Queensland Health

# Use of Email standard

## Queensland Health Digital Standard

**QH-IMP-484-3: 2021**

# 1. Statement

The purpose of this standard is to provide direction to staff regarding the use of email for the purpose of communicating information, including sensitive information, with other staff, health care professionals, patients/guardians, third party health providers and suppliers, whilst ensuring matters such as information privacy, confidentiality and security are addressed.
All Queensland Health staff members have an obligation under the *Hospital and Health Boards Act 2011* and *Information Privacy Act 2009* to protect personal information including, but not limited to, patient information, collected, managed, stored, disseminated, and disposed of by Queensland Health.

# 2. Scope

This standard supports the Use of ICT services and devices policy and applies to all staff within Queensland Health. Staff. Staff is defined as employees, students, interns, volunteers, contractors, consultants, Board Members 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. Obligations

3.1.1. All Queensland Health staff must ensure that all government business is conducted through their 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 Office 365 platform.

3.1.2. Queensland Health email accounts are for official purposes only. 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.

3.1.3. Staff must not forward in an email official information, whether in a picture or attachment, to a personal email account to avoid official review or scrutiny.

3.1.4. For more information refer to the Use of ICT services and devices – monitoring and reporting Standard.

## 3.2. Private email use

3.2.1. The use of private email accounts or systems (such as Gmail, Hotmail or similar) and messaging applications (such as Facebook Messenger, SnapChat, Wickr Me and WhatsApp), for government related business poses a security risk, prevents the proper management of records, and is prohibited.

3.2.2. The Director General or a Chief Executive may allow an employee or a group of employees or external parties to use a private email account in certain situations (eg. 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.

## 3.3. Communication with Patients/Guardians

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.

## 3.4. Official, Sensitive and Protected information

3.4.1. Official information may be sent and received using QH email accounts.

3.4.2. Information classified as 'sensitive' (including clinical and confidential information), 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 and Information Privacy Act.

3.4.3. Sensitive information sent to Queensland Government agencies or organisations must use the MS Office encrypt function or a higher level of encryption.

3.4.4. Where sensitive information is to be sent to agencies or organisations that do not support encryption, approval should be sought from the manager of the person accessing the information to be sent. Approving managers should verify that the intended email recipient has a legitimate business need and the right to access the clinical information and the decision recorded for audit purposes. The MS

Office encrypt- only function or higher level of encryption must always be used.

3.4.5. The transfer of sensitive information outside of Australia, including via email, must be done in accordance of the Information Privacy Act and for legitimate purposes only. Before sending personal information outside of Australia staff must take the necessary steps to ensure the transfer meets the legislative requirements.

3.4.6. Protected information must be encrypted using strong cryptography when transmitted externally, and when transmitted internally over a network with a lower classification. Email should be the last resort for the distribution of Protected information.

### 3.5. Recordkeeping

3.5.1. All 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 QGEA Records governance policy. These records should be managed according to departmental and HHS recordkeeping standards.

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 app (that are not captured elsewhere) can be a breach of the Public Records Act 2002.

3.5.5. Public records can only be of or destroyed in accordance with the Public Records Act 2002, QGEA Records governance policy, and an approved retention and disposal schedule.

## 4. Legislation

- *Anti-Discrimination Act 1991*
- *Crime and Corruption Act 2001*
- *Criminal Code Act 1899*
- *Electronic Transactions 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*
- *Public Interest Disclosure Act 2010*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*
- *Telecommunications (Interception and Access) Act 1979 (Cth)*
- *Right to Information Act 2009*

# 5. Supporting documents

- Use of ICT services and devices policy
- Access control standard
- Audit and recordkeeping standard
- Collaboration platforms standard
- External access standard
- Information access, use and disclosure standard
- Monitoring and reporting standard
- Training, awareness and disciplinary procedure standard
- Use of ICT services and devices standard
- Information Security policy
- How to email secure information Factsheet
- Methods to securely transfer information (electronically) Factsheet
- Data and application custodianship policy
- Requirements for reporting suspected corrupt conduct HR Policy E9
- Suspension of employment HR Policy E14
- Queensland Government Information Security Classification Framewotk

# 6. Additional resources

Contact the Secure Transfer Service for secure ways to transfer sensitive information: http://qheps.health.qld.gov.au/sts/

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

Outlook Email Encryption

https://qheps.health.qld.gov.au/__data/assets/pdf_file/0034/2498623/outlook-email-encryption.pdf

# 7. Definitions

| Term | Definition |
|---|---|
| Confidential information | (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<br>(b) information accessed by a prescribed health practitioner under section 161C (2) HHBA 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). |
| Official information | **Official Information** is information without special sensitivity or handling requirements.<br>Examples of official information include:<br>• ICT project plans<br>• Training materials<br>• System log files<br>Phone and email directories |
| Personal information | Information or an opinion (including information or opinion forming part of a data-base), 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. |
| Protected information | **Protected Information** is 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.<br>Examples of Protected information include:<br>• Information under the protection of the Child Protection Act 1999 (Qld) and Mental Health Act 2016 (Qld), 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 (Qld) |

| Term | Definition |
| --- | --- |
| | • Cardholder data (that includes the Primary Account Number (PAN) – see section 8 below). |
| Sensitive 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:<br>• All clinical information except information pursuant to the Child Protection Act 1999 (Qld) and Mental Health Act 2016 (Qld)<br>• Financial and procurement information<br>• General documents and records pursuant to Queensland Health's legal and regulatory obligations<br>• Contractual documents and records containing commercially sensitive information<br>Information about physical or technical aspects of Queensland Health networks, servers or workstations. |

For further ICT definitions please refer to:

Digital policy glossary

| Version | Date | Comments |
| --- | --- | --- |
| 1.0 | 01/03/2021 | New standard. Endorsed by Architecture and Standards Committee. Approved by Director-General. |