Queensland Health

Use of digital communication

Queensland Health Digital Standard

QH-IMP-484-3

1. Statement

The purpose of this standard is to provide direction to staff regarding the use of digital communication channels for the purpose of communicating information, including sensitive information, with other staff, healthcare professionals, patients/guardians, third party providers and suppliers, whilst ensuring matters such as information privacy, confidentiality and security are addressed.

All Queensland Health staff members are required to handle and protect all personal information including, but not limited to, patient and staff information, in compliance with the *Hospital and Health Boards Act 2011* and *Information Privacy Act 2009.* This includes how the information is collected, managed, stored, disseminated, and disposed of by Queensland Health.

This standard supports the Use of ICT services and devices policy and should be applied in conjunction with the policy and all supporting standards.

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, managed service providers working for Queensland Health. Queensland Health consists of:

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

Digital communication is any communication that uses electronic devices to share messages or collaborate with others. The scope of this standard includes, but not limited to:

- Committee/Consumer groups
- eConsult
- Email consultation
- SMS communication
- Patients/guardians Outpatient One-Way SMS Messaging

Out of scope

- Use of social media for official purposes.

3. Requirements

3.1. Obligations

3.1.1. All Queensland Health staff must comply with all legislative and Queensland Health policy requirements when communicating work-related information electronically.

3.1.2. Queensland Health staff should assess and use the most appropriate authorised electronic devices and communications methods for specific business purposes.

3.1.3. All staff must maintain the highest standards of security and professionalism when using digital communication channels and tools.

3.2. Official, Sensitive and Protected information

3.2.1. Sharing, disclosing, or releasing information outside of Queensland Health must be performed in accordance with applicable sharing and records management policy.

3.2.2. Information classified as 'OFFICIAL' may be sent and received using authorised digital communication channels.

3.2.3. Information classified as 'SENSITIVE' (including clinical, personal, and confidential information) and above, requires extra controls be applied and should only be sent when there is a legitimate and approved need to do so and in compliance with the *Hospital and Health Board Act 2011* and *Information Privacy Act 2009*. For more information refer to the Queensland Health Information Security Management System Framework.

3.2.4. Where sensitive information is being sent outside of Queensland Health and appropriate controls are not in place, approval should be sought from the line manager. Approving managers should:

- Follow their local authorisation process
- Consider security requirements and risks
- verify that the intended recipient has a legitimate business need and the right to access the sensitive information, and
- ensure the decision is recorded for audit purposes.

3.2.5. Personal, sensitive, and confidential information must not be transferred or sent outside of Australia, including via email, unless the legislative requirements set out in section 33 of the *Information Privacy Act 2009* have been met.

3.3. Business Email use

3.3.1. All Queensland Health staff must ensure that all government business is conducted through official Queensland Health email addresses - @health.qld.gov.au. Queensland Health email accounts can be accessed from personal devices – as part of the BYOD service and Office365 platform.

3.3.2. Email accounts are provided to staff to use for official purposes. Limited personal use is permitted as per the Use of ICT services and devices policy. Staff should consider security risks when using Queensland Health work emails for non-work related purposes.

3.3.3. Staff should be aware that employee email accounts may be monitored and accessed where there are concerns regarding security of compliance with the email account. Email accounts may be subject to access under the Right to Information and Information Privacy legislation.

3.3.4. Staff must not forward in an email business information, whether in a picture or attachment, to a personal email account unless authorised.

3.3.5. Staff must not craft emails or messages, or construct attachments, in a way that attempts to bypass content inspection software. For more information refer to the Use of ICT services and devices – ICT monitoring and reporting standard.

3.3.6. The use of private email accounts or systems (such as Gmail, Hotmail, Outlook or similar) and messaging applications (such as Facebook Messenger, Snapchat, and WhatsApp), for government related business is prohibited as it poses privacy and security risks, prevents the proper management of records, and is not compliant with legislative requirements.

3.3.7. The Director-General or a Health Service Chief Executive may allow an employee or a group of employees or external parties to use a private email account in certain situations (e.g., in emergency, disaster, IT systems limitations) provided adequate systems and processes are in place to ensure that resulting records are captured by the relevant record keeping systems, and sensitive information is protected.

3.4. Communication with Patients/Guardians

3.4.1. Queensland Health is committed to providing a patient/consumer centric service shaped around the health needs of individual patients, their families, and communities.

3.4.2. Face-to face visits, telephone, or telehealth (video call) appointments should be used as the primary method to communicate sensitive health and patient information.

3.4.3. Digital communication channels, including email and SMS, can be used to communicate information, including sensitive information, with patients and/or guardians, with their consent.

3.4.4. Business areas must undertake a risk assessment to assess the impact on the confidentiality, security, and privacy of the patient's personal and confidential information prior to implementing digital communication processes.

3.4.5. SMS communication for sensitive information may increase the likelihood of information breaches. Business areas should evaluate the potential risks and, where possible, consider using more secure electronic channels.

3.4.6. Staff using SMS to share sensitive information must only do so using an approved ICT system or service or a corporate device.

3.4.7. Consent to communicate with patients using electronic channels must be obtained prior to any digital communication activity being undertaken.

3.4.8. Staff collecting consent from patients/guardians to receive digital communication must ensure that the principles for informed consent are fulfilled and meet all legislative requirements set out, but not limited to, the:

- *Hospital and Health Boards Act 2011*
- *Public Sector Act 2022*
- *Public Sector Ethics Act 1994*
- *Information Privacy Act 1999*
- *Human Rights Act 2019.*

3.4.9. Consent should be obtained using an approved consent form and stored on the patients record. Where verbal consent has been obtained, the consent must be documented within the patient record and indicate the type of digital communication the patient has consented to.

3.4.10. Consent requirements apply to one way SMS and email messaging services, push notification services, and reply confirmation messaging services. For example: Outpatient One-Way SMS Messaging, SMS Message Media, Do-not-reply SMS or email messages.

3.4.11. Patients must be made aware of the conditions of use for electronic communication, the process for opting out explained to them and the risks associated with electronic communication methods.

3.4.12. Local procedures should be developed to outline how consent is to be captured, review frequency and where electronic communications are stored.

3.4.13. All clinical records must be captured within the patient's record.

3.5. Recordkeeping

3.5.1. Email communication sent and received through a Queensland Health email account are public records or documents within the meaning of the *Public Records Act 2002* and Queensland Government Enterprise Architecture Records governance policy. These records should be managed according to departmental and Hospital and Health Service recordkeeping requirements.

3.5.2. Where a communication is received through a private email account or messaging app that relates to government business it must be treated as a public record under the *Public Records Act 2002* and the obligations regarding recordkeeping under the Act must be complied with.

3.5.3. If a record relating to government business is received in a private email account, the email must be forwarded from the private email account to the employee's Queensland Health email account within 20 days of receipt of the email. If a response is required to an email received in a private email account, a Queensland Health email account must be used to respond.

3.5.4. The disposal of public records within a private email account or messaging application that are not captured in an approved record keeping system can be a breach of the *Public Records Act 2002*.

3.5.5. Public records can only be destroyed in accordance with the *Public Records Act 2002*, Queensland Government Enterprise Architecture Records governance policy, and an approved retention and disposal schedule.

3.6. Right to Information

3.6.1. All digital communication sent and received by Queensland Health staff are considered to be 'documents of an agency' and are therefore subject to the access provisions of the *Right to Information Act 2009* and *Information Privacy Act 2009.* This applies regardless of the type of digital communication format used.

3.6.2. A document of an agency includes any document the Department of Health or the relevant Hospital and Health Service is entitled to access, or which is in their physical possession or legal control, as long as it is not a document to which the legislation does not apply.

3.6.3. The *Right to Information Act 2009* contains both protections and offences for certain actions taken under the Act.

4. 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.

5. 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*
- *Invasion of Privacy Act 2009*
- *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 and Access) Act 1979 (Cth).*

6. 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 email 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
- Records governance policy

7. Additional resources

For more information on privacy and confidentiality 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
For more information consent please see:
Guide to Informed Decision-making in Health Care

8. Definitions

Term	Definition
Confidential information	This definition is extracted from, and has the meaning given in, Part 7 of *the Hospital and Health Boards Act 2011* as follows:

Term	Definition
	(a) information, acquired by a person in the person's capacity as a designated person, from which a person 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) *Hospital and Health Boards Act 2011*
Consent	For consent to be valid, an individual must have the capacity to agree, and the agreement must be voluntary, informed, specific and current. It is important to note that consent is not always required to collect, use or share personal information as some legislative provisions mandate these requirements (e.g., in areas such as criminal justice or child protection).
Digital communication channels	Refer to the various methods and platforms through which information is exchanged electronically.
eConsult	A form of virtual care that allows healthcare workers across Queensland, both Hospital and Health Service (HHS) staff and, non-HHS primary care clinicians, to ask a clinical question of a more senior or more specialised clinician about their patient. https://qheps.health.qld.gov.au/caru/telehealth/what-is-telehealth/econsult
Informed consent	Informed consent means that a patient has received the relevant information in a way they can understand, to enable them to make an informed decision and they have voluntarily given permission for the health care service to be provided. In an ethical sense, the agreement by a patient to receive public sector health services reflects the end point of a process of engagement in which one or more health practitioners have supported the patient to come to an informed decision to agree to the health care offered.
Official information	Information without special sensitivity or handling requirements. Examples of official information include: • ICT project plans • Training materials • System log files Phone and email directories
One way messaging	One-way SMS is a type of SMS message in which the recipient can only read the message and cannot respond to it. This is often used for broadcasting messages such as promotional messages, reminders, appointments or alerts.
Personal information	This definition is extracted from, and has the meaning given in, the *Information Privacy Act 2009*:

Term	Definition
	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.
PROTECTED information	Information that requires a substantial degree of control as compromise could cause serious damage to the State, the Government, commercial entities, or members of the public. Examples of Protected information include: • Information under the protection of the *Child Protection Act 1999* and *Mental Health Act 2016*, such as the address details of a patient under the protection of a Mental Health Court confidentiality order, pictures, videos, or detailed clinical reports of children under the protection of the *Child Protection Act 1999*. Cardholder data (that includes the Primary Account Number (PAN)).
Push notification	Push notification is the delivery of information from a software application to a computing device without a specific request from the client.
SENSITIVE Information Classification	The use of the SENSITIVE classification indicates that information requires additional handling care due to its sensitivity or moderate business impact if compromised or lost. SENSITIVE information must be labelled. Sensitive information as defined in this table is a subset of SENSITVE information.
Sensitive information	This definition is extracted from, and has the meaning given in, the *Information Privacy Act 2009*: 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: • All clinical information except information pursuant to the *Child Protection Act 1999* and *Mental Health Act 2016* • Financial and procurement information • General documents and records pursuant to Queensland Health's legal and regulatory obligations

Term	Definition
	• Contractual documents and records containing commercially sensitive information. Information about physical or technical aspects of Queensland Health networks, servers, or workstations. PROTECTED information is out of scope of this definition.

For further ICT definitions please refer to:

Digital policy glossary

9. 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	17/10/2024	New standard developed. Replaces the Use of email Standard. See Change Table below Endorsed IMSGC Endorsed ISC Endorsed ASC Approved Director-General.

Change table

Section	Change
General	New Use of digital communication Standard developed. All requirements from the Use of email Standard were reviewed and where appropriate transferred to the new standard.
Statement	Updated to cover all digital communication not just email specific.
Scope	Added: Clarification on digital communication and an out of scope included.

Section	Change
3. Requirements	New requirements 3.1 Obligations requirements developed to reflect the use of all digital communication. 3.1.1. All Queensland Health staff must comply with all legislative and Queensland Health policy requirements when communicating work-related information electronically. 3.1.2. Queensland Health staff should assess and use the most appropriate authorised electronic devices and communications methods for specific business purposes. 3.1.3. All staff must maintain the highest standards of security and professionalism when using digital communication channels and tools.
3.2	Requirement transferred 3.4 Official, sensitive and protected information from Use of email standard transferred to 3.2 Requirements renumbered accordingly.
3.3	Requirement transferred 3.2 Private email use from Use of email standard – transferred to 3.3 Business email use and requirements renumbered accordingly.
3.4	Requirement transferred and updated 3.3 Communication with Patients/Guardians from Use of email standard- transferred to 3.4. Following changes made: Removed 3.3.1 Email can be used to communicate with patients and/or guardians, with their consent, and must use the MS Office encryption-only function from QH email accounts about the following: • Provision of health care advice including written follow up instructions and test results (including patient's own information classified as Sensitive) • Appointment information and reminders • Services available, clinic hours and location details • Admission procedure information • Educational handouts 3.3.2 Email communication is not a substitute for care that may be provided during a scheduled appointment.

Section	Change
	New Requirements added 3.4.1. Queensland Health is committed to providing a patient/consumer centric service shaped around the health needs of individual patients, their families and communities. 3.4.2. Face-to face visits, telephone or telehealth (video call) appointments should be used as the primary method to communicate sensitive health and patient information. 3.4.3. Digital communication channels, including email and SMS, can be used to communicate information, including sensitive information, with patients and/or guardians, with their consent. 3.4.4. Business areas must undertake a risk assessment to assess the impact on the confidentiality, security and privacy of the patient's personal and confidential information prior to implementing digital communication processes. 3.4.5. SMS communication for sensitive information may increase the likelihood of information breaches. Business areas should evaluate the potential risks and, where possible, consider using more secure electronic channels. 3.4.6. Staff using SMS to share sensitive information must only do so using an approved ICT system or service or a corporate device. 3.4.7. Consent to communicate with patients using electronic channels must be obtained prior to any digital communication activity being undertaken. 3.4.8. Staff collecting consent from patients/guardians to receive digital communication must ensure that the principles for informed consent are fulfilled and meet all legislative requirements set out, but not limited to, the: • *Hospital and Health Boards Act 2011* • *Public Sector Act 2022* • *Public Sector Ethics Act 1994* • *Information Privacy Act 1999* • *Human Rights Act 2019.* 3.4.9. Consent should be obtained using an approved consent form and stored on the patients record. Where verbal consent has been obtained, the consent must be documented within the patient record and indicate the type of digital communication the patient has consented to.

Section	Change
	3.4.10. Consent requirements apply to one way SMS and email messaging services, push notification services, and reply confirmation messaging services. For example: Outpatient One-Way SMS Messaging, SMS Message Media, Do-not-reply SMS or email messages. 3.4.11. Patients must be made aware of the conditions of use for electronic communication, the process for opting out explained to them and the risks associated with electronic communication methods. 3.4.12. Local procedures should be developed to outline how consent is to be captured, review frequency and where electronic communications are stored. 3.4.13. All clinical records must be captured within the patient's record.
3.5	Recordkeeping – no change
3.6	New section 3.6 Right to information 3.6.1. All digital communication sent and received by Queensland Health staff are considered to be 'documents of an agency' and are therefore subject to the access provisions of the *Right to Information Act 2009* and *Information Privacy Act 2009*. This applies regardless of the type of digital communication format used. 3.6.2. A document of an agency includes any document the Department of Health or the relevant Hospital and Health Service is entitled to access, or which is in their physical possession or legal control, as long as it is not a document to which the legislation does not apply. 3.6.3. The *Right to Information Act 2009* contains both protections and offences for certain actions taken under the Act.
4. 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.