Queensland Health

Collaboration platform Standard

Queensland Health Digital Standard

QH-IMP-484-6: 2021

1. Statement

Queensland Health recognises the need for safe, reliable, interoperable, cost effective and standardised methods to collaborate and communicate within Queensland Health and across the Queensland public service. Queensland Health supports the use of collaboration tools which provide an integrated platform to share files, documents, videos and video conferencing, provide training, conduct interviews and other online services.

In line with the Queensland Government's position the core functionality of Microsoft Teams (MS Teams) is to be used by Queensland Health as the primary platform for all intra and inter departmental collaboration. The use of MS Teams as the primary platform does not preclude the use of alternative communications channels or tools where required.

Queensland Health is contractually covered to operate MS Teams under the following arrangements:

- Microsoft Products (including Online Services) (ICTSS.1305)
- Provision of Microsoft Products and Associated Licensing Solution Partner Services (ICTSS.1308)
- Microsoft licences already in place by Queensland government agencies

Note: The choice of tools for collaboration and communication with external users, for example engagement with the public as part of service delivery, is outside the scope of this standard. However, this does not explicitly exclude MS Teams as an option for this.

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. Microsoft Teams (MS Teams)

3.1.1. Queensland Health should use MS Teams as the primary platform for all intra and inter agency collaboration, including instant messaging, ad-hoc voice/video calls and audio/video meetings and other associated online services.

3.1.2. MS Teams may not be deemed an appropriate channel to discuss highly sensitive information due to 'high' confidentiality business impacts.

Information security classifications should be central to decisions to how products such as MS Teams are used. As per the Queensland Government Information Security Classification Framework, information that has been assessed as having a 'high' business impact level to confidentiality (C), integrity (I) or availability (A) may only be stored or processed offshore where:

- a risk assessment related to the C, I and A business impacts has been undertaken; and
- the accountable officer or delegate has documented acceptance of the offshore information risk assessment.

3.2. Alternative collaboration platforms

3.2.1. Where existing collaboration tools have been invested in or are currently being utilised, efforts are to be made to enable interoperability with MS Teams as the preferred platform when operationally viable.

3.2.2. Where an alternative collaboration platform is used, either as a host or attendee, the appropriate risk and privacy assessment is to be performed.

3.2.3. A Queensland Government Enterprise Architecture (QGEA) exemption is required by a division or HHS where MS Teams will not be used as the primary platform for intra and inter agency collaboration.

3.3. Alternative collaboration tools for sensitive information

3.3.1. In Queensland Health supported teleconferencing systems, such as Telehealth and Cisco WebEx, are authorised to be used to deliver services including meetings classified as Sensitive.

3.3.2. Where a Division or HHS elects to adopt an unauthorised and unsupported solution, such as Zoom a risk assessment is to be undertaken and the Chief Information Officer, Queensland Health, advised of the treatments to be implemented to mitigate the risks.

3.4. Collaboration platform security considerations

3.4.1. An appropriate risk-based approach will be used when adopting a collaboration platform.

3.4.2. Key security considerations when deciding on the use of a collaboration platform include:

- classification and sensitivity of information being used within the platform
- privacy policy and terms of use, particularly whether information can be shared or used by third parties.
- responsibility for granting and reviewing access
- ability to remove / block unauthorised attendees
- data sovereignty considerations

- encryption used by the solution for data at rest and data in transit
- role-based access control where possible
- leveraging existing solutions instead of looking for an alternative solution
- platform integration and use of web or dedicated desktop application
- ability to use the application on non-corporate devices (e.g. BYOD)
- ability to remove messages / files sent
- an incident response plan to addresses a security or privacy breach
- availability and quality of technical support in a timely fashion in the event the service is interrupted
- service provider's track record on supporting and maintaining the solution
- reliability and scalability of the service provider's solution
- use of strong encryption mechanisms for information in transit and at rest
- service provider's ability to quickly and effectively patch / remediate any existing or new vulnerabilities
- ability to manage the service provider through SLA's and contract(s).

3.5. Information privacy considerations

3.5.1. When assessing all collaboration platforms, areas need to ensure they understand how data is stored, and whether the product shares information with affiliates and/or other third parties.

3.5.2. The product should only collect information to support the provision of their services. Areas need to understand what information is collected and for what purpose it is used. Caution should be used where products are silent on whether they share data, or have statements stating they share data for 'business purposes', as these types of statements are unclear as to who the data is being shared with and to what degree.

3.5.3. Areas should choose products where they have control of privacy settings and ensure videos are not stored automatically (unless the host has chosen to record the meeting). The option of being able to 'consent' is an important feature, but note sometimes if you don't consent, you don't get to use the services (or sometimes specific features will be disabled).

3.5.4. Regardless of what tool is used the *Information Privacy Act 2009*, including the National Privacy Principles, must be adhered to.

3.6. Ownership of content and copyright

3.6.1. When selecting a product or tool, areas need to ensure they understand where ownership of intellectual property rights, including copyright, resides.

3.6.2. When using video conferencing and posting/sharing content, users should still ensure they are not breaching copyright laws, such as sharing works of others without their consent.

3.7. Recordkeeping

3.7.1. Staff should not use chat type features to record major business decisions unless a record of that decision is kept in an appropriate recordkeeping system.

3.7.2. Records associated with the usage of collaboration tools, including recordings, must be kept in accordance with the requirements of the *Public Records Act 2002*, QGEA *Records Governance policy*, related departmental and HHSs standards and any other recordkeeping policies.

3.7.3. Content created, received or stored by employees in the conduct of or in connection with departmental business are public records or documents within the meaning of the *Public Records Act 2002* and *QGEA Records Governance policy*. These records should be stored according to departmental and HHS recordkeeping standards.

4. Legislation

- *Anti-Discrimination Act 1991*
- *Crime and Corruption Act 2001*
- *Criminal Code Act 1899*
- *Criminal Justice Act 1988*
- *Cyber Crime Act 2001 (Cth)*
- *Electronic Transaction Act 2001*
- *Financial Accountability Act 2019*
- *Hospital and Health Boards Act 2011*
- *Human Rights Act 2019*
- *Information Privacy Act 2009*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*
- *Right to Information Act 2009*

- *Telecommunications (Interception and Access) Act 1979 (Cth)*
- *Workplace Health and Safety Regulation Act 2008*

5. Supporting documents

- Use of ICT services and devices policy
- Access control standard
- Audit and recordkeeping standard
- External access standard
- Information access, use and disclosure standard
- Monitoring and reporting standard
- Training, awareness and disciplinary procedure standard
- Use of email standard
- Use of ICT services and devices standard
- Information Security policy

6. Additional resources

For more information on the use of non-corporate/unsupported teleconferencing services please see:
https://qheps.health.qld.gov.au/__data/assets/pdf_file/0044/2497985/csc-use-of-non-corp-teleconf-systems.pdf

7. Definitions

For ICT definitions please refer to:

Digital policy glossary

Version Control

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