Illawarra Shoalhaven Local Health District

Data Governance Framework

July 2021

VERSION CONTROL:

September 2017: Version 1 - endorsed at strategic executive comm

June 2018: Version 2 - includes updates in line with NSW Health Procedure *NSW Health PD2018_001 Disclosure of unit record data by Local Health Districts for research or contractor services*

Contents

INTRODUCTION 3
Data Versus Information 3
Data Governance in ISLHD 3
Framework Overview 4
Data Users 5
DATA GOVERNANCE CONCEPTS 7
ISLHD DATA ROLES & RESPONSIBILITES 10
Data Relationships 11
ISLHD DATA REQUEST PROCESSES 14
LEGAL AND REGULATORY COMPLIANCE 20
Record Management, Collection & Reporting 21
Privacy 21
Common Law & Professional Obligations 22
Policies, Procedures and Guidelines 23
NSW ICT Strategy 23
FRAMEWORK & POLICY COMPLIANCE 24
APPENDIX 1: Consultation process for Data Governance Framework & Policy 25
APPENDIX 2: Data Request Process for External Organisation in Partnership with ISLHD 26
APPENDIX 3: Government Department or Organisation in Partnership with ISLHD External Data Request Form 27
APPENDIX 4: Procedure for response to a breach of conditions by a researcher or contractor following disclosure of unit record data (from the NSW Health breach procedure) 30
APPENDIX 5: Data Concepts Table 32
APPENDIX 6: Data Role and Responsibilities table 43
APPENDIX 7: List of Legislation, Policies and Guidelines 47
□ *Collection (1. Lawful, 2. Direct, 3. Open, 4. Relevant)* 51
□ *Storage (5. Secure)* 51
□ *Access and accuracy (6. Transparent, 7. Accessible, 8. Correct)* 51
□ *Use (9. Accurate, 10. Limited)* 51
□ *Disclosure (11. Restricted, 12. Safeguarded)* 51
APPENDIX 8: Reference List 57

INTRODUCTION

Data Versus Information

There are subtle differences between data and information. **Data** are the facts or details from which **information** is derived. Data and information are interrelated. In fact, they are often mistakenly used interchangeably.

	Data	***Information***
Meaning	*Considered to be raw data plain facts.* *Represents 'values of qualitative or quantitative variables, belonging to a set of items.' It may be in the form of numbers, letters, or a set of characters. It is often collected via measurements. Data is represented in a structure, such as tabular data.*	*The message that is being conveyed.* *Once the data is processed, organised, structured or presented in a given context, it can become useful. Then data becomes information, knowledge.*
Examples	*Each patient's presentation to the Emergency Department is one piece of data.*	*The average number of Emergency Presentations each day is information that can be derived from the data.*
	The amount each employee is paid is one piece of data.	*The total organisational budget for Human resources is information that can be derived from the data.*

This Framework only governs Data associated with the Illawarra Shoalhaven Local Health District's (ISLHD) Population or Health Services, with an emphasis on the associated issues around Quality, Integrity, Privacy and Security of this data. There are other governance structures in place for the management and dissemination of information across the Illawarra Shoalhaven Local Health District (ISLHD). This Framework is also in line with NSW Ministry of Health Data Governance concepts as outlined in http://internal.health.nsw.gov.au/data/governance/index.html.

Data Governance in ISLHD

Data governance is the overall management of data owned and managed within the organisation. It is critical for promoting data quality, integrity, privacy and security. It also identifies clear roles and responsibilities in relation to data.

Data Quality	**Data Integrity**	**Data Privacy**	**Data Security**

This Framework and corresponding policy have been created to:

- develop best practices for effective data management
- improve the quality and consistency of data
- reduce the risk of internal and external breaches of privacy and confidentiality, and
- maximise the value and integrity of data within ISLHD

It ensures adequate processes are in place to effectively retrieve report, manage and store data.

The Framework and corresponding Policy apply to all entities in ISLHD. They apply to all ISLHD staff, contractors and partners and govern both clinical and corporate data. These documents address governance in the context of State policies, guidelines and the broader system.

Framework Overview

This Framework:

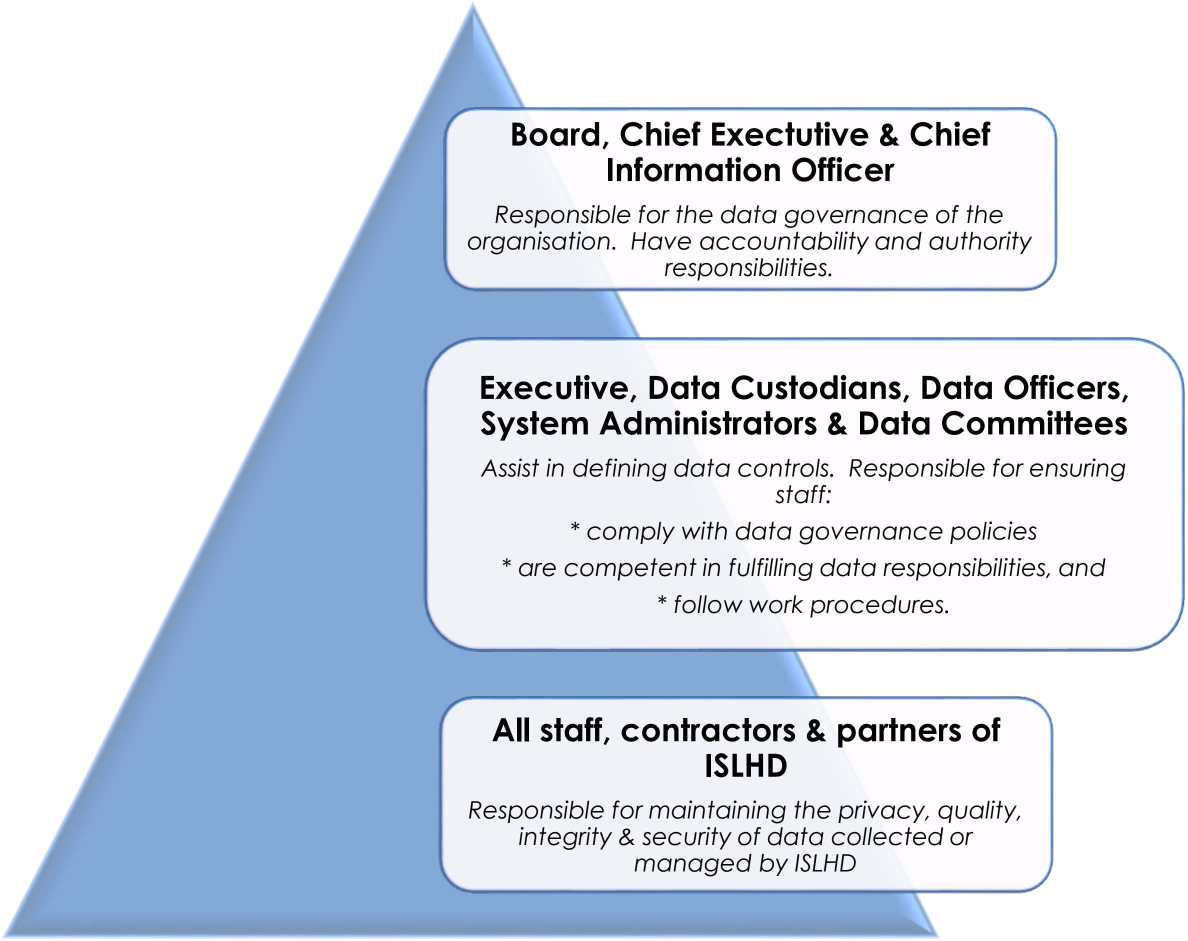
- describes key data governance concepts
- defines data users and their roles and responsibilities
- demonstrates the structure, systems and tools that are in place to support data governance
- references the organisation's legal and regulatory requirements
- outlines relationships between ISLHD and external entities when electronic access to de-identified data are required

These arrangements apply to data:

- collected and/or managed by ISLHD
- collected on ISLHD's behalf (for example under collaborative or sub-contractual agreements)
- obtained from external sources that are stored on District systems. In this instance the governance activities are undertaken in conjunction with the governance of the external body

Data Users

All employees, contractors and partners are data users within ISLHD. The principles and requirements in this document are therefore relevant to all staff. The ways in which data are used, and the responsibilities that staff have over data, vary across different corporate and clinical roles. The diagram below shows the types of data users.



Board, Chief Exectutive & Chief Information Officer

Responsible for the data governance of the organisation. Have accountability and authority responsibilities.

Executive, Data Custodians, Data Officers, System Administrators & Data Committees

Assist in defining data controls. Responsible for ensuring staff:

** comply with data governance policies*

** are competent in fulfilling data responsibilities, and*

** follow work procedures.*

All staff, contractors & partners of ISLHD

Responsible for maintaining the privacy, quality, integrity & security of data collected or managed by ISLHD

THREE KEY PRINCIPLES

The following three principles summarise the approach in which all staff need to take when collecting, using and storing data. All staff will be:

Responsible

- only access data relevant to their job
- always de-identify data, unless otherwise required
- comply with privacy legislation, confidentiality policies and de-identification processes.
- comply with any exisiting labelling standards

Accountable

- clearly record how and when data-related decisions and controls are made
- take practical steps to safeguard data from unauthorised or accidental use
- notify appropriate managers if they see the misuse of data
- ensure data are circulated in an appropriate manner, suitable to the intended audience, considering potential risks

Accurate

- ensure that data are collected and entered accurately
- ensure any data extracted, analysed or presented are checked and validated for reliability, accuracy and consistency
- ensure data are standardised, with consistent and common definitions to facilitate information sharing

DATA GOVERNANCE CONCEPTS

An understanding of the terms and concepts of data governance is important. It allows a standardised approach across the District. A short description of these has been provided below. Additional information, including examples and key reference documents can be found in Appendix 4.

Data Type	**Clinical Data** **Aggregated data:** consolidated data relating to multiple individuals. **Unit record data:** records of data that relate to the health of an individual. **De-identified data:** data about a person whose identity is not apparent and cannot be reasonably ascertained. **Identifiable data:** Personal, unique identifying data eg. name, address, age, date of birth, ethnicity or diagnosis. It can also be a combination of data that allows a person's identity to be "reasonably ascertained". **Corporate Data** Data about how the organisation is managed including its Finance, Human Resources and Records Management. This may or may not be of a sensitive nature.
Data Collection	The ongoing, systematic collection of clinical and corporate data. It allows a person to record, analyse, review, report, evaluate, monitor and disseminate data. In this framework it refers to data where ISLHD has explicit ownership. The methods of data collection vary by discipline. The ICT Systems Catalogue of all ISLHD systems can be obtained from the Chief Information Officer.
Data Quality	Data quality reflects the extent to which data are: • Complete: extent to which data fields have been entered/filled in. • Accurate: The degree to which data are correct in all details. • Unique: no duplication • Valid: the strength of data and whether it accurately describes the real world. • Consistent: done in the same way over time • Timely: The degree to which data represent reality • Objective and complies with known standards.
Data Use	In general terms, the 'use' of health data refers to the communication or handling of data. It is an assumption that when using data, the quality will be checked using the principles of data quality.
Data Analysis	The process of developing answers to questions by examining and interpreting data.

Data presentation

The method by which people summarize, organize and communicate data. They will use a variety of tools such as tables, diagrams, charts, histograms and graphs.

It is an assumption that when preparing data for presentation, the quality will be checked using the principles of data quality.

Data Dissemination

The act of spreading/circulating data widely.

It is important that this data meets ISLHD's quality standards. Eg. de-identified if being disseminated outside ISLHD.

The audience needs to be identified to determine the level of detail.

Data Disclosure

The selective release of data that relates to the health of an individual / group.

Disclosure should comply with legislation, be in line with ethical standards, and be approved prior to disclosure.

Data Access

Activities related to storing, retrieving, or acting on data housed in a database or other repository.

Data Security Management

Ensures privacy, confidentiality and appropriate access of data.

Effective data governance protects the security of sensitive and personally identifiable data. It also mitigates the risks of unauthorised disclosure of the data.

A key purpose of the framework is data security management.

Data Warehousing

A centralised electronic storage of multiple data collections. It is specifically designed for data analysis, generating reports and for other ad-hoc queries.

A data warehouse gathers data from different sources and converts it into a single and widely used format – thereby standardising the data.
Warehoused data must be stored in a manner that is secure, reliable, easy to retrieve and easy to manage.

Metadata

The structured description of the characteristics of data, including its content, quality and format. It provides a shared meaning, allows comparisons, and makes it easier to retrieve, use and manage data resources.

Data Definitions

Provides context and a written description for a data element or collection of data within a database or manual data collection. It is a component of metadata or a data dictionary.

Data Dictionaries

A resource that provides standard descriptions and definitions in relation to data collection. It may describe the content, format and structure of the collection and any relationships between data elements or data collections.

Data dictionaries and metadata serve a similar function. They provide a centralised resource to assist users to better understand data they are working with.

Data Request

The process of asking for data or applying for access to data. The data can be from an internal source or an external organisation.

Data Linkage

The joining of data from two or more records that relate to a common entity, e.g. individual, family, event or address. This can involve linkage of records within a single data collection or across two or more different sources.

When joining together pieces of data that belong to the same person, such as common identification and/or demographic fields.

Under the Health Records and Information Privacy (HRIP)Act 2002, a health records linkage system refers to a computerised system that is designed to link health records for an individual held by different organisations.

Data Storage

The practice of storing electronic data. This can be done in a variety of ways:

- online, whether locally on an agency server, or by hosted storage through the internet (eg cloud storage).
- In off-line storage on removable media (eg. CDs, USB sticks).
- Hard copy

Data Back-up

The activity of copying **files** or **databases** so that they will be preserved in case of mainframe / equipment failure or other catastrophic events.

Data Retention

The process of identifying how long records should be retained.

Data Archiving

The appropriate storage of data to safeguard and preserve records. This allows people to discover, use, and learn from this documentation. It also ensures continued access to this data.

Data Disposal

Electronic Data

Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless data.

Destruction of electronic media is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic data

Clearing data such as formatting or deleting data removes data from storage media in a manner that renders it unreadable

Paper Based Records

There are a number of ways in which paper based records can be disposed of. These include:

- Shredding
- Pulping

The disposal of any State record should be done in accordance with the NSW State Records Act.

ISLHD DATA ROLES & RESPONSIBILITES

Clarity around roles and responsibilities for all staff across the District is important. When staff understand what their role is, and how it relates to others, the Organisation can support and better manage good data governance and security. A short description of the roles is provided below. Additional information, including examples and key reference documents can be found in Appendix 5.

	Board	The Board has ultimate responsibility for the governance of the organisation.
	Chief Executive	Has authority and accountability under legislation, regulation, or policy for the collection, use, disclosure and storage of data. Can give delegation to a Tier 2 Executive to disclose data.
Data Sponsor	**Chief Information Officer**	Approves data governance and data management policies, and conducts an annual review of ISLHD's data governance.
	Executive	Undertake duties of ownership on behalf of the organisation. Ensure that all managers, staff and contractors comply with Data Governance Policies, and are trained and competent to fulfil their duties.
Data Custodian	**Senior Managers**	Manage a data collection system or have delegation to exercise overall responsibility for a data collection. Approve access to data and are responsible for the overall quality and security of the data.
Data Stewards	**Data Integrity Officer (DIO) / Data Manager**	Work with data custodians and data sponsors to define and control data. Responsible for the day to day operation of the data collection/asset, its completeness and quality.
	System Administrators	Are required to understand and follow acceptable procedures in managing the system, resolve known vulnerabilities, and monitor system access. Responsible for the upgrading of systems and archiving data contained within these systems.

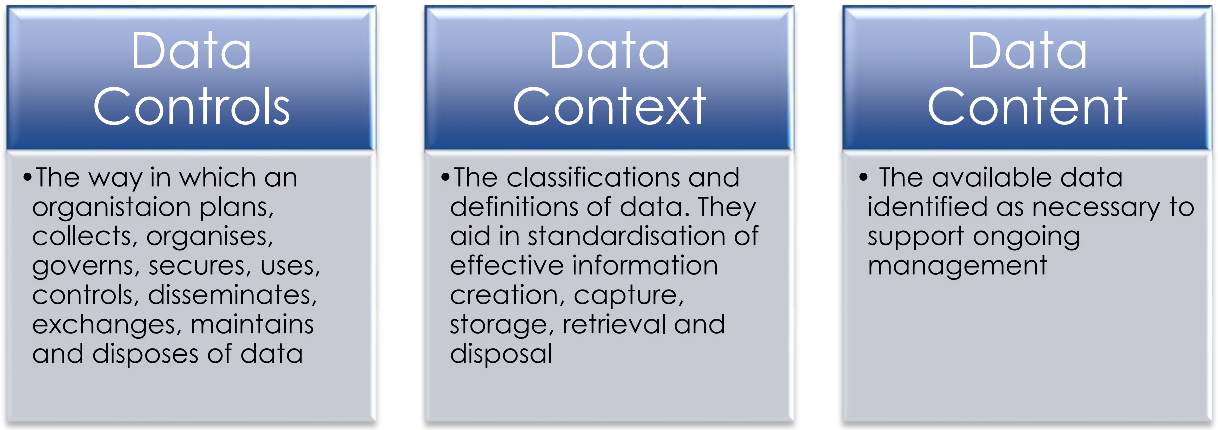
Data Users	**All Staff**	Have a duty to collect and maintain the privacy, quality, integrity and security of data held and managed by their Service / Division / Unit.

Committees	
ISLHD Committees	A range of ISLHD Committees support the District, Chief Executive & Executive to promote effective and efficient data governance.
Data Request Committee	Review internal and external data requests against criteria. Coordinate the approval, retrieval and dissemination of compliant data requests.
Audit & Risk Management Committee	Oversee and monitor ISLHD governance, risk and control frameworks in line with external accountability requirements

Data Relationships

The way data is managed can be categorised into three areas:

- Data Controls
- Data Context
- Data Content



Data Controls

- The way in which an organistaion plans, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains and disposes of data

Data Context

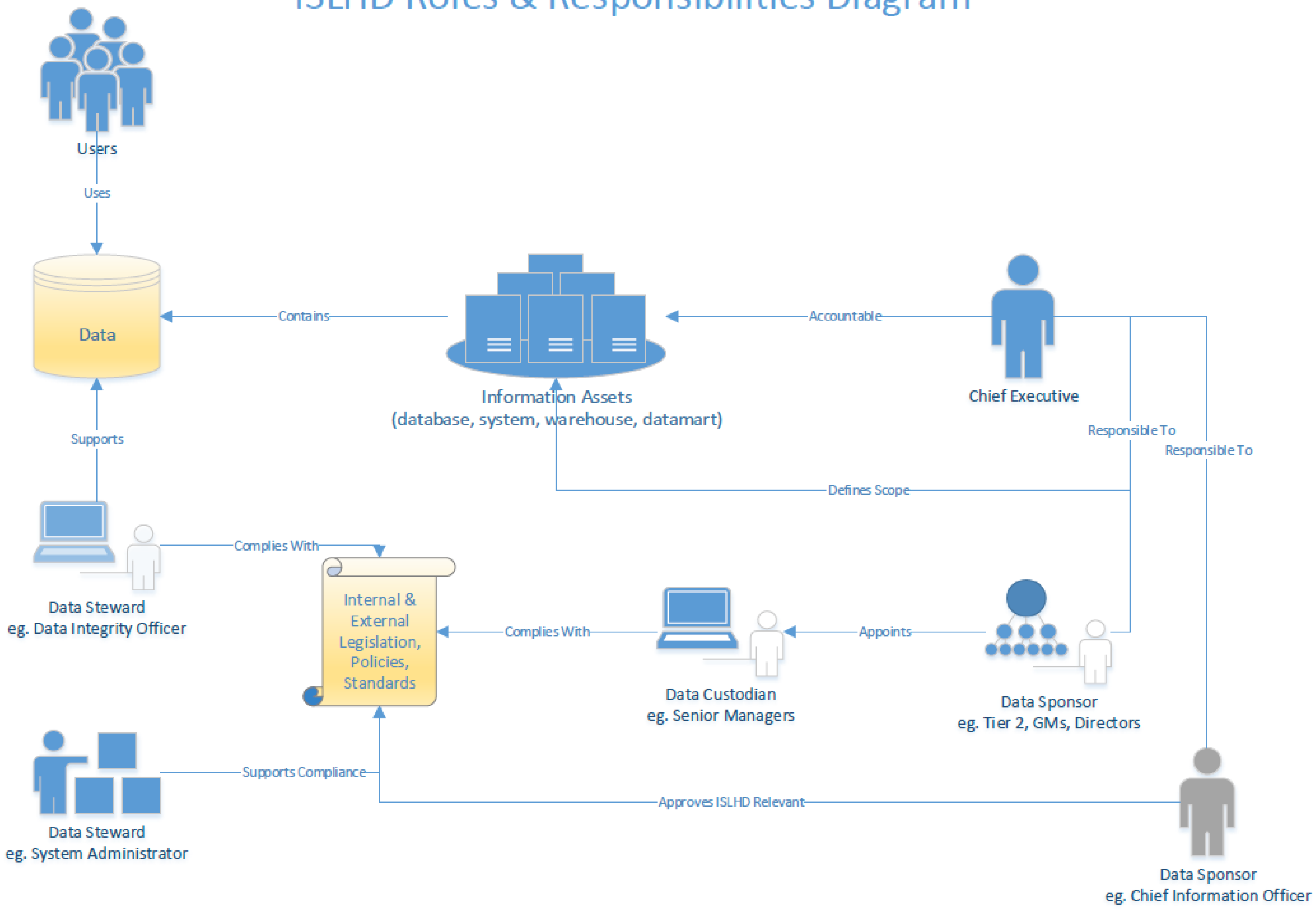
- The classifications and definitions of data. They aid in standardisation of effective information creation, capture, storage, retrieval and disposal

Data Content

- The available data identified as necessary to support ongoing management

The model for data governance is shown in the diagram below. Significant concepts or roles are expressed in the pictures, while relationships between the concepts are expressed as arrows.

ISLHD Roles & Responsibilities Diagram



ISLHD DATA REQUEST PROCESSES

The request for **<u>ISLHD population or health service data</u>** occurs frequently and can come from different sources. In order to ensure the Quality, Integrity, Privacy and Security of this population or service data across ISLHD is maintained, there are a number of processes in place to ensure the way in which ISLHD responds to these data requests is consistent. These requests can come from within ISLHD (Internal) or from external parties to ISLHD. In addition, ISLHD also has mandatory reporting requirements. The process in which data can be requested is described below:

- Internal
- External
- Mandatory Reporting

It should be noted that information sought by staff or external parties relating to personal health information, medical records, politically sensitive information, corporate information or complaints DO NOT fall under this Data Governance Framework. There are separate processes and governance arrangement to request this information (eg. GIPA, HRIPA, PPIPA, Subpoenas, 16A, Health Care Complaints).

Data Release and Security:

If the unit record data to be released should be de-identified, the data custodian should ensure that the data are released in such a way that minimises the chance of individuals being recognised:

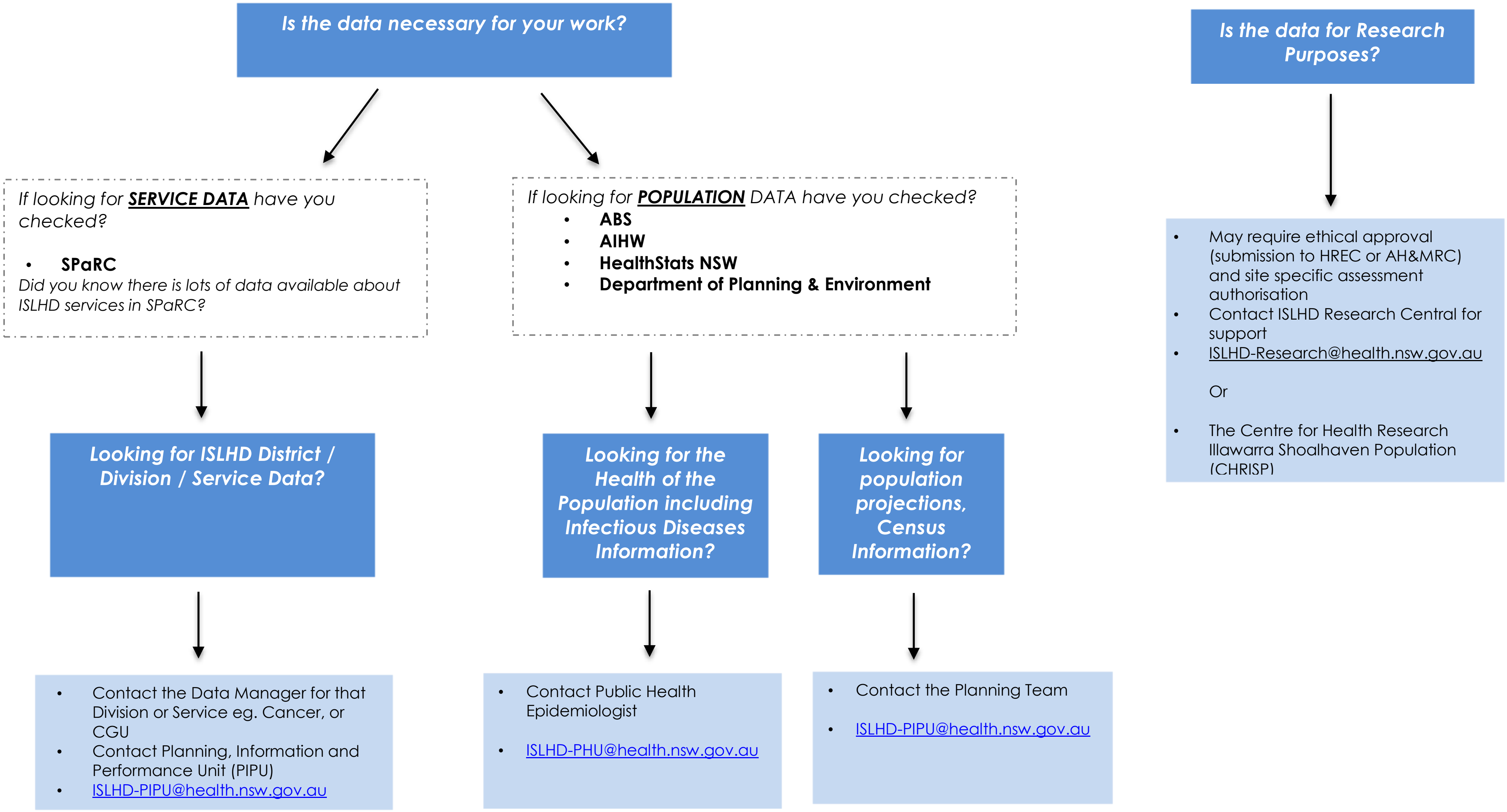
- Minimise the range of fields to be released
- Avoid the disclosure of dates. Eg, disclose age rather than date of birth, or length of hospital stay rather than date of admission.
- Grouping categories. Eg. age could be grouped into 5-year age groups
- Care should be taken when considering the disclosure of information concerning relatively small communities.

Data that are disclosed must be transferred using encryption technologies approved by the LHD. Accellion Secure File Transfer product is available for LHDs. Communication standards such as email and instant messaging are not considered secure and should be avoided in accordance with NSW Health Policy Directive Electronic Information Security Policy. Data that are disclosed must be stored by the recipient in a secure way. Acceptable secure storage includes physically secure file servers with universal password protection, or "strong" encryption software. Storage on portable media, laptops and desktop computer hard-drives is not acceptable. For more information, refer to NSW Health Procedure *NSW Health PD2018_001 Disclosure of unit record data by Local Health Districts for research or contractor services.*

Internal Data Requests

Staff within ISLHD require access to data to be able to do their job, and amount of data available is considerable. The diagram below describes the process in which ISLHD staff should follow when requesting data for work purposes.

Internal Data Requests Process Diagram



Is the data necessary for your work?

If looking for ***SERVICE DATA*** have you checked?

- **SPaRC**

Did you know there is lots of data available about ISLHD services in SPaRC?

Looking for ISLHD District / Division / Service Data?

- Contact the Data Manager for that Division or Service eg. Cancer, or CGU
- Contact Planning, Information and Performance Unit (PIPU)
- ISLHD-PIPU@health.nsw.gov.au

If looking for ***POPULATION*** DATA have you checked?

- **ABS**
- **AIHW**
- **HealthStats NSW**
- **Department of Planning & Environment**

Looking for the Health of the Population including Infectious Diseases Information?

- Contact Public Health Epidemiologist
- ISLHD-PHU@health.nsw.gov.au

Looking for population projections, Census Information?

- Contact the Planning Team
- ISLHD-PIPU@health.nsw.gov.au

Is the data for Research Purposes?

- May require ethical approval (submission to HREC or AH&MRC) and site specific assessment authorisation
- Contact ISLHD Research Central for support
- ISLHD-Research@health.nsw.gov.au

Or

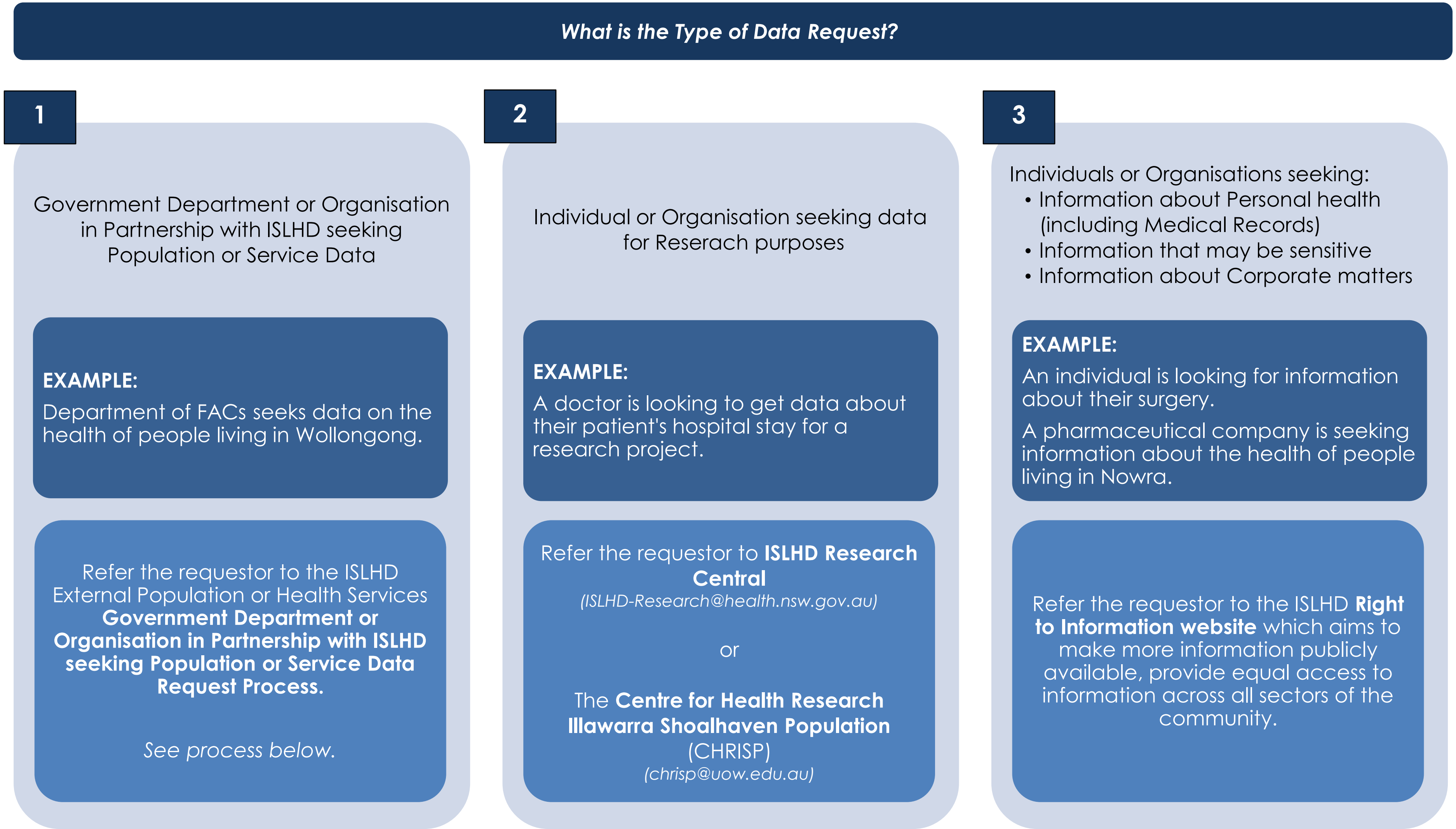
- The Centre for Health Research Illawarra Shoalhaven Population (CHRISP)

External Data Requests

Sometimes external organisations we work with (eg. Department of Families and Community Services or Primary Health Network) or individuals seek data that relates to the ISLHD population or health service data. There are a number of processes in place to ensure the way in which ISLHD responds to these external data requests is consistent.

The diagram below describes what data can be released by ISLHD to external organisations / individuals.

External Data Requests Process Diagram



What is the Type of Data Request?

1

Government Department or Organisation in Partnership with ISLHD seeking Population or Service Data

EXAMPLE:

Department of FACs seeks data on the health of people living in Wollongong.

Refer the requestor to the ISLHD External Population or Health Services **Government Department or Organisation in Partnership with ISLHD seeking Population or Service Data Request Process.**

See process below.

2

Individual or Organisation seeking data for Reserach purposes

EXAMPLE:

A doctor is looking to get data about their patient's hospital stay for a research project.

Refer the requestor to **ISLHD Research Central**

(ISLHD-Research@health.nsw.gov.au)

or

The **Centre for Health Research Illawarra Shoalhaven Population** (CHRISP)

(chrisp@uow.edu.au)

3

Individuals or Organisations seeking:

- Information about Personal health (including Medical Records)
- Information that may be sensitive
- Information about Corporate matters

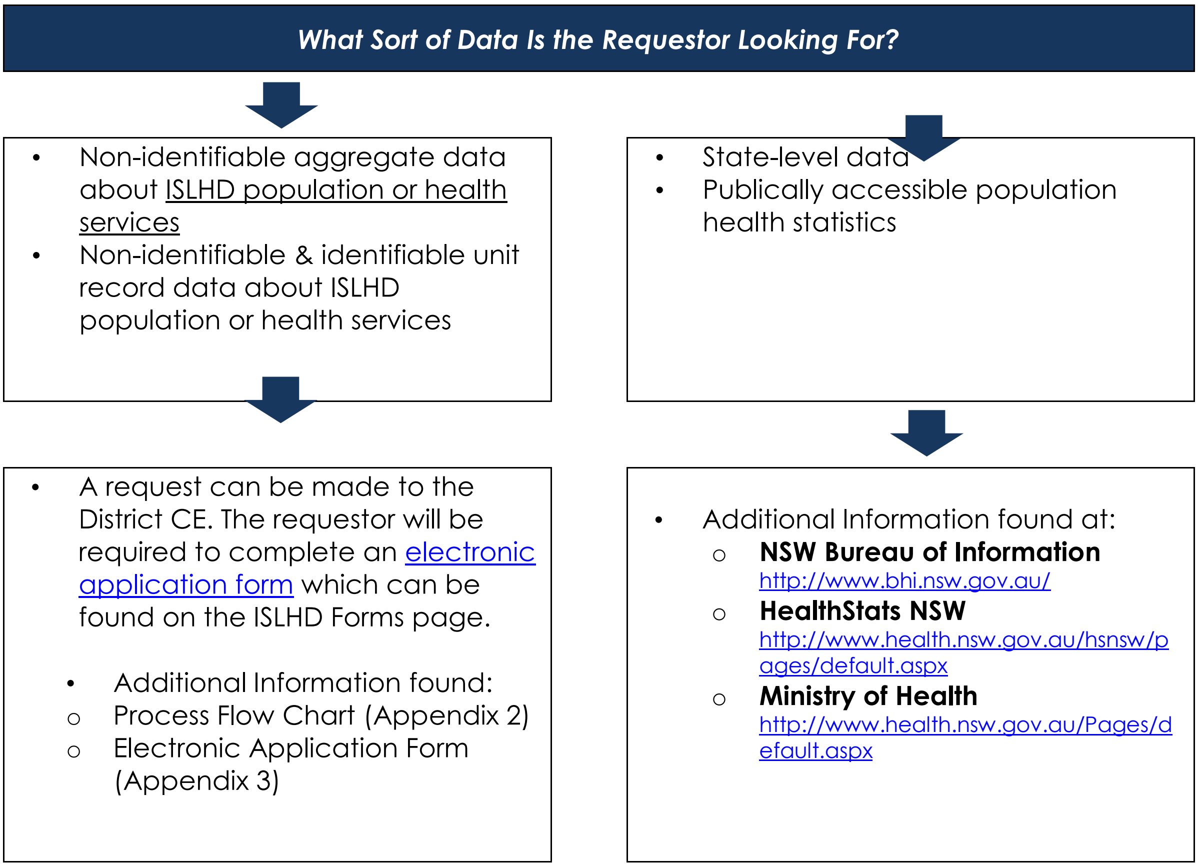
EXAMPLE:

An individual is looking for information about their surgery.

A pharmaceutical company is seeking information about the health of people living in Nowra.

Refer the requestor to the ISLHD **Right to Information website** which aims to make more information publicly available, provide equal access to information across all sectors of the community.

Data Request Process for Government Department or Organisation in Partnership with ISLHD



What Sort of Data Is the Requestor Looking For?

- Non-identifiable aggregate data about <u>ISLHD population or health services</u>
- Non-identifiable & identifiable unit record data about ISLHD population or health services

- A request can be made to the District CE. The requestor will be required to complete an electronic application form which can be found on the ISLHD Forms page.
  - Additional Information found:
    - Process Flow Chart (Appendix 2)
    - Electronic Application Form (Appendix 3)

- State-level data
- Publically accessible population health statistics

- Additional Information found at:
  - **NSW Bureau of Information** http://www.bhi.nsw.gov.au/
  - **HealthStats NSW** http://www.health.nsw.gov.au/hsnsw/pages/default.aspx
  - **Ministry of Health** http://www.health.nsw.gov.au/Pages/default.aspx

Mandatory Reporting

There are instances where ISLHD is required to mandatorily report ISLHD population or health services data to other organisations (eg. Ministry of Health, Cancer Institute or Commonwealth Department of Health). This usually occurs on a regular basis, and alternative governance arrangements are already in place for these transactions.

LEGAL AND REGULATORY COMPLIANCE

Data Governance within ISLHD is designed to ensure compliance with the legal, regulatory and governance environment.

All persons employed by, or providing a service on behalf of ISLHD have legislative obligations. Roles include, but are not limited to clinicians caring for consumers, administrative and support staff, senior managers, board members and contractors. Managers must ensure and monitor compliance with legislation, the general law, and NSW Health policy.

Clinical staff have a duty of care; and these staff should be familiar with relevant legislation, professional standards of practice, and NSW Health policy directives and guidelines.

The key legal instruments applicable to this Framework and requiring staff compliance are:

1. **The NSW Privacy and Personal Information Protection (PPIP) Act 1998** which regulates the collection and use of personal information in the public sector.
2. **The Commonwealth Privacy Act 1998 (Privacy Act)** regulates how personal information is handled.
3. **The Government Information (Public Access) Act 2009 (GIPA)**, allows any person to apply for access to any information held by the government.
4. **NSW Health Records and Information Privacy (HRIP) Act 2002** which regulates the collection and use of personal health information.
5. **The State Records Act 1998** which governs the creation, management and protection of public records. It also governs public access to those records.
6. **Common Law** which dictates that Health care providers have a duty to maintain consumer confidentiality in relation to information obtained as part of the treating relationship.
7. **The Health Practitioner Regulation National Law (NSW)** applies to some health professional groups. Breach of the confidence owed by a health practitioner to a consumer may constitute professional misconduct. It may therefore be subject to disciplinary action.
8. Various NSW MoH policies, procedures and guidelines that support good data governance and management, including the **Disclosure of unit record data by Local Health Districts for research or contractor services Policy. The NSW Health Accounts and Audit Determination (Determination)** requires all public health organisations to comply with policy directives issued by the Director General and the Ministry of Health (MoH).

9. **The NSW Health Code of Conduct** which states all staff members should report a breach or concerns about a breach of the Code of Conduct to a more senior staff member.

A brief summary of the various instruments is provided below. A comprehensive list of relevant legislation can be found in the Appendices 4, 5 and 6.

Record Management, Collection & Reporting

The State Records Act 1998 applies to all records maintained by ISLHD. It governs the creation, management and protection of public records. It also governs public access to those records. The Act overlaps with the NSW Health Records and Information Privacy (HRIP) Act, and public sector agencies must comply with the requirements of both Acts.

The State Records Act 1998 provides for:

- protecting records in the custody of a public office
- making and keeping full and accurate records of its activities
- establishing and maintaining a records management program in conformity with standards and codes of best practice
- making arrangements for monitoring and reporting on the records management program
- keeping technology-dependent records accessible

The Government Information (Public Access) Act 2009 (GIPA), allows any person to apply for access to any information held by the government. It is different from the HRIP Act as it is designed to facilitate government transparency. It is not restricted to personal information. Privacy laws are designed to provide individuals with greater knowledge and control over their own information. ISLHD generally relies on the access provisions in privacy legislation than the GIPA Act, and integrates the Privacy principles into day-to-day work.

Further details are described in Appendix 6 under 'Record Management, Collection & Reporting'.

Privacy

Public health organisations, including Non-Government organisations (NGOs) have a legal obligation to comply with privacy laws. Privacy obligations in NSW arise from two separate laws:

1. **NSW Privacy and Personal Information Protection (PPIP) Act 1998** which regulates the collection and use of personal information in the public sector and

2. **NSW Health Records and Information Privacy (HRIP) Act 2002** which regulates the collection and use of personal health information.

ISLHD's Chief Executive must ensure that the District has processes in place to comply with these legislative requirements. Processes include:

- notifying consumers on the collection of their personal information
- outlining their rights under privacy laws
- establishing internal review processes where patients wish to lodge a complaint if they believe their privacy has been breached
- establishing internal processes for patients / others who wish to access records under privacy legislation
- training staff on their privacy obligations and support them through local health information management processes
- providing a dedicated Privacy Contact Officer (PCO) to coordinate privacy implementation and oversee internal reviews
- Complying with the statutory requirement of annually reporting privacy matters

The Health Privacy Principles (or HPPs) contained in the HRIP Act establish 15 rules for the management of information. Some of these rules are relevant when:

- setting up data collections or patient information systems
- interacting with patients and meeting their information needs
- during the day-to-day use of personal health information and deciding when and how to share that information

There are 12 Information Protection Principles (IPPs) from the PPIP Act which are legal obligations which NSW public sector agencies must abide by when they collect, store, use or disclose personal information.

Due to the relatively small number of Aboriginal people in NSW specific guidelines for the release of Aboriginal health information are required to protect Aboriginal people from the risk of identification as individuals or communities. Disclosure of Aboriginal health information must comply with the NSW Aboriginal Health Information Guidelines.

See Appendix 6 under 'Privacy' for further details and relevant legislation.

Common Law & Professional Obligations

Health care providers have a duty to maintain consumer confidentiality in relation to information obtained as part of the treating relationship. The duty is not absolute and there are circumstances where a provider may lawfully disclose the information.

The Health Practitioner Regulation National Law (NSW) applies to some health professional groups. It provides clinical and professional standards based on definitions of 'unsatisfactory professional conduct' and 'professional misconduct'. Breach of the confidence owed by a health practitioner to a consumer may constitute professional misconduct, and therefore may be subject to disciplinary action.

See Appendix 6 under 'Common Law & Professional Obligations' for further details, and examples of breaches within NSW Health.

Policies, Procedures and Guidelines

The NSW Health Accounts and Audit Determination (Determination) requires all public health organisations to comply with policy directives issued by the Director General and the Ministry of Health (MoH). Compliance is a condition under the Health Services Act 1997.

Guidelines issued by the Ministry of Health establish best practice for NSW Health agencies. ISLHD must have sound reasons for not implementing standards or practices set out within these guidelines. A range of policy and procedure manuals for NSW Health are published on the MoH internet. These are updated continually to incorporate the latest policies. NSW Health policy directives and guidelines can be accessed at http://www.health.nsw.gov.au/policies

See Appendix 6 for a list of the most relevant policies, procedures and guidelines that support good data governance and management.

NSW ICT Strategy

The *NSW Government ICT Strategy* sets out a plan to build capability across the public sector in support of better, more customer-focused service delivery, and to derive better value for our investment in information and communications technology. Three key initiatives are the development of:

1. An ***Information Management Framework*** to support the way government administers and uses data and information. The Framework is a set of standards, policies, guidelines and procedures which will enable data and information to be managed in a secure, structured and consistent manner.
2. An ***Open Government*** where Government organisations are transparent and accountable. They collaborate with community and industry partners, encourages

participation in the policy formulation and decision making process, and encourages innovation from employees and external stakeholders.

3. The ***NSW Data Analytics Centre*** (DAC), which aims to become a world leader in whole-of-government data analytics, to provide insights into complex policy problems, support greater evidence-based decision-making and improve service delivery for the community.

FRAMEWORK & POLICY COMPLIANCE

This Framework and Policy provide guidance to all staff on the governance of data. This Framework should be followed when collecting, using or managing all types of organisational data.

All staff are responsible for preventing and reporting the misuse of data. As part of the NSW Health Code of Conduct:

- All staff are responsible for complying with the Code
- Managers are responsible for ensuring staff are aware of and understand their responsibilities
- Staff are encouraged to raise their concerns at any time with their managers
- Managers are responsible for addressing alleged breaches of the Code
- All staff face consequences for breaching the Code

Staff are responsible for reporting any matters of concern regarding the use and management of ISLHD Data. ISLHD has established a reporting system for suspect misuse, fraud, and corruption as well as Public Interest Disclosures (PIDs).

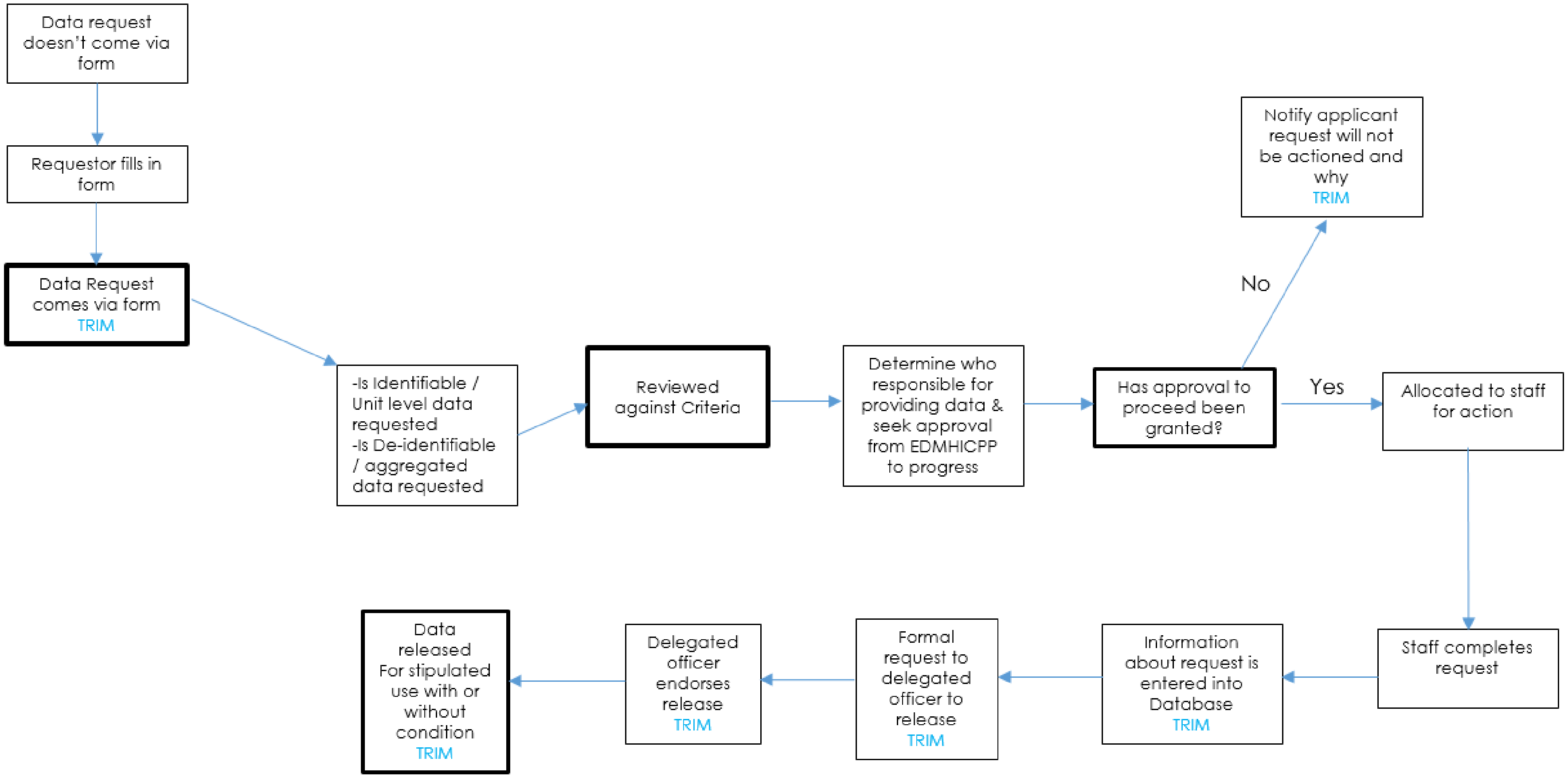
The Code of Conduct and Reporting of Corrupt Conduct, Fraud & Public Disclosures Policy (ISLHD PD2015_049) detail appropriate behaviour and responsibilities. Further information about the associated Policies can be found in Appendix 6.

In line with the NSW Health policy: *Disclosure of unit record data by Local Health Districts for research or contractor services*, a procedure has been developed for responding to a breach of conditions by a researcher or contractor following disclosure of unit record data. See Appendix 4.

APPENDIX 1: Consultation process for Data Governance Framework & Policy

July 2016 – current	Working group established & fortnightly meetings	Led by ISLHD Chief Health Information Officer, Information Management & Performance. With representatives from Planning, Population Health, Public Health - Epidemiology, Cancer Division, Clinical Governance, Mental Health Division & UOW AHSRI / CHRISP.
August 2016	Project scoping paper developed and submitted to Executive. Framework draft V1 commenced	Submitted to ISLHD Chief Health Information Officer / and Executive Director Integrated Care, Mental health, Planning, Information & Performance
November 2016	Email to key data representatives to understand key inputs that they expect in framework	ISLHD Research Director, Clinical Audit and Clinical Divisions
December 2016 - current	Meeting with Corporate Governance to review draft & discuss gap analysis and communication processes & support V1	
December 2016	Meeting with Manager Corporate Records & Right to Information Officer to review draft V1	
February 2017	Discussions with ISLHD Chief Health Information Officer, Executive Director Integrated Care, Mental health, Planning, Information & Performance to review draft V1	
March 2017	Clinical Governance to check readability of draft V1 (plain English)	
April 2017	Circulate draft Framework V2 to stakeholders for feedback	Stakeholders include: all positions that have been previously consulted, as well as Privacy Officer, Risk Manager, Data Managers & Integrity Officers, Research Governance Officer, Statutory Information Compliance Officer and other identified positions.
April 2017	Incorporating consultation feedback, finalising Framework, developing Policy	
June 2017	Final Endorsement and Implementation of Framework & Policy by Strategic Executive	
August 2017	Policy & Framework open for Comment by ISLHD staff	

APPENDIX 2: Data Request Process for External Organisation in Partnership with ISLHD


Data request doesn't come via form
Requestor fills in form
Data Request comes via form
TRIM
-Is Identifiable / Unit level data requested
-Is De-identifiable / aggregated data requested
Reviewed against Criteria
Determine who responsible for providing data & seek approval from EDMHICPP to progress
Has approval to proceed been granted?
No
Notify applicant request will not be actioned and why
TRIM
Yes
Allocated to staff for action
Staff completes request
Information about request is entered into Database
TRIM
Formal request to delegated officer to release
TRIM
Delegated officer endorses release
TRIM
Data released For stipulated use with or without condition
TRIM

Note: The ISLHD External Data Request committee will coordinate process

Documentation and approvals will be registered into the District's Official Recordkeeping Database (TRIM)

APPENDIX 3: Government Department or Organisation in Partnership with ISLHD External Data Request Form

Request for Non Identifiable ISLHD Health Services Data to a Third-party

This form is to be used by persons external to the Illawarra Shoalhaven Local Health District (ISLHD) and NSW Ministry of Health. **You are requesting the release of unit record data** (for research or contractor services) **or non-identifiable data** on the **population or services provided to the population**, of ISLHD.

THE FORM SHOULD BE COMPLETED BY THE PERSON MAKING THE REQUEST

This form is available online on the ISLHD Forms page. ISLHD CORP F 38 – Disclosure of ISLHD Health Services Data

Request for ISLHD Health Services Data to a Third-party
CONDITIONS FOR DISCLOSURE OF DATA

1. The data are to be used only for the purpose/s listed in this request. They are not to be used for any unlisted secondary purposes.

2. Use of data for research are carried out in accordance with the approved ethics application, site approval, and subsequent amendments, where relevant.

3. Data are to be kept in secure physical and electronic environment that is accessible by person/s directly involved in the above request. Confidentiality and security of data should be maintained.

4. Illawarra Shoalhaven Local Health District (ISLHD) are to be acknowledged in any publication or report that arises from the use of the data.

5. Data will not be matched with Data on individuals from another source

6. A copy of any publication or report is to be provided to the ***ISLHD Data Request Committee*** at least two weeks prior to its release

7. Data are to be destroyed after seven (7) years

8. Individuals identified in the data are not to be personally identified in any publication or report

9. The use of information on Aboriginal and Torres Strait Islander status is subject to the approval of the Aboriginal Health and Medical Research Council Ethics Committee if one or more of the following apply:
    - Aboriginality is a key determinant
    - Data collection is explicitly directed at Aboriginal peoples
    - Aboriginal peoples, as a group, are to be examined in the results
    - The information may have an impact on one or more Aboriginal communities
    - Aboriginal health funds are a source of funding.
10. This authority continues until and unless and it has been revoked in writing

11. Where relevant, ‘A Confidentiality Undertaking’ will be completed prior to receiving the data.

Note: Each application will be reviewed on an individual basis. Relevant conditions, in addition to those listed above, maybe applied with the release of the data.

CONFIDENTIALITY UNDERTAKING

I, ______________________________ ______________________________
[NAME] [POSITION]

understand that, in receiving unit record data of the [NAME OF DATA COLLECTION] Data Collection, I will have access to data about […]

Compliance with relevant legislation
I undertake to strictly preserve the confidentiality of these data, and understand that the disclosure of data may constitute an offence under Section 22 of the *Health Administration Act 1982* or Section 130 of the *Public Health Act 2010* (quoted below).
I understand and accept that my access to, holding and use of this data is subject to the Health Privacy Principles contained in the *NSW Health Records and Information Privacy Act 2002 and NSW Privacy and Personal Information Protection Act 1998.*

Identification of individuals
I undertake not to knowingly use any data obtained from this Data Collection to identify any individual person, including by linkage with other data.

Disclosure of data
I undertake not to disclose, pass on or otherwise make available to third parties any data, subset of data or any tables, graphs or other data aggregations or manipulations obtained or derived from these data where the data allows individual persons or providers to be identified by any means.

I undertake to ensure that any publicly available publication, report or presentation that is derived from the data will present data in an aggregate form only, which does not allow individual persons or providers to be identified by any means.

Security of data
I undertake to ensure that, so far as is under my control, such data, whether in the form of paper documents, computerised data or any other form, cannot be viewed by unauthorised persons, and that the data is stored and, where required, transmitted, in a secure and orderly manner which prevents unauthorised access.

Duty of notification
I undertake to inform ____________________ immediately if I become aware of any breach of privacy or security relating to data I access from the Data Collection.

I undertake to inform ____________________ of any change in my role or position that may affect my right to access this Data Collection.

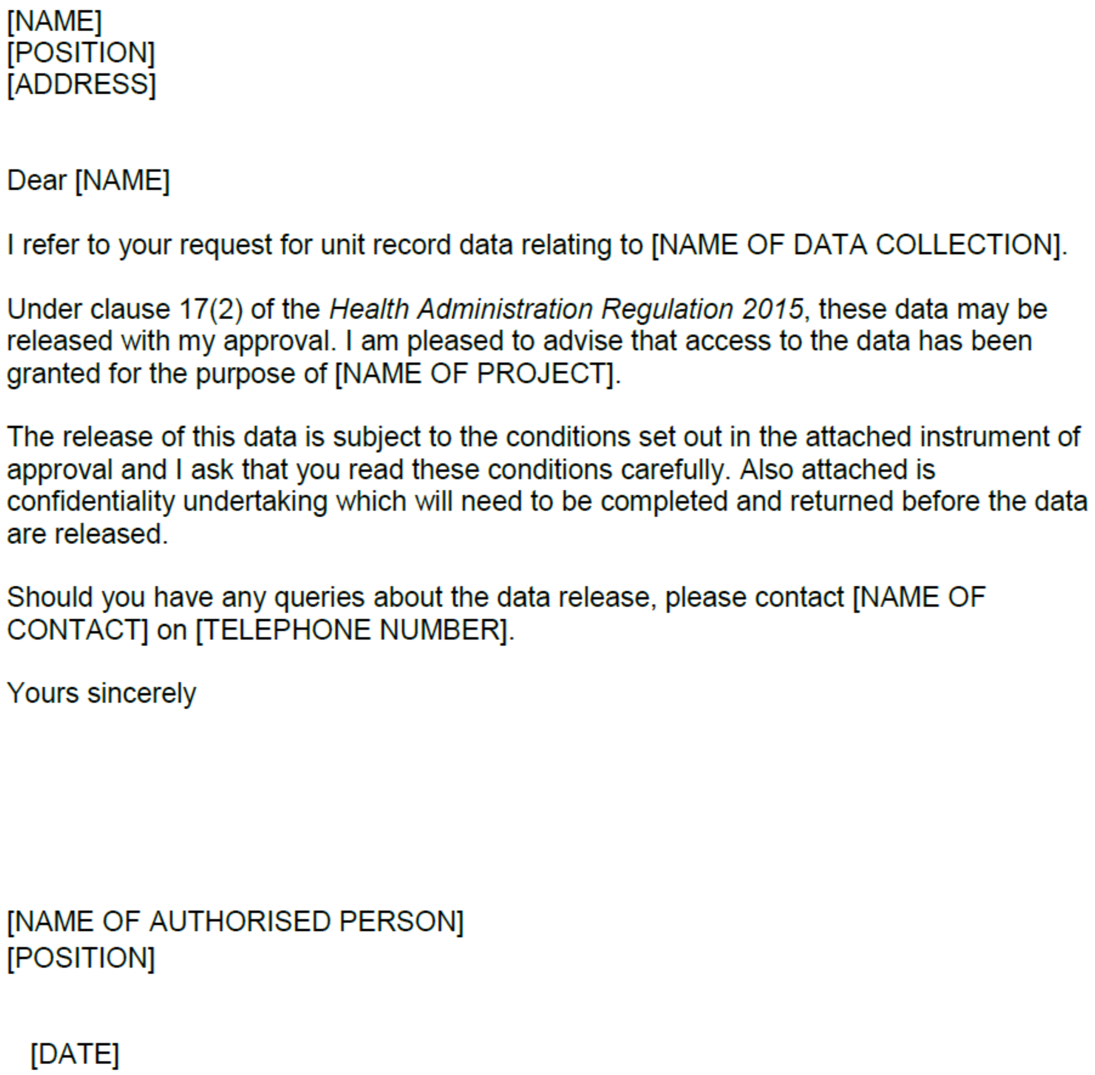
Consequence of non-compliance
I understand that non-compliance with the above conditions will result in removal of access to [NAME OF DATA COLLECTION] Data Collection.

Signed: ______________________________ ______________
[SIGNATURE] [DATE]

in the presence of:

______________________________ ______________________________
[WITNESS NAME] [WITNESS SIGNATURE]

LETTER FOR EXTERNAL RELEASE – Unit Record Data



[NAME]
[POSITION]
[ADDRESS]

Dear [NAME]

I refer to your request for unit record data relating to [NAME OF DATA COLLECTION].

Under clause 17(2) of the *Health Administration Regulation 2015*, these data may be released with my approval. I am pleased to advise that access to the data has been granted for the purpose of [NAME OF PROJECT].

The release of this data is subject to the conditions set out in the attached instrument of approval and I ask that you read these conditions carefully. Also attached is confidentiality undertaking which will need to be completed and returned before the data are released.

Should you have any queries about the data release, please contact [NAME OF CONTACT] on [TELEPHONE NUMBER].

Yours sincerely

[NAME OF AUTHORISED PERSON]
[POSITION]

[DATE]

APPENDIX 4: Procedure for response to a breach of conditions by a researcher or contractor following disclosure of unit record data (from the NSW Health breach procedure)

Breaches may range from minor infringements such as failure to make proper acknowledgements in a publication to serious breaches such as data being sold for commercial or personal gain, or data being unlawfully linked with personal information to re-identify an individual.

Procedure:
On becoming aware of any actual or possible breach of conditions, the LHD Data Custodian will make inquiries to ensure that the full facts of the situation are collected and information is provided to the relevant LHD Tier 2 officer.

The LHD Tier 2 will consider each situation, taking into account any previous breaches of conditions, and make a determination on one or more of the following actions:

1. No action (e.g. because the conclusion is that no breach took place).
2. A request for rectification of the circumstances causing the breach within a specified timeframe.
3. Counselling in the form of a warning.
4. A sanction: refer to NSW Health Procedure *NSW Health PD2018_001 Disclosure of unit record data by Local Health Districts for research or contractor services* for further information about possible sanctions.

In the case of a breach of conditions imposed by a HREC, information will be forwarded to the HREC.

The Chief Executive will be advised where a breach of conditions has occurred involving possible or actual breach of individual privacy.

APPENDIX 5: Data Concepts Table

Definition of concept ***(must relate to ISLHD)***	**Example of concept**	**Additional Information**	**Related Sections**	**Reference & Related Policies / Legislation**
Data				
Clinical Data **Aggregated data:** consolidated data relating to multiple individuals. **Unit record data:** records of data that relate to the health of an individual. **De-identified data:** data about a person whose identity is not apparent and cannot be reasonably ascertained. **Identifiable data:** Personal, unique identifying data eg. name, address, age, date of birth, ethnicity or diagnosis. It can also be a combination of data that allows a person's identity to be "reasonably ascertained". **Corporate Data** Data about how the organisation is managed including its Finance, Human Resources and Records Management. This may or may not be of a sensitive nature.			**Also See Data Disclosure, and Security.**	NSW Health Privacy Manual 2015
Data Collection				
The ongoing, systematic collection of clinical and corporate data. It allows a person to record, analyse, review, report, evaluate, monitor and disseminate data. In this framework it refers to data where ISLHD has explicit ownership. The methods of data collection vary by discipline.	Data collections can be both electronic and manual (paper-based). An example of an electronic data collection is FirstNet, which collects, stores and reports data on patients presenting to the District's Emergency Departments.	Data collections may contain aggregate data, de-identified data, or identifiable data (where data can identify an individual).	Also See Data Storage, Use, Linkage, Disclosure, Disposal, and Security.	NSW Health Data Collections website MoH Policy Directive: Data collections – Process for Approval of New or Modified (PD2005_155) MoH Policy Directive: Electronic Information Security Policy (PD2013_033)

Definition of concept *(must relate to ISLHD)*	Example of concept	Additional Information	Related Sections	Reference & Related Policies / Legislation
	Data collections can also be paper-based, for example a patient's written medical notes is a source of data collection that may be used for purposes of research, medico-legal etc.	All data collections are subject to policies, processes and controls with strict constraints regarding storage, use, linkage, disclosure, disposal, security. The following site provides some examples of data collections used within NSW Health: http://internal.health.nsw.gov.au/data/collections/index.html Data checking should be undertaken regularly, by episode and selectively. Routinely collected data is subject to quality assurance checking.		MOH Policy Directive: Health Care Records – Documentation and Management (PD2012_069) Nursing and Midwifery Documentation in the Health Care Record – ISLHD CLIN PD 28 Mental Health – Clinical Documentation MENT-H-CLIN-PROC-01 Medicare Patients Paperwork - CDH OPS BR 14 Oral Health Record Protocols – NSW Health GL2015_017 Minimum Data Set (MDS) – HIV/Aids and Sexual Health Radiation Safety - Record Keeping ISLHD CLIN PD 75 Receipting and Banking – CDH OPS BR 37 Outpatient Department Clinics Centralised Records - ISLHD OPS BR 52 Management of Clinical Indicators – SHN OPS P14 Rehabilitation Interventions Database – MENT-H CLIN BR 20
Data Quality				
Data quality reflects the extent to which data are: 1. Complete: extent to which data fields have been entered/filled in. 2. Accurate: The degree to which data are correct in all details. 3. Unique: no duplication	Manual data validation checks need to be undertaken by anyone using data. Examples:	ISLHD develop and maintain guidelines and procedures for maintaining the quality of data.	Also see Data Use	NSW & National Data Standards, NSW Health Non-Admitted Patient Activity Reporting Requirements. (Section 10)

Definition of concept ***(must relate to ISLHD)***	**Example of concept**	**Additional Information**	**Related Sections**	**Reference & Related Policies / Legislation**
4. Valid: the strength of data and whether they accurately describe the real world. 5. Consistent: done in the same way over time 6. Timely: The degree to which data represent reality 7. Objective and complies with known standards.	- Extracting data from HIE and comparing it to a SPaRC report - Extracting data from SPaRC - analyzing & synthesising the data to present a poster. Across ISLHD, data validation checks have been built into core systems to minimise the type and number of errors, and missing data in key fields. Data errors are then corrected at the source system with full traceability of the initial and updated values.	A data dictionary and coding guidelines is provided by NSW Ministry of Health to reduce variability in content and quality for both clinically coded and financial data. For some systems, exception reports are provided to users that detail missing data.		NSW Health Emergency Department Data Dictionary. ISLHD Clinical Documentation Policy Clinical Auditing Policy (ISLHD) ISLHD Service Level Agreement NSW MoH Key Performance Indicator Definitions Also consider: - Financial guidelines - HR guidelines and policies NSW Health Data Quality Assurance Framework for Activity Based Management PD2016_030 The Six Primary Dimensions for Data Quality Assessment
Data Use				
The communication or handling of data. It is an assumption that when using data, the quality will be checked using the principles of data quality.	A performance analyst extracts and manipulates data as part of routine reporting. A General Manager runs a SPaRC report and presents the d at a meeting		Also see Data Quality, Data Analysis, Data Presentation, and Dissemination	NSW Health Privacy Manual - Section 11 - Using and disclosing personal health information NSW Health Code of Conduct (PD2015_049)
Data Analysis				
The process of developing answers to questions through the examination and interpretation of data.	Analysis of Emergency Department presentations is made, investigating who presented to the ED and why they presented. Then this data is used to inform decision making.	The basic steps in the analytic process consist of identifying issues, determining the availability of suitable data, deciding on which methods are appropriate for answering the questions of interest, applying the methods and evaluating, summarizing and communicating the	Also see Data Quality	

Definition of concept *(must relate to ISLHD)*	**Example of concept**	**Additional Information**	**Related Sections**	**Reference & Related Policies / Legislation**
		results. This includes validating against benchmarks.		
Data Presentation				
The method by which people summarize, organize and communicate data. They use a variety of tools, such as tables, diagrams, charts, histograms and graphs. It is an assumption that when preparing data for presentation, the quality will be checked using the principles of data quality.	Data regarding the waiting list performance is presented in a report for an intended audience. Data in SPaRC presents data in a variety of formats		Also see Data Quality	
Data Dissemination				
The act of spreading/circulating data widely. It is important that this data meets ISLHD's quality standards. Eg. de-identified if being disseminated outside ISLHD. The audience needs to be identified to determine the level of detail.	Analysis of Emergency Department activity is circulated to the Strategic Executive for review and discussion. Data regarding operating theatre performance is circulated to key Surgical staff for review.	All staff have 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 including: - Is it identifiable? - Is data produced under contract with external agencies are also made publicly available - Does the data need to be made confidential & de-identifiable? - Are there any commercial interests? - Is there a risk to the organisation if data is disseminated?	Also see Data Quality	AIHW Governance Framework Disclosure of unit record data by Local Health Districts for research or contractor Services PD2018_001

Definition of concept ***(must relate to ISLHD)***	**Example of concept**	**Additional Information**	**Related Sections**	**Reference & Related Policies / Legislation**
Data Disclosure				
The selective release of data that relates to the health of an individual / group. Disclosure should comply with legislation, be in line with ethical standards, and be approved prior to disclosure.	The Planning Unit seeks approval then releases data about ED performance to the Primary Health Network on their request.	This includes release to other Local Health Districts, universities, and all other organisations or individuals. Authority for the disclosure and use of certain data is provided in section 10.1 of the Combined Delegations Manual.		Disclosure of unit record data by Local Health Districts for research or contractor Services PD2018_001 Data Collections – Disclosure of Unit Record Data for Research or Management of Health Services Policy PD2015_037 Request for Information Chapter 16A 003_10 – MENT-H CLIN BR 21
Data Access				
Activities related to storing, retrieving, or acting on data housed in a database or other repository.	Access to data within ISLHD will be provided to authorised users only. Data systems across the District should have in place a formalised process for approval of access to, and the use of, data. Data should be used in line with NSW Government policy.	Access to data for authorised users should be encouraged. Data stored within ISLHD databases has the potential to be utilised for improving service quality, patient safety, and efficiency of care.		NSW Government Digital Information Security Policy Electronic Information Security Policy – NSW Health Labelling of Sensitive Information (Expired) – PD018
Data Security Management				
Ensures privacy, confidentiality and appropriate access of data. Effective data governance protects the security of sensitive and personally identifiable data. It also mitigates the risks of unauthorised disclosure of the data. A key purpose of the framework is data security management.	General electronic security: ISLHD employees are provided with a NSW Health username & password that is used to access the shared drive and other data systems. Specific data systems require additional usernames and passwords.	Security steps include: • Encryption of data when transferring • Data checking and auditing • Role based access and authentication procedures • Backup & recovery plans • Technical standards		Australian government Protective Security Policy Framework Notifiable conditions data security and confidentiality', NSW Health Policy directive & Procedure (PD2012_047) NSW Health Code of Conduct (PD2015_049) Information Security Policy – ISLHD OPS PD 38

Definition of concept ***(must relate to ISLHD)***	**Example of concept**	**Additional Information**	**Related Sections**	**Reference & Related Policies / Legislation**
		The NSW Health Code of Conduct states that staff must: 4.5: Maintain the security of confidential and/or sensitive official data.		
Data Warehousing				
A centralised electronic storage of multiple data collections. It is specifically designed for data analysis, generating reports and for other ad-hoc queries. A data warehouse gathers data from different sources and converts it into a single and widely used format – thereby standardising the data. Warehoused data must be stored in a manner that is secure, reliable, easy to retrieve and easy to manage.	The Health Information Exchange (HIE) is NSW Health's network of corporate data warehouses. There are 16 data warehouses across NSW Health with each Local Health District managing their own data warehouse containing data specific to their organisation. A central warehouse at the Ministry of Health receives and stores an agreed set of state-wide data from all Districts.	EDWARD (Enterprise Data Warehouse Reporting & Decisions). EDWARD or EDW has been designed to replace the HIE as NSW Health's strategic data source of performance monitoring, health service purchasing and funding, health service planning and disease surveillance.		MOH HIE Support Site MOH EDW Support Site
Metadata				
The structured description of the characteristics of data, including its content, quality and format. It provides a shared meaning, allows comparisons, and makes it easier to retrieve, use and manage data resources. (AIHW Data Governance Framework, 2014)	The Health Information Resources Directory (HIRD)) serves as the 'Yellow Pages' for Data Elements and Data Domains in NSW Health, providing data analysts and health employees with a tool for browsing the various types of data and their attributes in datasets that are submitted to the Ministry of Health. This includes information such as how far back in history the data has been collected, the number of fields in a data set,	Other data collections may have their own set of data dictionaries and definitions not included in HIRD, some examples include- METeOR BreastScreen Australia etc		NSW's Health Information Resources Directory (HIRD)

Definition of concept ***(must relate to ISLHD)***	**Example of concept**	**Additional Information**	**Related Sections**	**Reference & Related Policies / Legislation**
	the definitions around different data sets.			
Data Definition				
Provides context and a written description for a data element or collection of data within a database or manual data collection. It is a component of metadata or a data dictionary.	An example of a data definition within the admitted patient data collection is: Medical Record Number: The number recorded by a hospital as the unique patient identifier for an admitted patient. It is the number which has been allocated to that patient by the hospital or health service for the purpose of distinguishing any medical records in relation to that patient, from the medical records relating to any other patient treated in that hospital or health service.	The Health Information Resource Directory (HIRD) is NSW Health's primary tool for identifying definitions for many of the data elements collected in the various data collections across the health service.		NSW's Health Information Resources Directory (HIRD)
Data Dictionaries				
A resource that provides standard descriptions and definitions in relation to data collection. It may describe the content, format and structure of the collection and any relationships between data elements or data collections. Data dictionaries and metadata serve a similar function. They provide a centralised resource to assist users better understand the data they are working with.	The National Health Data dictionary provides national standards for the broader health sector and includes the identity of data elements, definitions, attributes (format, data type etc.), usage guides, origin of data and related references.	The NSW Health Service Agreement KPI Data Dictionary is a resource document available to all Districts that provides definitions on the Service Agreement KPI's and Service Measures, how these KPI's are derived, the source of data, the data elements, inclusions and exclusions.		NSW Health Data Collection Dictionaries & Instructions, The National Health Data Dictionary NSW Health Service Agreement Key Performance Indicators and Service Measures Data Dictionary

Definition of concept ***(must relate to ISLHD)***	**Example of concept**	**Additional Information**	**Related Sections**	**Reference & Related Policies / Legislation**
Data Requests				
The process of asking for data or applying for access to data. The data can be from an internal source, or an external organisation.	ISLHD provides a custom data request service for access to our local statistics/ data that are not available in published reports or tables. Data requests are filtered and responded to by numerous units within the District, depending on the nature of the request, for example, the ISLHD Performance Unit, Cancer Care Services, Mental Health Services, all have different roles to responding to data requests.	With the increasing availability of data in ISLHD, there is an increased demand for data to inform / report on service delivery. The Data Governance Framework and Policy will aim to address governance arrangements for responding to these requests.		Privacy Manual for Health Information – NSW MOH Privacy Policy PD042
Data Linkage				
The joining of data from two or more records that relate to a common entity, e.g. individual, family, event or address. This can involve linkage of records within a single data collection or across two or more different sources. When joining together pieces of data that belong to the same person, common identification and/or demographic fields - personally identifying data - are used. Under the Health Records and Information Privacy (HRIP)Act 2002, a health records linkage system refers to a computerised system that is designed to link health records for an individual held by different organisations.	HIE contains data tables for inpatient episodes of care which can be joined together for individual patients – these are internally linked data. Inpatient data for ISLHD patients which are linked to records for the same individuals in another ISLHD dataset (e.g. Allied Health) or an external source (e.g. death registrations) are externally linked data. The HRIP Act 2002 is concerned with records linked across <u>different organisations.</u>	Infringements of privacy and breaches of confidentiality are the main risks associated with data linkage.To minimise risks, linkage should be done so that, for example: • the data linkage process (where access to personally identifying data is necessary) is separated from the analysis of health data (where such access is not necessary) • identifiable data are securely stored and the smallest number of people as possible have access	Also see <u>Data Disclosure</u>	Research Collaboration Agreement between University of Wollongong and ISLHD – ISLHD OPS BR 21 Healthcare Identifiers Act 2010 Personally controlled electronic health records act 2012

Definition of concept ***(must relate to ISLHD)***	**Example of concept**	**Additional Information**	**Related Sections**	**Reference & Related Policies / Legislation**
Data Storage				
Data storage is the practice of storing electronic data. This can be done in a variety of ways: • online, whether locally on an agency server, or by hosted storage through the internet (eg cloud storage). • In off-line storage on removable media (eg. CDs, USB sticks). • Hard copy	Data is stored within the HIE warehouse, which is housed on the LHD servers. Data is collected by the Renal Service and stored in a folder held in the NUMs office.	How and where digital data is stored will affect its viability over time. It's important to ensure the data remains authentic, reliable, discoverable, accessible, usable, protected and preserved for as long as needed. A secure physical and electronic environment should be maintained.		NSW Health Privacy Manual • Section 16 Electronic health information management systems NSW State Archives & Records Authority Medical Records Storage of Clinical Photography – ISLHD OPS BR 28 Records – Storage and Protection – ISLHNPD/22 Health care records – Storage and Custodian of Archived and Current HCRs – Drug and Alcohol Service – D&A SOP 03 Health care records – Tracking and storage for clinicians – Drug and Alcohol Service – D&A SOP 04
Data Backup				
The activity of copying **files** or **databases** so that they will be preserved in case of mainframe / equipment failure or other catastrophic events.	The data on ISLHD shared drives and data systems such as HIE and Business Objects (SPaRC) are backed up each night to protect ISLHD data from being lost.	Backup is a routine part of the operation of ISLHD through the ICT backup/restore strategy. The strategy is in place to ensure that data is available in line with business requirements.		Use and Management of Misuse of NSW Health Communications System PD2009_076. ICT backup Strategy Electronic Information Security Policy – NSW Health Health Records Disaster Management – PD150 Records – Disaster Management – ISLHNPD/26 eHealth NSW – Business Plan and Strategy for NSW Health 2016 – 2026 (Strategy 11 – Safeguarding Security & Privacy)

Definition of concept *(must relate to ISLHD)*	Example of concept	Additional Information	Related Sections	Reference & Related Policies / Legislation
				Health Security Operations Centre (HSOC)
Data Retention				
The process of identifying how long records should be retained.	• Records management team go through the process of determining what corporate records should be retained / archived or disposed of. • Medical Records team go through the process of determining what clinical records should be retained / archived or disposed of. •	Retention should also ensure the process of disposing of records is completed in an authorised and managed way.		NSW State Archives & Records Authority Records – Retention Periods –ISLHNPD/28
Data Archiving				
The appropriate storage of data to safeguard and preserve the records. This allows people to discover, use, and learn from this documentary heritage. It also ensures continued access to this data.	Old information systems/data collection tools that have been retired (eg. CHIME) will be archived and stored separately. The data can be retrieved if required through a separate process.	Storage is on a long-term or permanent basis. The storage must ensure the ability to preserve, verify, research and retrieve that data. An archived record has continuing value because of their legal, administrative or historical value.		NSW State Records Authority AIHW Governance Framework Corporate Records Management – Archiving – CDR OPS BR 09 (Coledale) NSW Government Information Classification, Labelling and Handling Guidelines
Data Disposal				
<u>Electronic Data</u> **Overwriting** of data means replacing previously stored data on a drive or disk with a random pattern of meaningless data. **Destruction** of electronic media is the process of physically damaging a medium so that it is not usable	The IT department physically destroys the hard drive of a PC that is no longer being used. A staff member deletes the data from a USB stick and	Authorised disposal of health records should be done in such a way as to render them unreadable and leave them in a format from which they cannot be reconstructed in whole or in part.		NSW State Records Authority AIHW Governance Framework Section 24 of the Archives Act 1983 Records – Destruction of – ISLHNPD/25

Definition of concept *(must relate to ISLHD)*	Example of concept	Additional Information	Related Sections	Reference & Related Policies / Legislation
by any device that may normally be used to read electronic data **Clearing** data such as formatting or deleting data removes data from storage media in a manner that renders it unreadable **<u>Paper Based Records</u>** There are a number of ways in which paper based records can be disposed of. These include: • Shredding • Pulping • Burning The disposal of any State record should be done in accordance with the NSW State Records Act.	then also deletes the data from the C: of the PC.	A register of records destroyed must be maintained for future reference and accountability.		

APPENDIX 6: Data Role and Responsibilities table

Description of Role	Responsibility of Role	Example of ISLHD Position	Reference / key legislation
Board			
The board has ultimate responsibility for the governance of the organisation. They set strategic organisational goals that drive the development and implementation of data governance across the District.	• Ensure robust organisational data governance practices are in place • Comply with all fiduciary and other corporate duties • Comply with all relevant laws • Ensure effective safety and quality systems are in place, supported by robust data frameworks; • Ensure data management supports the monitoring of safety and quality; • Ensure the organisation responds appropriately to data issues that impact on safety and quality matters. • Duty not to misuse the organisation's property, data or opportunities • Maintain the security/confidentiality of sensitive data	ISLHD Board	ISLHD Board Handbook
Chief Executive			
Officer with authority and accountability under legislation, regulation, or policy for the collection, use, disclosure and storage of data. The CE provides required resources to establish, implement, operate, review, maintain, and improve the organisation's data governance.	• Ensures that all staff members are aware of data governance requirements, have access to appropriate materials about related obligations, and undertake appropriate training • Ensures that the LHD complies with relevant legislative and ethical requirements, policy and guidelines, including reporting requirements eg. annual statutory annual reporting regarding privacy compliance • Designates a specific officer for the LHD to whom requests for guidance on data privacy should be referred and who should support staff in ensuring privacy policies and procedures are observed	CE	GEA White Paper Cancer Institute NSW Data Governance Policy
Data Sponsor			
A senior role responsible for the overall management of the data collection. They lay the foundation for the data governance framework and are responsible for the oversight.	They provide: • Direction, guidance and appropriate resources to Data Custodians	• CIO • Executive	Health Information and Performance Governance Committee, 2017

Description of Role	Responsibility of Role	Example of ISLHD Position	Reference / key legislation
Chief Information Officer			
Approves data governance and data management policies. Conducts an annual review of ISLHD's data governance.	Has oversight over the organisation's data governance; reviews and updates data governance and data management policies and procedures; implements actions arising from annual reviews of data governance.	Chief Information Officer	Cancer Institute NSW Data Governance Policy
Executive			
Ensure that all managers, staff and contractors comply with the Data Governance Policy and Framework, and are trained and competent to fulfil their duties.	The Executive define the data to be captured, stored, managed and maintained according to their delegation. They are responsible for ensuring business processes and procedures are aligned with National, State and Local Data Governance Requirements and priorities. The Executive ensure appropriate, trained resources are appointed to manage the data (custodians). They define and approve access and custody arrangements, including the authorisation to release data. They are responsible for ensuring staff are competent to fulfil their data management duties. They are responsible for monitoring and improving data and data management functions, and ensuring issues are resolved in a timely manner.	• Hospital General Manager • Director, Clinical Division • Director Public Health • Executive Director (Tier 2)	Cancer Institute NSW Data Governance Policy - Section 15.14.3 Staff roles
Data Custodian			
Manages a data collection system or has delegation to exercise overall responsibility for a data collection. Across ISLHD, Data Custodians can have dual roles for particular systems, e.g. The role of Data Custodian and Data Integrity Officer / Data Manager.	Data custodians are responsible for managing and implementing the data delivery process. They ensure compliance for: • Data collection implementation • Data storage, disposal and security • Relevant legislation and policies • Administration • Quality assurance • Maintaining data standards in line with the relevant policies and procedures • Data access and release • Complies with relevant classifications, definitions or categories • Implements and maintain data assets according to rules set by owner • Seek approval from Executive, if the release of data is required	• High level managers eg. Clinical Lead, Cancer Services Information System • Non-Admitted Performance Analyst	NSW Health Privacy Manual Section 15.14.3 Staff roles Cancer Institute NSW Data Governance Policy AIHW Governance Framework

Description of Role	Responsibility of Role	Example of ISLHD Position	Reference / key legislation
Data Steward			
Appointed by Data Custodians to develop, update and operationalise established data policies (approved by the custodian & sponsor).	Enact data management and organisation in line with data policy and procedures.	• Data Officer • DIO • System Administrators	Health Information and Performance Governance Committee, 2017
Data Integrity Officer (DIO) / Data Manager (Site & District level positions)			
Work with data custodians and business owners to define and control data. They have high level knowledge and expertise in the content of the data they manage. DIO's or Data Manager do not have delegated authority to add or modify clinical data unless appropriate authorisation is granted, and an appropriate audit trail / notes is applied. However they can modify administrative and clerical data issues. DIO's or Data Manager work with Data Custodian's to assist in the understanding of the data requirements and data rules.	Data Integrity Officer's / Data Manager's responsibilities are related to implementing the data management functions, including: • Defining data and data management requirements and specifications. • Improving data management (e.g. improving quality). • Identifying and resolving data management issues. • Measuring and monitoring data management activities and initiatives. • Maintaining data management processes (e.g. maintaining meta-data). • May provide training and assistance to staff on the data collection requirements • Participate in data quality improvement programs, often guided by the data custodian or policies	• Mental Health Information Development Coordinator • Cancer Services Information System Manager • Surginet Data Manager • Community Health Data Integrity Officer	HSIPR- Data Integrity Officer Position Description
System Administrators			
Understand and follow acceptable procedures in managing the system, resolving known vulnerabilities, and monitoring system access.	System Administrators are responsible for: • Development of practices and procedures to support the policies related to system use in consultation with the data custodians • Performs system health checks • May provide Service Desk support to trouble shoot user technical issues • Managing the process of granting and revoking access to the system, once approved by those with delegated authority.	• PAS Coordinator • eMR Team • HIE Coordinator • Oncology Information System Manager	
Data User / All Staff			
All staff have a duty to collect and maintain the privacy, quality, integrity and security of data held and managed by their Service / Division / Unit.	All staff (including contractors) will ensure that they: • Collect data that are complete, accurate and up-to-date • Comply with relevant data governance policies and legislation • Remain aware of their data governance roles, responsibilities and obligations. • Participate in related training	All Staff of ISLHD	NSW Health Privacy Manual - Section 15.14.3 Staff roles Cancer Institute NSW Data Governance Policy

Description of Role	Responsibility of Role	Example of ISLHD Position	Reference / key legislation
Staff with access to data may only access, view and use the data for purposes directly related to their work.	• Access to the data is carried out in a way that does not jeopardise data security and privacy. • Report any breach or suspected breaches of data security or privacy to the data custodian.		
Committees			
A range of ISLHD Committees support the District, CE & Executive to promote effective and efficient data governance. Committees provide support in a variety of ways: • Strategic direction • Ethical advice • Governance • Compliance • Coordination & integration • Staff engagement • Consistency	The responsibilities of committees are to: • Protect consumers and the District • Evaluate and contribute to improvement of governance • Contribute to improvement of policy compliance • Promote awareness and adoption of policies and procedures • Review and recommend strategies • Ensure input from stakeholders and provide feedback and advice • Identify resource requirements • Monitor risks	• Joint UOW & ISLHD Ethics Committee • Audit & Risk Committee • Clinical Informatics Committee	National Statement on Ethical Conduct in Human Research (2007) (Updated May 2015)

APPENDIX 7: List of Legislation, Policies and Guidelines

Legal obligations for Health Organisations and Employees[1]

Legislation

Government Information (Public Access) Act 2009 *This Act was established to provide an open and transparent process for giving public access to information from NSW public sector agencies and to encourage the proactive release of government information.*

Health Administration Act (Section 22) 1982 *covers any information which is provided or recorded pursuant to any Act in the health portfolio. It is binding on all persons working in the NSW Health system. Under the Act information cannot be disclosed unless certain specified criteria are satisfied.*

Health Administration Regulation (Section 13) 2000

Health Administration Regulation 2010 *It exists to allow the Chief Health Officer to release epidemiological data and the Secretary, NSW Health to release other information for the purposes of research. Such data are only released to researchers with the condition that the confidentiality of data are maintained. The regulation also allows disclosure of information in certain circumstances where it is necessary for Root Cause Analysis (RCA) related matters.*

Health Records and Information Privacy Act 2002 *The purpose of this Act is to promote fair and responsible handling of health information. Relevant Statutory guidelines:*

- *Use or Disclosure of Health Information for the Management of Health Services*
- *Use or Disclosure of Health Information for Training Purposes*
- *Use or Disclosure of Health Information for Research Purposes*
- *Use or Disclosure of Information from a Third Party*

Health Records and Information Privacy Code of Practice 2005 *This Code deals with the collection, use and disclosure of health information by human services agencies.*

Health Records and Information Privacy Regulation 2006

Health Records and Information Privacy Regulation 2012*This Regulation deals with use and disclosure of health information by health services for certain reasons including chaplaincy*

[1] **Privacy Act 1988 (Commonwealth)** This Act and the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth) do NOT apply to the NSW public sector. The Commonwealth privacy legislation is limited to the regulation of the Commonwealth public sector and the private sector in NSW including non-government organisations. Its provisions relating to health information do not therefore apply to NSW Health and should not be relied on. NSW Health agencies however should be aware that Commonwealth privacy legislation may bind non-government organisations and private sector health providers (such as individual health practitioners and private hospitals), and so may be relevant to the way these organisations interact with NSW Health.

services, Health Practitioner Regulation National Law, organ donation registers and limited other purposes.

Health Services Act 1997 *is the principal Act regulating the governance and management of the public health system in NSW. The Local Health District is established and operates under the Health Services Act 1997.*

National Statement on Ethical Conduct in Human Research (2007) - *Updated May 2015*

Privacy and Personal Information Protection Act 1998 *The purpose of this Act is to promote fair and responsible handling of information.*

Public Health Act (Section 75) 1991

Public Health Act 2010

Public Health Regulation (Section 81A) 1991

State Records Act 1998
The State Records Act 1998 is designed to: ensure the better management of Government records throughout their existence, promote more efficient and accountable government through improved recordkeeping, and provider better protection for an important part of the State's cultural heritage

Government Information (Public Access) Act 2009
In order to maintain and advance a system of responsible and representative democratic Government that is open, accountable, fair and effective, the object of this Act is to open government information to the public by:

- *authorising and encouraging the proactive public release of government information by agencies, and*
- *giving members of the public an enforceable right to access government information, and*
- *providing that access to government information is restricted only when there is an overriding public interest against disclosure.*

Other relevant legislation include:

Births, Deaths and Marriages Registration Act 1991

Cancer Institute Act (NSW) 2003

Health Care Complaints Act 1993

Public Health Regulation 2012

The Commonwealth Privacy Act 1998 (Privacy Act) regulates how personal information is handled.

Authorities:

State Archives & Records Authority of New South Wales:

- Health Services, Public: Administrative Records (GDA21)- *This authority applies to records created and maintained to support the management and delivery of public health care services and programs.*
- Health Services, Public: Patient/Client records (GDA17) - *This authority covers records documenting the provision of health care to patients and clients of the public health system. It applies to any organisation, facility or service which is part of the NSW public health system.*
- General Retention and Disposal Authority (GA28) - *identifies common or general administrative records created and maintained by NSW public offices which are required as State archives and provides approval for the destruction of certain other administrative records after minimum retention periods have been met.*
- Original or source records that have been copied (GA45) - *This general retention and disposal authority provides for the authorised destruction of original or source records that have been copied, provided that certain conditions are met.*

NSW Department of Premier & Cabinet

- NSW State Digital Information Security Policy

Privacy

In NSW, the Privacy and Personal Information Protection Act 1998 (PPIP Act) applies to non-health personal information, e.g. employee records. The NSW Health Records and Information Privacy Act 2002 (HRIP Act) regulates privacy related to personal health information, being information about physical health, mental health or disability, including information collected for the purposes of providing a health service. The obligations of public health organisations are addressed in the NSW Health Privacy Manual 2015 and the Privacy Management Plan. The NSW Health Internal Review Guidelines are used when managing complaints about a breach of the HRIP or PPIP Acts.

Statutory guidelines expand upon the Health Privacy Principles (HPPs) within the HRIP Act. Their purpose is to guide organisations in their handling of health information and provide more detailed information regarding the scope of the principles.

Organisations seeking to use or disclose health information, without the individual's consent, must comply with the statutory guidelines if they want to rely on exemptions within the principles:

- management of health services exemption (HPP 10(1)(d) or 11(1)(d))
- research exemption (HPP 10(1)(f) or 11(1)(f))
- training exemption (HPP 10(1)(e) or 11(1)(e))
- information from third party exemption (HPP 4(3))

These exemptions can apply when the public interest in the activity substantially outweighs the public interest in maintaining the level of privacy otherwise afforded by the HPPs.

Health Privacy Principles (HPP):

- Collection (HPPs 1-4): *Personal health information must be collected by lawful means and for a lawful purpose. The purpose must be directly related to, and reasonably necessary for, an organisation's functions or activities. Collection and information sought must be relevant, not excessive, accurate and not intrusive. Personal health information must be collected from the individual it relates to, unless that is unreasonable or impractical.*
- *Reasonable steps must be taken to inform the individual about how the information may be used, who may access it, and the consequences of not providing it. The individual should be told what agency is collecting the information and that they have a right to access it. This information should generally also be given to the individual where information about them is collected from someone else, unless certain exemptions, listed in the Act and the guidelines apply.*

Information protection principles (IPPs)

The 12 Information Protection Principles (IPPs) are your key to the *Privacy and Personal Information Protection Act 1998* (PPIP Act). These are legal obligations which NSW public sector agencies, statutory bodies, universities and local councils must abide by when they collect, store, use or disclose personal information. As exemptions may apply in some instances, it is therefore suggested you contact the Privacy Contact Officer in your agency or the Information and Privacy Commission NSW (IPC) for further advice.

- Collection (1. Lawful, 2. Direct, 3. Open, 4. Relevant)
- Storage (5. Secure)
- Access and accuracy (6. Transparent, 7. Accessible, 8. Correct)
- Use (9. Accurate, 10. Limited)
- Disclosure (11. Restricted, 12. Safeguarded)

Retention and Security (HPP 5): *Personal health information held by public health agencies must be securely housed and protected against loss or misuse. Information must be kept only as long as is necessary for the purpose (or as required by a law, such as the NSW State Records Act 1998), and must be disposed of securely*

Access (HPPs 6-7) *Organisations that hold personal health information must allow individuals to find out if they hold information about that individual, and, if so, what kind of information they hold, what it is used for, and whether and how the individual can access it. Individuals must be allowed to access the personal health information held about them. This must be done without excessive expense or delay.*

Amendment (HPP 8): *Individuals may request that their personal health information be amended to ensure that it is accurate, relevant, up to date, complete and not misleading. Organisations must either make the requested amendments or, if requested, attach to the information a statement by the individual of the amendment they sought.*

Accuracy (HPP 9): *Before using personal health information, organisations must take reasonable steps to ensure that the personal health information they hold is relevant, up to date, complete and not misleading.*

Use (HPP 10): *Personal health information can be used for the purpose for which it was collected, or for other purposes recognised by the Act. These include a "secondary purpose" such as where there is consent for the use, the use is a "directly related purpose", for management, training and research activities, for investigation and law enforcement, or where there are serious threats to individuals or the public.*

Disclosure (HPP 11): *The provisions for disclosure of personal health information are the same as those for use of this information. They also include a provision that a person's personal health information may be disclosed to immediate family members for compassionate reasons, provided that this is not contrary to the expressed wish of the individual.*

Identifiers (HPP 12): *Identifiers can only be applied to personal health information if this is reasonably necessary to carry out the organisation's functions. Public health system identifiers may be used by private sector agencies, but only in defined circumstances and with strict controls*

Anonymity (HPP 13): *Provided that it is lawful and practicable, individuals should be given the option of not identifying themselves when dealing with health organisations.*

Transfer of Information across State Borders (HPP 14): *As a general principle, personal health information must not be transferred to a Commonwealth agency or an organisation in another state jurisdiction unless the receiving agency applies personal health information privacy policies and procedures substantially similar to those of NSW.*

Linkage of Electronic Records (HPP 15): *Personal health information must not be included in a system outside NSW Health that links health records of one health service with health records in another health service, unless the individual it relates to has expressly consented. HPP 15 only applies to linkages of an ongoing record of health care for an individual and does not restrict linkage of other personal health information held electronically. HPP 15 will apply to the linkage of records of health care at a state or national level between the public and private sectors, or between two or more private health services.*

Common Law & Professional Obligations

Circumstances where a health care provider may disclose information include:

- where the consumer waives their right to confidentiality
- where there is some statutory or other lawful reason (e.g. statutory provisions for mandatory notifications).
- "in the public interest" where the public benefit of disclosure would outweigh the public interest in maintaining confidentiality. The exact nature and extent of this interest remains uncertain, but is likely to be similar to Health Privacy Principle 11(1)(c) where disclosure is permitted where there is a serious and imminent threat to the life, health or safety of an individual, or a serious threat to public health or public safety.

Various professional codes of ethics also require that confidentiality of personal information be maintained. Although such codes do not have the binding authority of a statute, breaches may incur disciplinary action for registered health practitioners under the National Law.

Policies, Procedures, Guidelines

NSW policy directives and guidelines

Aboriginal and Torres Strait Islander Origin – Recording of Information of Patients and Clients (PD2012_042):*outlines the requirements for collecting and recording accurate information on the Aboriginal and Torres Strait Islander status of all clients of public health services in NSW.*

Client Registration Guidelines (GL2007_024)

Client Registration Policy (PD2007_094): *outlines the process and requirements for uniquely identifying and collecting data on an individual, and recording those data within a District-wide database. The intent of client registration is to be able to link information held on a client/patient and thereby, support the delivery of services.*

Corporate Governance & Accountability Compendium for NSW Health 2014: *It provides a summary of the key governance requirements applying to NSW Health agencies that apply at both a system and whole of Government level. Section 4 of the compendium covers Legal and Policy Requirements.*

Data and Records Management (ISLHD OPS PROC 92)

Data Collections - Disclosure of Unit Record Data for Research or Management of Health Services (PD2015_037) *outlines conditions and procedures for release of unit record data, with and without personal information.*

Electronic Information Security Policy (PD2013_033): *covers security requirements for NSW Health information including electronic personal health information. This policy applies to all employees, contractors and other persons who, in the course of their work, have access to information (including electronic personal health information) in or on behalf of the NSW public health system. The policy outlines roles and responsibilities.*

General Retention and Disposal Authority - Public Health Services: Patient/Client Records (IB2004/20): *applies to any organisation, facility or service which is part of NSW public health system and covers records documenting the provision of health care to patients and clients of the public health system. The Authority has been approved by the Board of the State Records Authority.*

Health Care Records – Documentation and Management (PD2012_069): *The Health Care Records Policy defines the requirements for the documentation and management of health care records across public health organisations in the NSW public health system. The Policy ensures that high standards for documentation and management of health care records are maintained consistent with common law, legislation, ethical and current best practice requirements. The policy delineates responsibilities of Chief Executives, Facility / service managers and Health care personnel.*

NSW Aboriginal Health Information Guidelines *The purpose of the NSW Aboriginal Health Information Guidelines is to ensure consistency and good practice in the management of health and health-related information about Aboriginal peoples in NSW. This extends to issues surrounding the collection, ownership, storage, security, access, release, usage, reporting and interpretation of information, as well as issues of confidentiality and privacy.*

NSW Health Privacy Manual (2015): *provides operational guidance to the legislative obligations imposed by the HRIP Act 2002. The manual outlines procedures to support compliance with the Act in any activity that involves personal health information.*

NSW Standard on Digital Recordkeeping (IB2009_027) *advises about compliance with and implementation of the provisions of the NSW Standard on Digital Recordkeeping issued by the State Records Authority Board. The Standard sets out minimum requirements for digital recordkeeping system functionality and the creation and management of recordkeeping metadata for digital records.*

Privacy Management Plan - NSW Health(PD2005_554)

Records Management - Department of Health (PD2009_057):*This policy statement and protocol sets out the requirements, roles and responsibilities for ensuring compliance with the legislation and benefits of good recordkeeping practices. Compliance enables the Department to meet its business needs, accountability and governance requirements and protects the interests of all parties. The policy applies to records in all formats, including digital (electronic) records.*

Records Management Policy (ISLHNDP/23)

Records Retention and Disposal on the Closure of Health Organisations (PD2005_282): *This policy statement and protocol sets out the requirements, roles and responsibilities for the disposal of records on the closure of health organisations*

Risk Management - Enterprise-Wide Risk Management Policy and Framework - NSW Health (PD2015_043): *It outlines the minimum mandatory requirements for NSW Health staff in* *complying with risk management standards, consistent with Principle 1 and Core Requirement 1.1 and 1.2 of the NSW Treasury Policy TPP15-03. The NSW Health Risk Category Communication and Information is concerned with, for example: Information and data management systems; Informed consent; Privacy and confidentiality; Knowledge management; Records management; Release of information; Digital Information Security e.g. electronic medical record; Social Media.*

Information Security Policy (Including Digital Information Asset Security Policy) (ISLHD OPS PD 38): Describes the measures to be used to protect IS LHD information assets from deliberate or inadvertent unauthorised acquisition, damage, disclosure, manipulation, modification, loss or use. The policy encompasses the behaviour of the people who manage and use information in the line of NSW Health business.

Policies and Guidelines specifically related to data collections and reporting:

Child Death Review Team - Access to Records (IB2014_028)

Congenital Conditions Register - Reporting Requirements (PD2012_055)

Deaths - Reporting of Maternal Deaths to the NSW Department of Health (PD2005_219)

Deaths - Review and Reporting of Perinatal Deaths (PD2011_076)

Disclosure of unit record data by Local Health Districts for research or contractor Services PD2018_001

Home and Community Care Minimum Data Set Version 2 - Collection & Reporting Requirements (PD2008_050)

Immunisation Register - Australian Childhood (PD2005_085)

Mental Health Clinical Documentation (PD2010_018)

Mental Health Clinical Documentation Guidelines (GL2014_002)

Non-Admitted Patient Activity Reporting Requirements (PD2013_010)

Notifiable Disease Data Security and Confidentiality (PD2012_047)

Notification of Infectious Diseases under the NSW Public Health Act 2010 (IB2013_010)

Perinatal Data Collection (PDC) Reporting and Submission Requirements (PD2010_072)

SNAP Data Collection - Australian National Sub-Acute and Non-Acute Patient (AN_SNAP) Classification (PD2008_025)

NSW Government Open Data Policy

Policies and Guidelines related to Roles and Responsibilities of Staff:

Combined Delegations Manual: *Authority for the disclosure and use of certain information is provided in section 10.1 of this manual.*

NSW Health Code of Conduct (PD2015_049): *defines standards of ethical and professional conduct that are required of everyone working in NSW Health in any capacity, the outcomes we are committed to, and the behaviours which are unacceptable. The code includes six standards, outlining requirements for observing the privacy, confidentiality and security of information obtained during the course of employment within NSW Health.*

Privacy Internal Review Guidelines NSW Health (GL2006_007)

Complaint Management Guidelines (GL2006_023)

To provide an operational framework for dealing with a complaint in accordance with the Complaint Management Policy (PD2006_073)

Public Interest Disclosures (PD2016_027)

This Policy Directive provides procedures for receiving, assessing and managing public interest disclosures in compliance with the Public Interest Disclosures Act 1994

Reporting of corrupt conduct, fraud and Public Interest Disclosures (ISLHD OPS PD 35)

This document outlines ISLHD's internal and external reporting process, including public interest disclosures and reports of corrupt conduct.

Fraud and Corruption Prevention Strategy (ISLHD OPS PROC 64)

The document outlines the framework to ensure staff awareness, and that active fraud and corruption prevention becomes a core responsibility of every staff member

APPENDIX 8: Reference List

Please see below reference documents and services used in the development of the Framework, in addition to the legislation and policy documents listed in Appendix 5, 6 and 7..

- NSW Heath Data Governance: http://internal.health.nsw.gov.au/data/governance/index.html
- Australian Institute of Health & Welfare 2016, *Data Governance Framework 2014,* accessed 02/08/2016, http://www.aihw.gov.au/data-governance-framework/
- Cancer Institute NSW 2016, *Data Governance Policy Version 2.0 2015,* accessed 02/08/2016, https://www.cancerinstitute.org.au/data-research/data-governance
- Data Governance Institute 2015, http://www.datagovernance.com/adg_data_governance_goals/, accessed 21/11/2015
- Health Stats NSW 2015,*Privacy issues and the reporting of small numbers, accessed 16/08/2016, http://www.health.nsw.gov.au/hsnsw/Publications/privacy-small-numbers.pdf*
- National Health & Medical Research Council 2014,*Ethical Considerations in Quality Assurance and Evaluation Activities*
- National Health Information Standards and Statistics Committee 2015, *Guidelines for the Disclosure of Secondary Use Health Information for Statistical Reporting, Research and Analysis 2015*
- New South Wales Department of Health. *NSW Aboriginal Health Information Guidelines. Sydney, 1998,* accessed 28/02/2018 *http://www.ahmrc.org.au/media/resources/ethics/ethics-backgroundresources/281-nsw-health-information-guidelines/file.html*
- NSW Finance & Services, *NSW Government Information Classification and Labelling Guidelines V1.1,* accessed 21/12/2016, https://www.finance.nsw.gov.au/ict/sites/default/files/NSW%20Government%20Classification%20and%20Labelling%20Guidelines%20v1.1%20Oct%202013.pdf
- QLD Government Chief Information Office 2006, *What is Information Architecture* – White Paper 1.0.0, accessed 01/09/2016 https://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2338-information-architecture-white-paper?lnk=QS0xLTIzMzgtMQ
- Queensland Government 2010-16, *Queensland Compact Principles for Data and Information Collection, Storage, Sharing and Use*, accessed 21/11/2015,https://www.communities.qld.gov.au/resources/communityservices/about/corporate-plans/queensland-compact/principles-data-information-sharing.pdf
- Information Management Services Directorate (IMSD)
- NSW ICT Strategy https://www.finance.nsw.gov.au/ict/
- NSW Information Management Framework https://www.finance.nsw.gov.au/ict/priorities/managing-information-better-services/information-management-framework
- eHealth NSW – Business Plan and Strategy for NSW Health 2016 – 2026 http://www.health.nsw.gov.au/eHealth/Documents/eHealth-Strategy-for-NSW-Health-2016-2026.pdf