Queensland Health

Monitoring and reporting Standard

Queensland Health Digital Standard

QH-IMP-484-7: 2021

1. Statement

Queensland Health monitors activity and use of Government owned information and communication technology (ICT) services and devices by all employees, in order to:

- Identify instances of inappropriate or unauthorised use.
- Assist in operational activities, investigations and Right to Information requests.
- Protect system security.
- Protect the rights and property of Queensland Health.
- Ensure compliance with government and Queensland Health policy.
- Ensure compliance with legislation.

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.

NB: BYOD is out of scope for this standard.

3. Requirements

3.1. Monitoring and filtering

Queensland Health protects the operation of the departmental network and seeks to ensure compliance with the Code of Conduct for the Queensland Public Service, legislation and policy by monitoring and/or filtering the use of ICT services and devices.

3.1.1. Monitoring activities may include access to any information that is the property of Queensland Health including documents, messages, email or correspondence that is created, sent, received or stored by Authorised Users on Queensland Health ICT services, facilities and devices.

3.1.2. In monitoring to determine potential breaches to this standard, or security risks to the Queensland Health network, an authorised ICT support or Cyber Security Group personnel, where directed by the authorised delegate, may:

1. Access details of user actions and/or system activities including but not limited to:
   - addresses of internet sites visited.

- the number of incorrect password attempts.
- attempts by unauthorised persons to access Authorised User accounts or systems.
- systems and database/application logs.
- email activity in accordance with 3.3 Employee email and short messaging monitoring and reporting.
- actions or key events for accounts with administrative/ privileged access.

2. Suspend connectivity and access to an ICT device and/or service without notice.
3. Remove or suspend access to all data at any time without notice due to events including:
   - a breach of legislation, policy, order or direction having been detected.
   - a device having been reported lost or stolen.
   - disposal or transfer of the device to another authorised user (permanent data removal).
   - the device no longer being required to connect to Queensland Health's ICT services.
4. Use the results of monitoring for the purposes of detecting breach of legislation, policy, order or direction, malicious and/or suspicious activity, responding to security-related events and alerts or for gathering forensic evidence in accordance with ICT incident management processes.

3.2. Employee internet monitoring authorisation and reporting

3.2.1. The Director-General of Queensland Health or a Hospital and Health Service (HHS) Chief Executive or their approved Human Resources delegate, may authorise eHealth Queensland to undertake a review of a user's internet account where there is reasonable suspicion of unauthorised or inappropriate use.

3.2.2. Monitoring software is in use to protect the security and integrity of Queensland Health's network. This software is also used to help prevent unauthorised internet use, for example, blocking access to inappropriate sites or materials by using filtering software.

3.2.3. Information recorded by the automated monitoring systems can be used to identify an individual user, the site they accessed and the time and duration that they accessed the site.

3.2.4. A Queensland Health user who suspects another user of unauthorised or inappropriate internet use, has a duty to immediately report those matters to their manager. Managers shall assess the information and make the necessary referrals to the approved Human Resources delegate.

3.2.5. Where inappropriate or unauthorised use of Queensland Health's internet is detected through monitoring, it shall be reported to the approved Human Resources delegate, who will be responsible for coordinating an appropriate response including and, if necessary,

instigating action under the relevant disciplinary and conduct policy and procedures.

3.2.6. If unauthorised or inappropriate use is established the user shall be notified in writing of the findings and informed of what, if any, action is to be taken to address the concern.

3.3. Employee email and short messaging monitoring authorisation and reporting

Employee emails 'accessible' to the 'intended recipient' under the Telecommunications (Interception and Access) Act 1979 (Cth)1 may be monitored where there are concerns regarding security or compliance with the email account. Access to an employee's email account may be authorised where required for operational reasons.

Note: Automated electronic scanning of emails sent to Queensland Health email addresses for the purposes of performing 'network protection duties' under the Telecommunications (Interception and Access) Act 1979 (Cth) 2are out of scope.

3.3.1. It is an offence for a person to access a stored communication account[3], without the appropriate authorisation and approval.

3.3.2. Where concerns are raised in relation to security or compliance with the law, including legislation, regarding an employee's email account or stored communication account, managers and supervisor are to report concerns to either the relevant human resources representative, the Chief Legal Counsel, Ethical Standards Unit or a HHS Executive member nominated by the HHS Chief Executive.

3.3.3. The Director-General of Queensland Health or a HHS Chief Executive or specified delegate (3.3.4) may authorise eHealth Queensland to access or monitor an employee's email account or stored communication account where there are concerns about the security and compliance that may warrant further investigation. The authorisation is to be in writing or via email.

3.3.4. Specified delegates are:

- Department of Health Chief Human Resources Officer
- Department of Health Chief Legal Counsel

[1] *Telecommunications (Interception and Access) Act 1979* (Cth) regulates the interception of telephone communications, and it is considered 'highly likely' that it also regulates the interception of other communications using a telecommunications network, for example short message services (commonly referred to as 'SMS' or 'text messages') and emails.

[2] *Examples of this could include scanning for viruses, security threats or flooding attacks and inappropriate content such as pornography, sexually explicit or obscene material.*

[3] *Stored communications, being communications that are not in transit and that have been held by a 'carrier' of communications services, are protected. Common examples of stored communications are emails, text messages and voice mail messages that are not in transit.*

- HHS Executive Member nominated by the HHS Chief Executive
- 'Health service investigators', as defined in the *Hospital and Health Boards Act 2011*, appointed under an instrument of delegation authorising the activity in relation to the investigation.

3.3.5. Access to an employee's email account for operational reasons, must be authorised by the Director-General Department of Health or a HHS Chief Executive or their approved delegate.

3.3.6. An employee's email account or other stored communication account may contain 'personal information' as defined in *the Information Privacy Act 2009* (IP Act). Any person authorised to access an employee's email account must ensure they do so in accordance with the requirements of the IP Act, including the National Privacy Principles.

4. Legislation

- *Anti-Discrimination Act 1991*
- *Crime and Corruption Act 2001*
- *Criminal Code Act 1899*
- *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 Act 2009 (Cth)*
- *Right to Information Act 2009*
- *Telecommunications (Interception and Access) Act 1979 (Cth)*
- *Telecommunications Interception 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
  - Training, awareness and disciplinary procedure standard
  - Use of email standard
  - Use of ICT services and devices standard
- Data and application custodianship policy

- Information Security policy
- Requirements for reporting suspected corrupt conduct HR Policy E9
- Suspension of employment HR Policy E14
- Workplace conduct and ethics HR Policy E1

6. Definitions

For ICT definitions please refer to:

Digital policy glossary

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