Queensland Health

Information access, use and disclosure

Queensland Health Digital Standard

QH-IMP-484-2

1. Statement

The purpose of this standard is to facilitate lawful and appropriate information access, use and disclosure. Confidentiality and privacy of information is governed by legislation including:

- The *Hospital and Health Boards Act 2011 (HHBA)* prohibits disclosure of information that may identify a patient/client (i.e., confidential information) to any other person, including staff, unless an exception under Part 7 of the Act applies.
- The *Information Privacy Act 2009* applies to the handling of all personal information, including collection, security, access, use and disclosure of personal information.
- The *Human Rights Act 2019* protects a person's right to privacy, family, home, or correspondence being unlawfully or arbitrarily interfered with.
- Code of Conduct for the Queensland Public Service.
- *Public Health Act 2005.*

This standard supports the Use of ICT services and devices policy. This standard must be applied in conjunction with the Use of ICT services and device policy and supporting standards. It applies to all information (clinical and corporate) in all formats (physical, electronic and hybrid) that is created, collected, managed, stored, disseminated, and disposed of by Queensland Health.

2. Scope

This standard applies to all staff within Queensland Health.
Staff is defined as employees, students, interns, volunteers, contractors, consultants, Board and committee members, third-party providers, and managed service providers working for Queensland Health. Queensland Health consists of:

- the Department of Health, and
- Hospital and Health Services.

3. Requirements

3.1. Information access, use and disclosure

3.1.1. Appropriate and relevant information is to be available to the right person, in the right place, at the right time, to ensure optimum service delivery while not compromising information security, privacy and confidentiality of information.

3.1.2. Information is to be shared in a timely and secure manner, where there is demonstrated need and benefit, and it is legally permissible to do so.

3.1.3. All information must be classified appropriately as per the Information classification and handling standard and managed as per the Queensland Health Information Asset Standard.

3.1.4. All Queensland Health employees are bound by a legal duty of confidentiality to protect private, personal, confidential, or otherwise sensitive information they may come into contact with during the course of their work. The obligation to maintain confidentiality also applies between staff members.

3.1.5. Staff must respect the confidentiality of official information even after ceasing employment with Queensland Health.

3.1.6. Staff must not use information gained by or conveyed to them for any other purpose other than for the discharge of their official duties.

3.1.7. Staff undertaking projects must consider the privacy and confidentiality implications of their projects.

3.1.8. Staff must not procure or use any service to store or process or use Queensland Health information, including free or trial cloud-based applications and artificial intelligence technologies, without prior assessment of the privacy, confidentiality and security risks, legislative compliance and the appropriate approval being received.

3.2. Access to Personal and Confidential Information

3.2.1. Confidential, personal, or otherwise sensitive information that requires additional handling or use must be secured according to legislative, regulatory and policy requirements.

3.2.2. Confidential and personal information must only be shared with those with a legitimate reason for access where lawful and authorised, and where applicable, within the constraints of information sharing agreements and permissions.

3.2.3. Personal and confidential information collected for specific purposes (such as care and treatment) must not be used or disclosed for secondary purposes without consent, except where it is permitted under legislation.

3.2.4. Authorised users must only access, use or disclose confidential, personal, and sensitive information when it is required for, and consistent with, the performance of the functions and duties of their role and in accordance with relevant legislation and authorisations.

3.2.5. Staff personal information must not be disclosed to third parties without the appropriate consent or lawful authority.

3.2.6. Staff must not access their own records, or their own personal or confidential information, including medical records and results, whether paper-based or electronic, except through approved processes or access mechanisms. Approved processes or access mechanisms include the Information Privacy Act 2009 and the Right to Information Act 2009, Queensland Health's MyHR system, and external mechanisms such as your My Health Record account.

3.2.7. Staff must not disclose or discuss with family or friends any personal, sensitive or confidential information about colleagues, patients or clients.

3.2.8. Staff must not inappropriately use Queensland Health systems or records, to access, use or disclose personal, confidential or official information held by Queensland Health for personal reasons.

3.3. Access to Information Systems

3.3.1. Only staff in positions with appropriate delegations are to authorise user access to information systems.

3.3.2. Access permissions must be limited to only those staff who have a genuine work requirement to access the information and limited to the minimum access level they need to perform their duties.

3.3.3. Access to information systems must only be authorised where:

- access is required for and consistent with the performance of the user's role and responsibilities; or
- access directly relates to the care of a patient; or
- access is directly related to approved data, research, audit, review, or quality activities.

3.3.4. Staff must not look up personal, confidential or health information of a friend, family member or colleague, unless required to undertake their duties or under relevant legislation.

3.3.5. Staff must not inappropriately use Queensland Health systems or records, to access, use or disclose personal, confidential or official information held by Queensland Health for their own personal interests, curiosity or gain.

3.3.6. The ability to access a system does not give staff authorisation to look up personal, sensitive or confidential information, including health information, at the request of a friend, family member or colleague.

3.3.7. Staff must not access a system to look up sensitive or confidential corporate information not directly related to their duties or when accessing is not provided for under relevant legislation, including:

- Viewing timesheets of other people

- Payroll information of other people
- HR information of other people.

3.3.8. Access must be reviewed, and where necessary removed, when staff move positions, this includes when moving positions within the same organisation. Access must be removed when staff leave the organisation.

For further information please see Access control standard.

3.4. Right to information/Open Data

3.4.1. The Right to Information (RTI) process is the Queensland Government's approach to giving the community greater access to information. The Queensland Government has made a commitment to provide access to information held by the government in accordance with the *Right to Information Act 2009*.

3.4.2. Queensland Health will publicly release information in a way that is meaningful and useful to the public, except where the release of information is contrary to the public interest or is restricted by legislation or law.

3.5. Non-compliance

3.5.1. Unauthorised access to information systems can constitute a criminal offence and may be referred to the Queensland Police Service or other relevant authorities.

3.5.2. Any staff member who accesses, uses, discloses, or modifies personal, sensitive, or confidential information other than in accordance with legislation and this standard may breach privacy and confidentiality requirements which may result in disciplinary action, up to and including termination of employment.

3.5.3. All inappropriate access, use or disclosure of personal or confidential information is to be reported in accordance with your local policy and process for reporting corrupt conduct.

3.5.4. All suspected or confirmed privacy breaches should to be referred to your local Privacy and Confidentiality Officers at the earliest opportunity.

Human rights

The standard aligns with the Human Rights Act 2019, emphasising adherence to its principles. This ensures that our operations prioritise legal compliance and respect for individual rights.

Legislation

- *Anti-Discrimination Act 1991*
- *Crime and Corruption Act 2001*
- *Criminal Code Act 1899*
- *Cybercrime Act 2001*
- *Electronic Transactions (Queensland) Act 2001*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2019*
- *Hospital and Health Boards Act 2011*
- *Human Rights Act 2019*
- *Information Privacy Act 2009*
- *Medicines and Poisons Act 2019*
- *Public Health Act 2005*
- *Public Interest Disclosure Act 2010*
- *Public Records Act 2002*
- *Public Sector Act 2022*
- *Public Sector Ethics Act 1994*
- *Right to Information Act 2009*
- *Telecommunications Interception Act 2009*
- *Telecommunications (Interception and Access) Act 1979 (Cth).*

Supporting documents

- Use of ICT services and devices policy
  - Audit and recordkeeping standard
  - Collaboration platforms standard
  - Monitoring and reporting standard
  - Training, awareness and disciplinary procedure standard
  - Use of digital communication standard
  - Use of ICT services and devices standard
- Data and application custodianship policy
- Data and application custodianship standard
- Discipline HR Policy E10

- Information Security Policy
  - Access control standard
  - External access standard
  - Information security classification and handling standard
- Patient Safety Alert 04/2024: Use of mobile phones by clinicians in clinical settings
- Performance improvement HR Policy G11
- Queensland Health Use of Mobile Phone Position Statement
- Requirements for reporting suspected corrupt conduct HR Policy E9
- Suspension of employment HR Policy E14
- Workplace conduct and ethics HR Policy E1.

Public Service Commission:

- Code of Conduct for the Queensland Public Service
- Private Email Use policy
- Use of Internet and email policy.

Queensland Government Enterprise Architecture (QGEA)

- Use of ICT services, facilities and devices policy (IS38)
- Information access and use policy (IS33)
- Information asset custodianship policy (IS44)
- Information Security Policy (IS18:2018)
- Records governance policy.

4. Additional resources

For information please contact your local Privacy and confidentiality officers.
https://www.health.qld.gov.au/system-governance/contact-us/access-info/privacy-contacts

For more information on accessing Queensland Health information please see:
https://www.health.qld.gov.au/system-governance/contact-us/access-info

5. Definitions

Term	Definition
Authorised use	Use by individuals who have received authorisation before operating the relevant device or service and agreed to abide by the policies, guidelines, and local practice arrangements for use of the relevant facility or device, and who have appropriately acknowledged this agreement where required.
Confidential information	(a) information, acquired by a person in the person's capacity as a designated person, from which a person

Term	Definition
	who is receiving or has received a public sector health service could be identified; or (b) information accessed by a prescribed health practitioner under section 161C (2) HHBA 2011
Corporate records	Records that provide evidence of administrative and non-clinical functions of Queensland Health (e.g. executive correspondence, finance, human resource, legal, research, scientific, cancer screening etc.).
Information Security classification	As per the Information Security Classification and Handling Standard.
Official information	Official information is routine information without special sensitivity or handling requirements.
Personal information	Information or an opinion (including information or opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained from that information or opinion. See also Sensitive Information.
Privacy breach	A privacy breach occurs when there is a failure to comply with one or more of the privacy principles set out in the Information Privacy Act 2009 (Qld) (IP Act). A privacy breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.
Private information	Private information means information that has been provided for specific purposes by an individual and the individual can reasonably expect will not be made public And information about behaviour that in a context in which an individual can reasonably expect that no observation or recording is taking place.
Sensitive information	Sensitive information is a subset of personal information and can include (but not limited to) any of the following: racial or ethnic origin; political opinions; religious beliefs, sexual preferences; criminal record; or health information. Sensitive information is information that requires additional handling or care due to its sensitivity or moderate business impact if compromised or lost. Examples of Sensitive information include:

Term	Definition
	• All clinical information except information pursuant to the *Child Protection Act 1999 (Qld)* and *Mental Health Act 2016 (Qld)* • Financial and procurement information • General documents and records pursuant to Queensland Health's legal and regulatory obligations • Contractual documents and records containing commercially sensitive information Information about physical or technical aspects of Queensland Health networks, servers, or workstations.
Unauthorised disclosure	Unauthorised disclosure refers to the release or dissemination of sensitive information, data, or material without proper authorization, breaching established protocols, policies, or legal frameworks within the Queensland government. This may include unauthorised access to confidential documents, sharing of classified information without clearance, or any action that compromises the security, integrity, or confidentiality of government information assets
Unauthorised use	Access that has not been authorised including use which is inappropriate, unlawful and/or criminal

For further ICT definitions please refer to:

Digital policy glossary

Approval and implementation

Policy Custodian	Policy Contact Details	Approval Date	Approver
Deputy Director-General eHealth Queensland	Digital-policy@health.qld.gov.au	17/10/2024	Director General

Version control

Version	Date	Comments
1.0	01/03/2021	New standard. Endorsed by Architecture and Standards Committee. Approved by the Director-General.
2.0	17/10/2024	Cyclic review See Change Table below. Endorsed IMSGC Endorsed ISC

Version	Date	Comments
		Endorsed ASC Approved Director-General.

Change Table

Section	Change
Statement	Reworded Dot point reworded for greater clarity: *The Hospital and Health Boards Act 2011* (HHBA) prohibits disclosure of information that may identify a patient/client (i.e., confidential information) to any other person, including staff, unless an exception under Part 7 of the Act applies.
	Reworded Dot point reworded for greater clarity: The Information Privacy Act 2009 applies to the handling of all personal information, including collection, security, access, use and disclosure of personal information. Reference to National Privacy Principles removed.
	New dot point New dot point added: The *Human Rights Act 2019* protects a person's right to privacy, family, home or correspondence being unlawfully or arbitrarily interfered with.
Scope	Alignment to policy statement removed – added to Statement. Updated to include committee members and third-party providers.
3. Requirements 3.1	New requirement 3.1.3. All information must be classified appropriately as per the Information classification and handling standard and managed as per the Queensland Health Information Asset Standard.
	Requirement updated 3.1.4 Updated to include All Queensland Health employees are bound by a legal duty of confidentiality to protect private, personal, confidential or otherwise sensitive information
3.2	Requirement updated 3.2.1 Updated to include Confidential, and personal or otherwise sensitive information that requires additional handling or use must be classified and must be secured according to legislative, regulatory and policy requirements.
	3.2.2 Updated to include 'and permissions.
	Requirement updated 3.2.4 ~~The duty of confidentiality in regards to confidential and personal information is specifically provided for in the HHBA~~.

Section	Change
	Authorised users must only access, use or disclose confidential, personal, and sensitive information when it is required for, and consistent with, the performance of the functions and duties of their role and in accordance with relevant legislation and authorisations.
	Requirement updated 3.2.6. Staff must not access their own records, or their own personal or confidential information, including medical records and results, whether paper-based or electronic, except through approved processes or access mechanisms. Approved processes or access mechanisms include the Information Privacy Act 2009 and the Right to Information Act 2009, Queensland Health's MyHR system, and external mechanisms such as your My Health Record account.
	New requirement 3.2.7. Staff must not disclose or discuss with family or friends any personal, sensitive or confidential information about colleagues, patients or clients.
3.3	New requirement 3.3.4. Staff must not look up personal, confidential or health information of a friend, family member or colleague, unless required to undertake their duties or under relevant legislation.
	New requirement 3.3.5. Staff must not inappropriately use Queensland Health systems or records, to access, use or disclose personal, confidential or official information held by Queensland Health for their own personal interests, curiosity or gain.
	New requirement 3.3.6. The ability to access a system does not give staff authorisation to look up personal, sensitive or confidential information, including health information, at the request of a friend, family member or colleague.
	New requirement 3.3.7. Staff must not access a system to look up sensitive or confidential corporate information not directly related to their duties or when accessing is not provided for under relevant legislation, including: • Viewing timesheets of other people • Payroll information of other people • HR information of other people.
	New requirement

Section	Change
	3.3.8. Access must be reviewed, and where appropriate removed, when staff move positions, this includes when moving positions within the same organisation, and access must be removed when staff leve the organisation. For further information please see Access control standard.
3.5	Requirement updated 3.5.1. Unauthorised access to information systems can constitute a criminal offence and may be referred to the Queensland Police Service or other relevant authorities.
	New requirement 3.5.2. Any staff member who accesses, uses, discloses, or modifies personal, sensitive, or confidential information other than in accordance with legislation and this standard may breach privacy and confidentiality requirements which may result in disciplinary action, up to and including termination of employment.
	New requirement 3.5.4. All suspected or confirmed privacy breaches should to be referred to your local Privacy and Confidentiality Officers at the earliest opportunity.
Human Rights	New requirement (Added to support the *Human Rights Act 2019*) The standard aligns with the *Human Rights Act 2019*, emphasising adherence to its principles. This ensures that our operations prioritise legal compliance and respect for individual rights.