metadata registry - ISO/IEC 11179.

Through METeOR users can find, view and download over 2,600 data standards. METeOR also provides powerful search and metadata creations facilities to help users find metadata quickly, or to create quality metadata and have them endorsed. All these services are available free of charge.

Validata™

The AIHW's Validata™ is a system that assists data providers to check and validate their data submissions against a set of validation rules to ensure that their data is of the highest possible quality. It enhances business processes and data management and applies data policies through to checking and validation. Data providers may validate their data as many times as they wish before formally submitting it to the AIHW. 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. *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.

Data requests

The AIHW's data request database holds a standard set of information about each request from the public for new (unpublished) analysis, including an electronic record of the clearance process and a copy of the data as transmitted to the client. By incorporating role-based clearance steps, the application supports the AIHW's policies on data custodianship and data release.

ASM

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.

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 Governance 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 it approved in 2013. The audits occur as part of the AIHW's internal audit program and their outcome are also reported to the 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 providers (for example, under conditions specified in data supply agreements) and by statutory office holders, such as the Australian Information Commissioner.

Work is presently under way to combine the register of data collections approved by the Ethics Committee with the data catalogue to provide a comprehensive list of AIHW collections.

Breaches and sanctions for breaches of information security/confidentiality

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.

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 an offence.
- If a breach is thought to have occurred, it must be reported immediately to the Director through normal management reporting channels.

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

Dealing with complaints

The AIHW Privacy Policy, and two brochures *Safeguarding your privacy* and *Privacy at the AIHW* published on the AIHW website <www.aihw.gov.au> provide 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 Freedom of 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 officer.

The Charter of Corporate Governance provides guidance on the management of complaints about Board members. The AIHW Ethics Committee Background and Practice document provides guidance on the management of complaints made in respect of the Committee's functions.

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 Director for management/action in or by the appropriate forum.

Review and feedback

As data governance and data management should be reviewed regularly to ensure that existing arrangements reflect contemporary relationships, practices and available technology, this Framework will be considered for currency and accuracy on a yearly basis. This function will be undertaken by the Data Governance Committee during its last scheduled meeting of each year.

Questions and comments

AIHW staff should direct questions regarding the Framework, or suggestions for inclusions or enhancements, to the AIHW Governance 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.

Attachments

1. Acronyms and Definitions
2. Alphabetical list of Acts, policies and guidelines contained in this Data Governance Framework

Attachment 1

Acronyms and definitions

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

AIHW	means the Australian Institute of Health and Welfare
AIHW Act	means the *Australian Institute of Health and Welfare Act 1987* (Cth)
AIHW Ethics Committee	means the committee established under section 16(1) of the *Australian Institute of Health and Welfare Act 1987* (Cth), with a membership prescribed in the Australian Institute of Health and Welfare Ethics Committee Regulations 1989
Archiving	means 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	means resources under the control of a person or entity that have recognised value
Data	means factual information used as a basis for reasoning, discussion or calculation
Data catalogue	means the AIHW data catalogue (formerly known as Data Hound), which is the official listing of AIHW's data collections
Data collection	means a cohesive set of data with measurable value that is designed to address a specific set of business needs
Data custodian	means a staff member with delegation from the AIHW Director 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. The data custodian for a particular data collection is listed in the data catalogue entry for that collection.
Data governance	means "…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."[7]
Data management	is "the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets."[8]
FOI	means freedom of information
FOI Act	means the *Freedom of Information Act 1982* (Cth)

[7] Data Governance Institute, http://datagovernance.com/adg_data_governance_definition.html , accessed 22 January 2014.

[8] http://www.dama.org/files/public/DI_DAMA_DMBOK_Guide_Presentation_2007.pdf

Identifiable data	Data from which a person's identity may reasonably be ascertained. Of relevance to data at AIHW, 'person' is defined more broadly in the AIHW Act and includes deceased persons and bodies corporate.
'information concerning a person'	means information from which the identity of a person could be reasonably ascertained. Release of this information in a manner other than as permitted by s. 29 of the AIHW Act is an offence.
metadata	means a structured description of the characteristics of specified data, including its content, quality and format.
Personal information	as defined in the *Privacy Act 1988*, means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
Privacy Act	means the *Privacy Act 1988* (Cth)

Attachment 2

Alphabetical list of 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 1989

Freedom of Information Act 1982

Privacy Act 1988

External policies and standards

Australian Government Information Security Manual

Australian Government Protective Security Policy Framework

Australian Public Service Code of Conduct

High level principles for data integration (Cross Portfolio Statistical Integration Committee)

AIHW corporate documents, policies and guidelines

AIHW Ethics Committee background and practice document

Charter of Corporate Governance

Data Collection Management Principles

Data Custodianship Delegations

Data linkage and protecting privacy policy

Data Quality Statements policy and guidelines

Delegations

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

Guidelines for the custody of AIHW data

Guidelines for the Preparation of Submissions for Ethical Clearance

Information Security and Privacy Policy and Procedures

Instrument of Delegation dated 25 March 2010 (delegates powers of the Board to the Director)

ICT strategic plan 2011–14

Physical security policy

Policy on reporting to manage confidentiality and reliability

Privacy Policy

Publications Review Policy

Secure use of ICT systems procedures

Secure messaging user guide and procedures

Security Risk Management Policy

Statistics for the AIHW

Strategic Directions

Work in the Public Domain Policy Statement

AIHW repositories, tools, systems and fact sheets

AIHW data catalogue

AIHW data catalogue (public version)

AIHW data request application

AIHW Ethics Committee – annual (routine) monitoring report

AIHW Ethics Committee - final monitoring report

EthOS™

METeOR

Privacy at the AIHW

Safeguarding your privacy

Validata™