Queensland Health

Creation of corporate records

Department of Health Standard

QH-IMP-467-2:2019

1. Statement

Public Authorities are required to make 'full and accurate records' of their activities in accordance with the *Public Records Act 2002*. The creation and capture of records helps to ensure reliable and dependable evidence of business decisions and activities is available when required.

This standard describes the requirements for the identification, creation and capture of Corporate Records in the Department of Health (the Department). It is part of the Corporate Records Management Policy Framework which exists to ensure records are made, kept, and where possible, disposed appropriately.

2. Scope

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

It applies to:

- corporate records – it does not include clinical records.
- all formats (physical and digital) regardless of the system in which they are maintained.

This standard may be adopted, or re-branded, for use by Hospital and Health Services (HHS) or statutory bodies.

3. Requirements

3.1. Creation

The creation of records may occur as a natural consequence of business (e.g. writing a letter, email or report) or as a deliberate action after an event (e.g. drafting minutes or file notes). Records must have Queensland State Archivist authorisation to be lawfully disposed.

3.1.1. Full and accurate records must be created routinely to provide evidence of decisions and activities.

3.1.2. Records that are not created as part of a business process must be created as soon as practicable following the event.

3.1.3. Security classification and labelling must be applied in accordance with the Queensland Health Information Security Policy Framework.

3.1.4. Analogue records must be created on appropriate quality materials having regard to the likely use, and the required retention period of the records.

Refer to Appendix 1 – Paper Formats *for more information regarding the selection of appropriate quality of paper to meet the retention and use requirements. For other formats such as film or plans, contact Corporate Information Management for advice.*

3.1.5. Digital records must be created using a format that is likely to remain accessible and usable for the required retention period of the records.

Refer to Appendix 2 – Digital File Formats *for more information regarding the selection of appropriate digital file formats.*

3.2. Capture

Capture is the act of registering metadata about records and transactions (including notes) and saving the associated records and transactions into an approved recordkeeping system or approved business system.

3.2.1. Information identified as a record must be captured into an approved recordkeeping system or an approved business system.

- transitory and short-term records, as identified in the General Retention and Disposal Schedule do not need to be formally captured into an approved recordkeeping system or approved business system.

3.2.2. Records must be captured as soon as practicable after creation or receipt of the record.

3.2.3. Physical records must be attached to an identifiable file folder.

3.2.4. Responsibility for the capture of records is in accordance with the Corporate Records Management Policy Framework. This includes:

- The creator of an internal or outgoing record
- The recipient of an incoming record

- A staff member delegated responsibility (e.g. an Executive Support Officer).

Refer to Appendix 3 – Responsibilities for Capturing of Records for more information about who is responsible for capturing of different types and in different circumstances.

3.2.5. The capture of records should include minimum mandatory recordkeeping metadata in accordance with the Queensland Government Recordkeeping Metadata Standard and Guideline. This includes (but is not limited to):

- **Agent metadata:** creator, recipient etc.
- **Record metadata:** title, format, security, location, dates created / registered etc.
- **Function metadata:** business classification.

3.2.6. Security and access controls must be applied as soon as practical upon receipt and capture of records to limit access to staff with a legitimate need to know. This includes:

- **personal information** must be collected and stored in accordance with the National Privacy Principles (Schedule 4, *Information Privacy Act 2009*)
- **confidential information** must be secured, and the confidentiality of the information maintained, in accordance with the *Hospital and Health Boards Act 2011*
- Other **sensitive and protected information** must be secured as defined in the Department's Information Classification and Handling Standard.

Private, confidential and sensitive records must be secured to only those employees with a legitimate business 'need to know'. However, security and access controls should not otherwise inhibit shared access to records when it is permissible to do so.

3.2.7. Records deemed vital to operations, or re-establishing operations in the event of a disaster, must have business continuity contingency to ensure the records remain accessible and fit for purpose in the event of an emergency.

3.2.8. Records that are born digital should remain digital where practical.

3.3. Email

Emails are digital messages that can be sent from one person (an author) to one or more recipients. The department uses Microsoft Outlook for email and Microsoft Lync for messages.

Emails that are public records must be captured into an approved recordkeeping system, or approved business system. Microsoft Outlook, Skype and the Enterprise Vault are not suitable for the retention of emails or messages that are records.

3.3.1. Emails (including attachments) identified as records must be captured into an approved recordkeeping system or an approved business system as a record. This includes government business conducted via private email accounts.

3.3.2. All parts of an email, including attachments, links, graphics and sound must be captured to retain the context, content and structure of the email.

3.3.3. Email sequences (one or more replies) and email threads (forwarded to additional recipients) must capture the complete history of the communication to ensure the value of the record is preserved.

3.3.4. To mitigate the risk of non-capture by waiting until the end of a sequence (as the end may not always be apparent), capture should occur at significant points where decisions are made, the subject changes, or issues are addressed.

3.3.5. Emails must be captured by the creator of internal or outgoing emails, and the recipient of incoming emails.

Refer to ***Appendix 3 – Responsibilities for Capturing of Records*** *for more information about who is responsible for capturing emails in different circumstances.*

3.4. Social Media and Smart Devices

Social media is comprised of websites and computer programs that allow people to communicate and share information on the internet using a computer or smart device.

3.4.1. Records published using official departmental Social Media accounts (e.g. Facebook, Twitter, LinkedIn and Yammer) must be captured as a record as soon as practical after creation.

3.4.2. Records created or received on mobile or smart devices (e.g. iPad, Tablets and Smart Phones) must be captured as a record as soon as practical after creation.

3.4.3. Public records created or received in a private social media or messaging account must be captured into an approved recordkeeping system or approved business system within 20 calendar days of creation or receipt.

3.5. Approved Business Systems

Business systems are systems designed to perform a business process or processes. Whilst they may create, receive, manage and maintain business information and transactions that meet the definition of a record, their primary function is not concerned with the management of this information as public records.

An approved business system (for the purpose of recordkeeping) is a system that has been assigned a Data Custodian and/or Application Custodian in accordance with the Data and Application Custodianship Policy.

3.5.1 Records created or received within approved business systems are not required to also be captured into an approved recordkeeping system. Exceptions include records within:

- Microsoft Outlook (emails and calendar entries)
- Skype (messages)
- Microsoft Enterprise Vault (email archives)
- Back-ups and archives (Backup tapes, CD, DVD, External Drives etc.)
- Microsoft 365 (i.e. SharePoint, OneDrive, OneNote, Teams etc.).

4. Legislation

4.1. Queensland Government Legislation

- *Electronic Transactions (Queensland) Act 2001*
- *Evidence Act 1977*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2019*
- *Hospital and Health Boards Act 2011*
- *Information Privacy Act 2009*
- *Public Health Act 2005*
- *Public Records Act 2002*
- *Public Service Act 2008*
- *Right to Information Act 2009*

4.2. Queensland Government Information Standards:

- Information Access and Use Policy (IS33)
- Information Asset Custodianship Policy (IS44)
- Information Security Policy (IS18:2018)
    - Queensland Government Information Security Classification Framework
- Queensland Recordkeeping Metadata Standard and Guideline
- Records Governance Policy
    - Records Governance Policy – Implementation Guideline

5. Supporting documents

5.1. Corporate Records Management Policy Framework:

- Corporate Records Management Policy
- Corporate Records Roles and Responsibilities Standard
- Creation of Corporate Records Standard (this document)
- Use of Corporate Records Standard
- Digitisation Disposal of Corporate Records Standard
- Disposal of Corporate Records Standard
- Identification of Corporate Records Guideline

- Data Entry and Naming of Corporate Records Guideline
- Disposal of Corporate Records Guideline

5.2. Other Related Documents:

- Clinical Records Management Policy
  - Retention and Disposal of Clinical Records Standard
- Code of Conduct for the Queensland Public Service
- Information Security Policy
  - Information Security Standard
  - Information Security Roles and Responsibilities Standard
  - ICT Physical Access Security Standard
- Data and Application Custodianship Policy
  - Data and Application Custodianship Roles and Responsibilities
- Electronic Approval Policy
  - Electronic Approval Guideline
  - Electronic Approval Impact Assessment
- Instrument of Delegation for the Public Records Act 2002

6. Definitions

Term	Definition
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. See also: *Data Custodian*; *Approved Business System*
Approved Business System	An approved business system (for the purpose of recordkeeping) is a system that has been assigned a Data Custodian and/or Application Custodian in accordance with the Data and Application Custodianship Policy. Custodians are responsible for understanding, managing and controlling risks associated with applications and the collections of data held within these applications. They are also responsible for ensuring that legal, regulatory, policy, standards and other business requirements of the application continue to be met. See also: *Application Custodian*; *Data Custodian*
Approved Recordkeeping System	An approved recordkeeping system refers to the Department's electronic Document and Records Management System (eDRMS) or legacy Records Management System, RecFind.
Business Classification Scheme (BCS)	A BCS is a records management tool used to categorise information resources in a consistent and organised manner. It is comprised of a hierarchy of terms that describe the broad business functions of the department and the activities and transactions that enable those functions to be delivered.
Capture	A deliberate action which results in the registration of a record into a recordkeeping system. For certain business activities, this action may be designed into electronic systems so that the capture of records is concurrent with the creation of records.
Clinical Records	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 or healthcare record. Refer Clinical Records Management Policy (QH-POL-280:2014). See also: *Corporate Records*

Term	Definition
Confidential Information	In this standard, confidential information has the same meaning as 'confidential information' in the *Hospital and Health Boards Act 2011*, namely: ***confidential information*** *means any information that ––* *(a) is about a person who is receiving or has received a public health sector health service; and* *(b) could identify the person.* Confidential information most often relates to patients of Queensland Health (including deceased persons) and can include information such as patient UR number, name, address, date of birth, admission and discharge dates, billing information, Medicare number, medical record and referrals (note this list is not exhaustive). For further information, you can refer to the Department's Confidentiality General Principles to understand the duty of confidentiality and the circumstances when 'confidential information' may be disclosed. It is an offence to disclose 'confidential information' about a person unless one of the exceptions in Part 7 of the HHB Act applies. See also: *Information Privacy*; *Personal Information; Right to Information*
Corporate Records	Records that provide evidence of administrative and non-clinical functions of the Department (e.g. executive correspondence, finance, human resource, legal, research, scientific, cancer screening etc.). See also: *Clinical Records*
Corporate Records Management	The application of efficient and systematic controls for the creation, receipt, maintenance, use and disposal of Corporate Records.
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. See also: *Application Custodian*; *Approved Business System*
Digital Records	Records created, communicated and/or maintained by means of electronic or computer technology, including both 'born digital' records and records that have been digitised. See also: *Physical Records*

Term	Definition
Disposal	In this standard, disposal has the same meaning as 'disposal' in the Public Records Act 2002, namely: disposal, of a record, includes–– a) destroying, or damaging the records, or part of it; or b) abandoning, transferring, donating, giving away or selling the record, or part of it. Records disposal includes the following activities. • **Destroy:** complete and irreversible physical erasure of the record, ensuring it cannot be reconstituted, recreated or reconstructed. • **Transfer:** permanent transfer to another public authority because of a machinery-of-government change. • **Sell:** records cannot be sold, except if an agency or function is sold or privatised (i.e. under a machinery-of-government change). • **Donate:** giving records to a museum or historical society must be authorised by the State Archivist. • **Loss or damage:** because of a disaster or other circumstances beyond your agency's control, such as contamination. • **Abandon:** neglect, which can lead to loss or damage to records, is a form of disposal. • **Amend:** unauthorised changing of a record by addition, deletion, revision or obliteration of information, particularly if it modifies the meaning or intent of the record's content or renders it unusable.
Document	Recorded information or an object which can be treated as a unit. Some documents are records because they have been part of a business transaction, or were created to document such a transaction. Conversely, some documents are not records because they do not function as evidence of a business transaction. See also: *Record*
Electronic Document and Records Management System (eDRMS)	An eDRMS is a system that combines electronic document management with records management functionality by enabling appropriate contextual information (metadata) to support the evidential value of the information. The recordkeeping metadata assist users to find, manage, control and understand the records over time
Electronic Records	See *Digital Records*.

Term	Definition
Evidence	Documentation, records or proof of a business transaction that can be shown to have been created in the normal course of business activities and which are inviolate and complete. It is not limited to the legal sense of the term.
Information	Information is any collection of data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, and textual or numerical form. For the purpose of this document the terms, data, information and records are considered synonymous.
Identifiable File Folder	A folder printed, stamped or otherwise marked in a manner that it can be clearly identified as the property of the Department.
Information Privacy (IP)	Information Privacy for Queensland Government is legislated through the Information Privacy Act 2009 (IP Act) which recognises the importance of protecting the personal information of individuals. Under the IP Act, health agencies must comply with the privacy principles contained in the IP Act, which include the nine National Privacy Principles (NPPs) and provisions regarding contracted service providers and the transfer of personal information out of Australia. These rules govern how personal information must be collected, stored, used and disclosed. The IP Act also allows an individual to seek access to their own personal information or make a complaint about a breach of the privacy principles. See also: *Right to Information*; *Personal Information; Confidential Information*
Information Security	The protection of information from unauthorised use or accidental modification, loss or release. Information security is based on three elements: • confidentiality – ensuring information is only accessible to authorised persons; • integrity – safeguarding the accuracy and completeness of information and processing methods; and • availability – ensuring that authorised users have access to information when required

Term	Definition
Metadata	Data that describes the content, context and structure of records. Metadata is structured or semi-structured, descriptive information about a record and usually includes the title of the record, author, date created, any changes to the record, and applicable disposal or sentencing information. Recordkeeping metadata enables a record to be managed over time and assists in identifying and retrieving records and supporting long term record functionality, reliability, and effective preservation or disposal authentication.
Personal Information	Personal information is information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about a person whose identity is apparent or whose identity can be reasonably ascertained from the information or opinion. See also: *Confidential Information; Information Privacy; Right to Information*
Physical Records	A record that is tangible and takes up physical space (e.g. paper, photographs or index cards) See also: *Digital Records*
Record	In this standard, record has the same meaning as 'record' in the *Public Records Act 2002*, namely: ***record** means 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 without the aid of anything else; or* d) *a map, plan, drawing or photograph*

Term	Definition
Recordkeeping	The making and maintaining of complete, accurate and reliable evidence of business transactions in the form of recorded information. Recordkeeping includes: • the creation of records in the course of business activity • the means to ensure the creation of adequate records • the design, establishment and operation of recordkeeping systems • the management of records used in business and as archives.
Recordkeeping System	A system capable of capturing, maintaining and providing access to records over time.
Records Management	Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.
Retention Period	The minimum period of time that records need to be kept before their final disposal as specified in an authorised retention and disposal schedule.
Right to Information (RTI)	The RTI process established by the Queensland Government aims to give the community greater access to information, and also provides the right to apply for access to government held information, unless on balance it is contrary to the public interest to provide that information. This process is governed by the following two statutory instruments: • Right to Information Act 2009 which allows you to apply for access to documents held by Queensland Government agencies • Information Privacy Act 2009 which in addition to the privacy principles, allows individuals to apply for access to, and amendment of, their own personal information held by Queensland Government agencies. See also: *Confidential Information; Information Privacy; Personal Information*
Vital Records	Records that an agency could not continue to operate without and which would be needed to re-establish the agency in the event of a disaster and satisfy ongoing core business responsibilities.

Version Control

Version	Date	Comments
v1.0	19 February 2019	*Initial draft in consideration of changes to Queensland Government policies and information standards.*
v1.0	1 July 2019	*Approved.*
v1.1	20 October 2021	*Approved. Minor amendments (updated references to legislation, standards and policies).*
V1.2	25 October 2022	*Minor amendments. (Change Branch name as a result of Department of Health's Business Case for Change from Risk, Assurance and Information Management Branch)*

Business Area Contact

Corporate Information Management is responsible for the strategic direction and support of the Corporate Records Management function of the Department.

Please refer any corporate records management queries, or feedback to:

Corporate Information Management Unit
Governance, Assurance and Information Management Branch
Corporate Services Division
Department of Health

Phone: (07) 3082 0582
Email: Records-Corporate@health.qld.gov.au
Intranet: https://qheps.health.qld.gov.au/csd/business/records-and-information-management

Appendix 1 Paper Formats

For records required for long term or permanent retention it is important to ensure the records remain 'fit for use' for as long as they are required to be retained.

Paper breaks down chemically and physically as it ages and the chemical degradation can contaminate and react with other records. Aged paper may also become fragile and is more susceptible to damage when handled. How well paper lasts over time is determined by the quality and type of paper used in addition to how it is stored, used and handled.

The type of paper used should be according to the retention requirements, use and likely storage conditions. The paper type will contribute to the preservation of the records.

Examples of Paper Formats			
Paper Type	**Permanent Paper**	**Office Paper**	**Thermal Paper**
Retention and Use Requirements	• Permanent and long-term Records *(more than 30 years)* If library and archival conditions are ***not*** met use: • NAA approved paper If library and archival conditions ***are*** met use: • NAA approved paper or • ISO9706 or AS4003 paper If the records are subject to frequent use and handling: • ISO9706 or AS4003 paper	• Short-term Records *(less than 30 years)* Includes both recycled and non-recycled paper: • ISO9706 paper	• Transitory Records. Not recommended for records. If records are captured on thermal paper they should be copied to an alternate paper type

Thermal paper. Thermal paper is highly unstable and is not recommended for use. The text can fade within months and may not last longer than 5 years. Records created on this paper should be copied to a better quality paper or scanned electronically.

Office Paper. Office paper should meet ISO9706 standard. It may include non-recycled or recycled paper (measured as a percentage of the paper's weight which may not be detailed on the product label making it difficult to gauge its durability and longevity). Recycled paper may be adequate for records of short-term retention, drafts and other casual use.

Permanent Paper. Permanent paper must meet certain standards and specifications. Paper advertised as lasting 100 years, 'durable', 'acid-free', 'lignin-free' and 'buffered' does not necessarily meet these relevant standards. Archival paper will be watermarked or have packaging labelled with a statement of compliance with the relevant standard(s):

- ISO9706/AS4003: Australian Standard for Permanent Paper
- National Archives of Australia (NAA) archival paper for records with a retention period of 30 years or more (see following registered trademark)
- ISO18916 Imaging materials – used for photographic prints.

Papers that meet ISO 9706/AS 4003 are available from most stationery suppliers (for more information visit the following ForGov website: '[Choose the right materials and formats]'.

Appendix 2 – Digital File Formats

The choice of file format may impact upon the longevity of digital records. The choice of format is more critical the longer a record is to be kept.

Example of Digital File Formats			
File type	**Open Formats** (low risk)	**Open proprietary formats** (moderate risk)	**Closed proprietary formats** (high risk)
Word processing	• OpenDocument Text (ODT)	• MS Word (DOC) 1997-2010 • MS Office Open XML (DOCX)	• MS Word (DOC) pre 1997 • Rich Text Format (RTF) • WordPerfect (WPD)
Spreadsheet	• OpenDocument Spreadsheet (ODS)	• MS Excel (XLS) 1997-2010 • MS Office Open XML (XLSX)	• MS Excel (XLS) pre 1997 • Quattro Pro (QPW, WQ1, WQ2, WB1, WB2, WB3) • Lotus 1-2-3 (WKS, WK2, WK3, WK4)
Presentation	• OpenDocument Presentation (ODP)	• MS PowerPoint (PPT) 1997-2010 • MS Office Open XML (PPTX)	• MS PowerPoint (PPT) pre 1997 • Corel Presentation (SHW)
Images	• Portable Network Graphics (PNG) • JPEG 2000 (JP2) • JPEG File Interchange Format (JFIF) • Tagged Image File Format (TIFF) • Graphics Interchange Format (GIF) • Digital Negative (DNG)	• JPEG (JPG) • Bitmap (BMP)	• RAW image formats • Paint Shop Pro (PSP) • Photoshop Document (PSD) • HD Photo (HDR) • JPEG XR (JXR) • PCX (PCX)
Document exchange	• Portable Document Format (PDF)	• Open XML Paper Specification (XPS)	
Vector graphics	• Scalable Vector Graphics (SVG) • OpenDocument Graphics (ODG)	• AutoCAD Drawing Exchange Format (DXF)	• CorelDraw (CDR) • Adobe Illustrator (AI)
Graphics metafiles	• Computer Graphics Metafile (CGM)	• Windows Enhanced Metafile (EMF)	• Windows Metafile (WMF) • WordPerfect Graphics Metafile (WPG)

Video	• Matroska (MKV) • Ogg (OGV) • Motion JPEG 2000 (MJ2)	• Flash Video (FLV) • MPEG-4 (MP4)	• Windows Media Video (WMV, ASF) • DivX Media Format (DMF, DIVX) • Audio Video Interleaved (AVI) • QuickTime (QT, MOV) • Real Media (RM)
Audio	• Free Lossless Audio Codec (FLAC) • Ogg (OGA) • MPEG-4 (M4A)	• MPEG-2 Audio Layer 3 (MP3)	• Windows Media Audio (WMA, ASF) • Waveform Audio (WAV) • Real Audio (RA, RAM) • Audio Interchange File Format (AI, AIFF)

Avoid high risk file formats where possible, including those:

- that are or will soon be obsolete
- that are no longer supported by the developer
- where the developer will not share information about the format
- that use 'lossy' compression techniques
- accessed or read with unsupported hardware or software
- restricted by intellectual property or that use digital rights management

File formats for long-term temporary and permanent records should be:

- based on open, documented standards (those developed by standards organisations)
- an open/open proprietary format as opposed to closed proprietary
- developed by a community rather than by single vendor
- portable (can be independent of specific hardware, operating systems and software)
- commonly used (at least within a specific community of practice)
- not encumbered by intellectual property restrictions
- uncompressed or use lossless compression
- unencrypted.

For more information visit the Queensland Government – Recordkeeping webpage '[Choose the right materials and formats]'.

Appendix 3 – Responsibilities for Capturing Records

The general responsibility for the capture of a record lies with the:

- **Creator of internal records:** records created within and distributed within the Department
- **Creator of outgoing records:** records created within and distributed outside of the Department
- **Receiver of incoming records:** records created outside of the Department and distributed to one or more people within the Department.

Responsibilities for the capture of particular records types are identified in the below table:

Responsibilities for Capturing Records			
Record Type Responsibilities	**Creator** (or Delegated Officer)	**Receiver** (or Delegated Officer)	**Info Asset Custodian** (Collector/Processor)
Executive Correspondence	✓		
General Incoming Correspondence		✓	
General Outgoing Correspondence	✓		
Forms			✓
Social Media			✓
Audio/Video			✓
Email - Internal	✓		
Email - Incoming		✓	
Email - Outgoing	✓		

The creator (sender) of an internal email is responsible for the capture of sent emails. This includes:

- **Single email:** The sender of the email
- **An email sequence**: The sender of the first email of a sequence (a sequence is considered an email conversation which contains one or more replies)
- **An email thread:** The sender of the first email of a thread (a diverted/forwarded email) which may result in a new/related issues and which may not include the original sender.

The receiver of an email that originated external to the Department is responsible for the capture of the received email. This includes:

- **Single recipient:** The receiver of the email is responsible for capture.
- **Multiple recipients:** The first listed '@health' recipient in the 'TO' list is responsible for capture.
- **CC and BC recipients:** The nature of 'CC' (carbon copy) and 'BC' (blind copy) suggests the email is for reference and is not required to be actioned.