Coronavirus (COVID-19) data and application custodianship

Department of Health Guideline

QH-GDL-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.

This guideline provides detail to support the coronavirus data and application custodianship policy.

2. Scope

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

The scope of the guideline 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.

3. Requirements

The following guideline is to be adopted within Queensland Health:

3.1. Assign roles and responsibilities for data and applications

3.1.1. Relevant staff involved in the coronavirus initiative must identify if data and application custodianship arrangements are in place for the relevant data and application(s) required to be accessed. This is to be done by checking the Queensland Health Information Knowledgebase (QHIK).

Within QHIK, search for the application(s) name that contains the data to be accessed. If the application(s) are listed, the data and application custodianship arrangements have been formalised through statewide governance. If the application(s) are not listed, the data and application custodianship arrangements have not been formalised.

3.1.2. If data and application custodianship arrangements are not in place for the data and/or application(s) required to be accessed, the relevant staff involved in the coronavirus initiative are to follow the steps as defined in the Data and application custodianship standard.

The Data Custodian for the coronavirus data is the Chief Health Officer and Deputy Director General Prevention Division. The Application Custodian

requires identification and formal approval. This will be progressed by Health Informatics Services (HIS), eHealth Queensland through the Information Management Strategic Governance Committee (IMSGC).

3.1.3. The steps outlined in the Data and application custodianship standard are to be applied for the following data and applications:

- Office 365 including Microsoft teams for coronavirus data
- Coronavirus Data Set(s)
- Any other application(s), data warehouse(s) and/or data set(s) being used to manage coronavirus within Queensland Health where data and application custodianship arrangements are not listed in QHIK.

3.1.4. The Data Custodian and/or Application Custodian for relevant coronavirus data may implement a delegation framework in accordance with the Data and application roles and responsibilities.

For coronavirus data there maybe consideration whether some functions are delegated to the State Health Emergency Coordination Centre (SHECC) and/or the Chair of SHECC.

3.2. Data Custodian data access request approvals

3.2.1. Where possible documented authorisation is required from the Data Custodian(s) for the access, use and disclosure of data. Data Custodian(s) may have different processes for requestors seeking access to data. The relevant staff involved in the coronavirus initiative are to confirm the required process for data access with the Data Custodian(s) of the relevant data.

The Data Custodian(s) is responsible for approving or declining the request. The Data Custodian(s) also have responsibility for defining any conditions under which authorisation is provided, if required.

3.2.2. Retrospective authorisation is required from a Data Custodian(s) in the case where data has been accessed urgently to support the management of coronavirus. Where this has occurred, retrospective authorisation must be obtained by the Data Custodian(s) as a matter of priority and in alignment with 3.2.1.

3.3. Recordkeeping

3.3.1. Data Custodian(s) and Application Custodian(s) must ensure:

- Full and accurate records to support management of the coronavirus are created routinely to provide evidence of decisions and activities.
- Records that are not created as part of a business process must be created as soon as practicable following the event.
- Records must be appraised at the time of creation to identify recordkeeping requirements and appropriately manage records of continuing value.

- Information security classification and labelling must be applied in accordance with the Queensland Health information security policy framework (see section 3.4.2).
- Emails (including attachments) identified as records must be captured into an approved recordkeeping application as a record.

3.3.2. Records must be sentenced using a current Queensland State Archives approved retention and disposal schedule(s) as follows:

- General Retention and Disposal Schedule (GRDS)
- QDAN 678 v.1 – GRDS for Digital Source Records
- QDAN 683 v.1 – Health Sector (clinical records) Retention and Disposal Schedule

Data Custodian(s) and Application Custodian(s) must plan for how and when they will dispose of records, using a risk based approach.

The relevant staff involved in the coronavirus initiative are to contact the Corporate Information Management team within Risk, Audit and Information Management Branch, Corporate Services Division for advice in relation to the appropriate sentencing in accordance with the GRDS.

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.

Records must be disposed of in a planned and authorised way by:

- Developing and implementing a disposal plan, which details disposal decisions and actions. The Plan must, at a minimum, cover:
    - Disposal endorsement, including how internal endorsement is given.
    - Disposal methods, including how records will be disposed of (physical and digital).
    - Disposal frequency, including specifying how often certain types of records will be disposed of.
    - Formally documenting the disposal of records.

The relevant staff involved in the coronavirus initiative are to prepare the plan for Data Custodian(s) and Application Custodian(s) approval.

3.3.3. Data Custodian(s) and Application Custodian(s) must review records created in Microsoft Outlook (emails) and Office 365 (including SharePoint, OneDrive, OneNote, Teams) and must ensure that these records are managed and retained in accordance with an approved retention and disposal schedule(s) (see section 3.3.2).

3.3.4. Information related to coronavirus must be captured into an approved recordkeeping application.

Relevant staff of the coronavirus initiative must refer to the Corporate Records Management policy for information regarding the approved recordkeeping application(s).

The Data Custodian(s) and Application Custodian(s) are to identify any transitory and short-term records that have been created to support management of the coronavirus within Queensland Health. Transitory and short term records are created as part of routine transactional business practice and are only required to be kept for a short period of time. As described in the GRDS, these records do not need to be formally captured into an approved recordkeeping application.

3.4. Information security

3.4.1. There are a number of information security resources available in relation to the use of secure email, which is intended to provide secure encrypted email facilities to communicate sensitive and private information between Queensland Health and external Health Practitioners.

Relevant staff involved in the coronavirus initiative should review the following resources:

- Secure transfer service
- Information security standard
- Office of the Information Commissioner (Qld) guideline: Health Agencies – Data Quality and Data Security.

3.4.2. Access controls for data and application(s) related to the management of coronavirus within Queensland Health must be:

- Compliant with legislative requirements and
- Consistent with business requirements and information classification.

3.4.3. Engagement with the Cyber Security Group is required.

Relevant staff involved in the coronavirus initiative must meet obligations to maintain security defined requirements and where required complete an Information Security Risk Assessment Process.

3.5. Access, use and disclosure

3.5.1. Access to information relating to coronavirus must be managed to protect the security and privacy of the data held by Queensland Health.

3.5.2. Please refer to section 3.2 for the processes relating to Data Custodian(s) approval for data access requests.

3.5.3. Data Custodian(s) and Application Custodian(s) must report any incidents of inappropriate use and/or access to coronavirus data, including privacy breaches.

Data Custodian(s) and Application Custodian(s) must ensure privacy and confidentiality of the coronavirus data in line with the National Privacy Principles (NPPs) set out in schedule 4 of the Information Privacy Act 2009 (Qld) (IP Act) and strict confidentiality obligations found in Part 7 of the Hospital and Health Boards Act 2011 (Qld) (HHB Act), including the department's Privacy Plan and Confidentiality General Principles. This means if handling information:

- it shall only be shared with those with a legitimate reason for access where lawful and authorised and within the constraints of information sharing agreements.
- it shall not be disclosed unless permitted by one of the exceptions in Part 7 of the HHB Act.
- it shall be in accordance with the NPPs, as set out in schedule 4 of the IP Act.
- Note: Where doubt exists as to the handling and sharing of Queensland Health information, advice should be sought from either the Legal Branch in the Department of Health or the relevant Hospital and Health Service legal team, whichever is applicable.

4. 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)*

5. 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)
    - Office of the Information Commissioner (Qld) guideline: Health Agencies – Data Quality and Data Security
    - Records governance policy
    - Records governance policy implementation guide
- Queensland Health
    - Clinical Records Management Policy
    - Confidentiality General Principles
    - Coronavirus (COVID-19) data and application custodianship policy
    - Corporate Records Management Policy
    - Cyber Security Group
    - Data and application custodianship nomination template
    - 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 Risk Assessment Process
    - Information Security Standard
    - List of approved Data and Application Custodians
    - Management and access to documents and records factsheet
    - Management of statewide data and application custodianship roles process
    - Privacy Breach Management
    - Privacy Plan

- Queensland Health Data and application custodianship policy
- Queensland Health Information Knowledgebase (QHIK)
- Secure Transfer Service

- Queensland State Archives
  - General Retention and Disposal Schedule
  - General Retention and Disposal Schedule for Digital Source Records (QDAN678)
  - Health Sector (Clinical Records) Retention and Disposal schedule (QDAN683)

6. 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), interview(s), observation, existing record(s) and electronic device(s). A data collection is a type of data set for a specific named purpose.

Term	Definition
	Supports clinical care, funding, management, planning, monitoring, improvement, research and evaluation of health and health services.
Data Custodian	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.
Data Set	A set of data items that is collected for a specific purpose. 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.
Data Warehouse	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.
Delegation Framework	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.
Personal Information	Any information or opinion about an identifiable living individual.
Record	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: 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.

Term	Definition
Transitory and Short-term records	Records that have a low or limited value (and therefore are only required to be kept for a short period of time (e.g. 2 days, 1 week, until business use ceases). They are generally created as part of routine transactional business practices and are not required to support the business functions (of an agency. They also have little or no value to the agency or community.

Version Control

Version	Date	Comments
1.0	7 February 2020	*New Guideline*