

Coronavirus (COVID-19) data and application custodianship

Department of Health Policy

QH-POL-477:2020

1. Statement

Queensland Health will ensure appropriate roles and responsibilities for Data Custodians and Application Custodians are implemented to support the effective management of information related to the Novel coronavirus (COVID-19) (coronavirus) within Queensland Health.

2. Purpose

The intent of this policy is to:

- Ensure Data Custodians and Application Custodians are identified, formally approved and have accountability for data and applications that are being accessed to support the effective management of the coronavirus
- Ensure formal approval processes are implemented for access to data to support effective management of the coronavirus within Queensland Health
- Support compliance with the Queensland Health Data and application custodianship policy, including the assignment of roles and responsibilities for the administration and management of data and applications that support effective management of the coronavirus
- Support compliance with the Data and application custodianship standard, including the process required to obtain formal approval of Data Custodians and Application Custodians where these roles do not exist
- Ensure implementation of the Data and application custodianship roles and responsibilities
- Support best practice recordkeeping requirements
- Ensure privacy, confidentiality and security requirements are met.

3. Scope

This policy applies to all employees, contractors and consultants within the Department of Health divisions and business units.

The scope of the policy is:

- Data and applications (clinical and non-clinical), including data in electronic or non-electronic formats created, collected, managed, stored, disseminated and disposed of within Queensland Health.

4. Principles

- **Governed** – Roles and responsibilities are clearly defined and formally assigned through statewide governance.
- **Managed** – Data Custodians and Application Custodians are identified and formally appointed. Complete and accurate records are made, managed and preserved for as long as they are required for business, legislative, accountability and cultural purposes. Records must only be destroyed in accordance with approved retention and disposal schedule(s).
- **Transparent** – The process of identification and formal approval of Data Custodians and Application Custodians is undertaken collaboratively and is available and shared.
- **Privacy, confidentiality and security** – Privacy, confidentiality and security provisions are implemented to maintain record integrity and authenticity by preventing unauthorised access, damage, alteration or misuse.
- **Valued** – Data and applications are recognised as strategic assets.
- **Standardised** – Data and application custodianship terms and definitions are standardised and consistent.

5. Requirements

Queensland Health must:

5.1. Assign roles and responsibilities for data and applications

- 5.1.1. Identify formally approved Data Custodian(s) and Application Custodian(s) that exist for data and application(s) required to be accessed to support management of the coronavirus. Formally approved Data Custodians and Application Custodians are published in the Queensland Health Information Knowledgebase (QHIK).
- 5.1.2. If Data Custodian(s) and Application Custodian(s) for data and applications required to be accessed to support management of coronavirus are not formally approved, formal approval is to be undertaken as defined in the Data and application custodianship standard. This will include engagement with Health Informatics Services (HIS), eHealth Queensland and submission to the Information Management Strategic Governance Committee (IMSGC).
- 5.1.3. Data and application custodianship arrangements are to be identified and formally approved for the following:
 - Office 365 including Microsoft teams for coronavirus data (Data Custodian Chief Health Officer and Deputy Director-General Prevention Division)
 - Coronavirus Data Set(s) (Data Custodian Chief Health Officer and Deputy Director-General Prevention Division)

- Any other application(s), data warehouse(s) and/or data set(s) being used to manage coronavirus within Queensland Health, not listed in QHIK.

5.1.4. Data Custodians and Application Custodians have overall accountability and responsibility for decision making in relation to the data set, data collection and/or application allocated.

A Data Custodian or an Application Custodian may develop a delegation framework permitting the delegation of specified responsibilities to appropriate qualified staff.

5.1.5. Data Custodian and Application Custodian responsibilities are defined in the Data and application custodianship roles and responsibilities document.

5.2. Data Custodian data access request approvals

5.2.1. Where possible ensure Data Custodian authorisation is obtained for the access, use and disclosure of data from the data set, data collection and/or application in compliance with relevant legislative requirements.

For the coronavirus for Queensland Health the State Health Emergency Coordination Centre (SHECC) is the coordination point for the incoming data on arrival activity being collated at a Hospital and Health Service level.

5.2.2. Existing approved Data Custodian(s) and Application Custodian(s) are to be made aware as a matter of priority if the data set, data collection and/or application has been accessed, used or disclosed to support management of the coronavirus.

5.3. Recordkeeping

5.3.1. Data Custodians and Application Custodians must ensure that complete and accurate records to support management of the coronavirus are made, managed and preserved for as long as they are required for business, legislative, accountability and cultural purposes.

5.3.2. Records to support the management of coronavirus must only be destroyed in accordance with approved retention and disposal schedule(s).

- For clinical records displaying evidence of clinical care to an individual patient/client who has coronavirus, these are retained and disposed of in line with the Health Sector (Clinical Records) Retention and Disposal Schedule section 1. Clinical records general.
- For corporate records (administrative), retention and disposal is to be in accordance with the General Retention and Disposal Schedule.

- For corporate records (non clinical functions), these records are to be retained until the draft Health Sector (Corporate) Records Retention and Disposal is approved.

5.3.3. Office 365 (including Microsoft teams) is not an authorised recordkeeping application. Any data that pertains to coronavirus held in Office 365 (including Microsoft teams) must be captured and recorded into an authorised recordkeeping application.

5.3.4. Any data stored in Office 365 (including Microsoft teams) will require appropriate retention and disposal requirements to be implemented, in accordance with the relevant approved Retention and Disposal schedule as listed in 5.3.2.

5.4. Information security

5.4.1. Confidential information must be encrypted prior to emailing outside of Queensland Health.

5.4.2. In alignment with the Information, Communications Technology (ICT) physical access security standard:

- Access controls must apply to all Queensland Health electronic information and ICT equipment to keep information secure. Access controls must be applied to the coronavirus data set and application(s) where the coronavirus data is managed.
- The Application Custodian and the Data Custodian for the coronavirus data and application(s) must ensure the data has been security classified and that physical controls are implemented commensurate with the security classification in accordance with legislative, regulatory and policy requirements.

5.4.3. Data Custodians and Application Custodians are responsible for managing information security matters to ensure compliance with information security policy and standards.

5.5. Access, use and disclosure

5.5.1. Coronavirus data must only be shared with those with a legitimate reason for access where lawful and authorised.

5.5.2. The Data Custodian(s) for the coronavirus is to ensure the conditions for appropriate access, collection, use, storage, sharing and distribution of the data are established, maintained and monitored.

5.5.3. Data Custodian(s) and Application Custodian(s) are to ensure privacy and confidentiality of information in line with legislative requirements (Information Privacy Act 2009 (Qld) and the Hospital and Health Boards Act 2011 (Qld)) and are responsible for privacy breach management.

6. Legislation

- *Electronic Transactions (Queensland) Act 2001*
- *Evidence Act 1977 (Qld)*
- *Hospital and Health Boards Act 2011 (Qld)*
- *Information Privacy Act 2009 (Qld)*
- *Private Health Facilities Act 1999 (Qld)*
- *Public Health Act 2005 (Qld)*
- *Public Records Act 2002 (Qld)*
- *Public Sector Ethics Act 1994 (Qld)*
- *Public Service Act 2008 (Qld)*
- *Right to Information Act 2009 (Qld)*

7. Supporting documents

Queensland Government

- [Code of Conduct for the Queensland Public Service](#)
- [Information access and use policy \(IS33\)](#)
- [Information asset custodianship policy \(IS44\)](#)
- [Information security assurance and classification guideline](#)
- [Information security classification framework \(QGISCF\)](#)
- [Information security policy \(IS18:2018\)](#)
- [Records governance policy](#)
- [Records governance policy implementation guide](#)

Queensland Health

- [Clinical Records Management Policy](#)
- Coronavirus (COVID-19) data and application custodianship guideline
- [Corporate Records Management Policy](#)
- [Data and application custodianship roles and responsibilities](#)
- [Data and application custodianship standard](#)
- [Data and application custodianship toolkit](#)
- [ICT physical access security standard](#)
- [Information Management Framework](#)

- [Information Security Policy](#)
- [Information Security Standard](#)
- [List of approved Data and Application Custodians](#)
- [Management and access to documents and records factsheet](#)
- [Privacy breach management](#)
- [Queensland Health Data and application custodianship policy](#)
- [Queensland Health Information Knowledgebase \(QHIK\)](#)

Queensland State Archives

- [General Retention and Disposal Schedule](#)
- [Health Sector \(Clinical Records\) Retention and Disposal schedule \(QDAN683\)](#)

8. Definitions

Term	Definition
Application	A software system deployed by the agency which has part of an agency's business process embedded with it.
Application Custodian	A position designated with overall accountability and responsibility for decision making in relation to the ongoing development, management, compliance, care and maintenance of an application to support business needs.
Clinical Record	A collection of data and information gathered or generated to record the clinical care and health status of an individual or group. Also referred to as a Health Record, Medical Record, Healthcare Record.
Confidential Information	Relates to patients of Queensland Health who may be living or deceased.
Corporate Record	Records that provide evidence of administrative and non clinical functions.
Data	The representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means. Typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not information until it is utilised in a particular context for a particular purpose.
Data Collection	The systematic gathering of data designed to address a specific set of business needs which may be from various sources, including manual entry into application(s), questionnaire(s),

Term	Definition
	<p>interview(s), observation, existing record(s) and electronic device(s).</p> <p>A data collection is a type of data set for a specific named purpose.</p> <p>Supports clinical care, funding, management, planning, monitoring, improvement, research and evaluation of health and health services.</p>
Data Custodian	<p>A position designated with overall accountability and responsibility for decision making in relation to the data set, data collection and / or application allocated and the ongoing capture, compliance, development, management, care and maintenance of data to support business needs.</p>
Data Set	<p>A set of data items that is collected for a specific purpose.</p> <p>A data set may comprise a smaller grouping (or subset) of data which, though limited by some constraint or feature type, is located physically within a larger data set.</p>
Data Warehouse	<p>Data warehouses are central repositories of integrated data from one or more disparate sources. They store current and historical data and are used for creating analytical reports for knowledge workers throughout the enterprise. Data warehousing are systems used for reporting and data analysis, and are considered core components of business intelligence.</p>
Delegation Framework	<p>A delegation framework ensures that the most appropriate individuals (officers) can act autonomously to make decisions on behalf of a Data Custodian or an Application Custodian, if required.</p>
Personal Information	<p>Any information or opinion about an identifiable living individual.</p>
Record	<p>Recorded information created or received by an entity in the transaction of business or the conduct of affairs that provides evidence of the business or affairs and includes:</p> <ol style="list-style-type: none"> a) Anything on which there is writing b) Anything on which there are marks, figures, symbols or perforations having a meaning for persons, including persons qualified to interpret them c) Anything from which sounds, images or writings can be reproduced with or d) A map, plan, drawing or photograph.

Version Control

Version	Date	Comments
1.0	7 February 2020	<i>New Policy</i>