Queensland Health

BYOD Self-managed service

Department of Health Standard

QH-IMP-484-10: 2021

1. Statement

The BYOD (Bring Your Own Devices) self-managed service provides authorised users with access to ICT systems on their personal devices while protecting the confidentiality, privacy, integrity, security and availability of Queensland Health Information.

2. Scope

Compliance with this standard is mandatory.

This standard supports the Use of ICT services and devices policy and applies to all employees, contractors, students, volunteers and consultants within Queensland Health accessing the BYOD Self-managed Service offered by eHealth Queensland.

This Standard relates to personal devices running the following operating systems

- iOS
- Android
- any other operating system facilitated by the BYOD Self-managed Service.

3. Requirements

The BYOD Service be used in accordance with the requirements of the Department of Health *Information Security Standard* and the *Use of ICT services and devices Policy.*

3.1. BYOD service provision

3.1.1 The *ICT Service Catalogue* must be the approved source of information about the BYOD Service.

3.1.2 Personal devices accessing Queensland Health ICT resources and Queensland Health Information must be managed by an enterprise mobile management platform (including a user portal) that applies a security profile to the personal device prior to connecting to any ICT service on the network, including the BYOD Service.

3.1.3 Where there is a proposal for additional Queensland Health ICT services and systems to be made available through the BYOD Service, the proposal must be subject to a risk assessment by the eHealth Queensland ICT Service Provider in consultation with the Application, Service or Business Custodian, eHealth Queensland Cyber Security Group and the Privacy and Right to Information Unit. Refer to the eHealth Queensland ICT External Access Service Security Standard for further guidance.

3.1.4 Enrolment or connection to the BYOD service is at the discretion of the Department of Health. The Department of Health may refuse enrolment or connection of personal devices to the BYOD Service where:

- the device does not meet required minimum-security standards or
- when manufacturer support of the operating system on the device reaches end of life or
- the applicant has not complied with Department of Health requirements for official duties regarding conduct, appropriate use, privacy, security and record keeping in relation to ICT and Information Management, including use of ICT services and information security.

3.2. Authorised User compliance

3.2.1 Access to the BYOD service must only be provided to authenticated Authorised Users.

3.2.2 All Authorised Users of the BYOD Service must comply with the provisions of the BYOD User Agreement and agree to the requirements of the online enrolment process.

3.2.3 Use of the BYOD Service must comply with Department of Health policies, including ICT and information management, and relevant legislation including the Hospital and Health Boards Act 2011, Public Health Act 2005, and Information Privacy Act 2009, particularly regarding disclosure and use of confidential information and personal information as defined in those Acts, and the Public Records Act 2002.

3.2.4 Non-compliance with BYOD service requirements may result in loss of privilege to enrol in the BYOD Service, suspension or termination of existing enrolment, and all Queensland Health Information being removed from the Authorised User's personal device at the discretion of the Department of Health.

3.2.5 Personal devices utilising the BYOD service must comply with the Code of Conduct for the Queensland Public Service, the Department of Health Use of ICT Services Standard and the Queensland Government Enterprise Architecture Information Standard IS38 Use of ICT Services, Facilities and Devices.

3.2.6 Accessing the BYOD Service must not affect conditions of employment or, of itself, accrue to the Authorised User any related benefits or privileges not otherwise able to be accrued by the Authorised User. For example, the ability to claim time for accessing the BYOD Service outside of normal work hours is subject to Queensland Health human resource policies.

3.2.7 Authorised User must have a maximum of three (3) personal devices connected to the BYOD Service.

3.3. Infection control

3.3.1 In order to reduce the risk of bacterial cross-contamination all personal devices used in a clinical setting must be kept clean and should be disinfected between patients.

3.3.2 All personal devices used in a clinical setting undergo regular decontamination.

3.3.3 A review of the appropriateness of personal devices used within high risk clinical areas should be undertaken.

3.4. Security requirements for personal devices and the BYOD service

3.4.1 Enrolment and pre-requisites for use

All requests for enrolling in the BYOD Service must be made through the online ServiceNow and associated processes.

Prior to enrolment in, and during the use of, the BYOD Service, the Authorised User must ensure that:

- The operating system on the personal device is up to date and in the form intended by the manufacturer i.e. not Jailbroken or Rooted.
- Malware is not installed on the personal device.
- Personal information on the device has been copied to a secure backup location if the Authorised User seeks to retain the information.
- The Authorised User must ensure their personal information is current at all times in their Queensland Health Authorised User record.
- It is recommended that mobile security (anti-virus) software is installed and configured with daily updates and real time scanning of local files, emails and attachments to keep the personal device, the BYOD Service and Queensland Health Information, secure.

3.4.2 Security setup on the personal device

The following security settings must be requirements of enrolling one or more Authorised User's personal devices:

- The Authorised User set a device passcode of 6 characters or touchpoints (passcode, password, touch-point pattern or backup access password) on their personal device as a pre-requisite to accessing the BYOD Service.
- The Authorised User will be required to reset the device passcode on the personal device every 90 days.
- The Authorised User set the device to lock after 5 minutes of inactivity
- Maximum of 10 consecutive incorrect access attempts permitted before access to the device is suspended and all information on the personal device is automatically erased, including all personal files (data, photographs, applications, text messages, contacts etc.)

- The security settings on the device must be monitored by the BYOD Service both regularly and on connecting to the BYOD Service with immediate blocking if the device is not compliant with the BYOD Service requirements.
- The BYOD Service will maintain a list of all of the applications installed on the device for security monitoring.

3.4.3 Authorised User security responsibilities

Authorised Users must agree to comply with the following BYOD Service conditions of use as a requirement of enrolling to the BYOD Service:

- Keep the security code on the device secret and not disclosed to any other person.
- Keep the device compliant with all of the security settings required for access to the BYOD Service as outlined in 3.4.2. For assistance please refer to the FAQ & Help Guide: http://qheps.health.qld.gov.au/byod/docs/byod-faq_and_help_guide.pdf
- Do not modify or attempt to modify the configuration of the BYOD Service client App on the device, attempt to circumvent any security measures implemented as part of the BYOD Service or attempt to install malware Apps.
- When connected to the Queensland Health network:
  - do not allow any other person to access Queensland Health Information by way of the device or the BYOD Service
  - do not leave the device connected or unattended without adequate security code protection
  - ensure that all Queensland Health Information and other material incorporating that of a private or confidential nature is viewable only in an environment where the content cannot be observed or heard by persons who are not authorised to access the information
  - do not misuse any Queensland Health Information – for example by using screen capture tools or unauthorised disclosure or copying.

3.5. BYOD Service Managers and administrators' responsibilities

3.5.1 BYOD Service managers and administrators must be responsible for:

- ensuring that Authorised Users of the BYOD Service have been approved through existing approval channels that are available within the online ServiceNow.
- maintaining a register of all Authorised User access to the BYOD Service including the duration and dates of enrolment and suspension per device.
- publishing information about the BYOD Agreement, including any changes, on the Queensland Health intranet including the range and availability of support services for Authorised Users.
- dealing with the personal information of Authorised Users and applicants in accordance with the policies of the Department of

Health and the *Information Privacy Act 2009* which includes the nine National Privacy Principles (NPPs).

- regularly monitoring the BYOD Service portal to ensure that:
  - erasure of Queensland Health Information on devices is performed as soon as possible after notification of the requirement
  - an Authorised User's enrolment is cancelled for staff leaving the employment of Queensland Health permanently or temporarily (e.g. to undertake a secondment in another agency) or no longer requiring the BYOD Service
  - BYOD do not remain enrolled when they have not been in contact with the BYOD Service for a period greater than 30 calendar days unless otherwise agreed with the ICT Service Provider
  - Authorised User and BYOD enrolment is suspended if the same do not comply with BYOD and BYOD Service requirements
  - the security of the portal on the enterprise mobile management platform is adequately maintained.
- ensuring that the BYOD Service client App includes controls to isolate access to the BYOD Service and Queensland Health network from potentially harmful mobile Apps or other security hazards.
- ensuring secure transmission of Queensland Health Information to BYOD.
- periodically auditing and deleting suspended Authorised User accounts that are no longer required to be retained in the BYOD Service portal.

3.6. Privacy and security

3.6.1 Your personal information must be securely stored and only accessible by appropriately authorised staff.

3.6.2 All personal information collected or accessed by appropriately authorised staff must be handled in accordance with the Information Privacy Act 2009.

3.6.3 Your personal information will not be disclosed to other third parties without consent, unless required by law or legislation.

3.6.4 BYOD Service administrators and ICT support staff cannot access the personal files (including email, text messages, contacts, photos, videos and voicemail) of Authorised Users on their BYODs which is not Queensland Health Information.

3.6.5 Information classified as 'In-Confidence' or 'Protected' should not be transferred on to a personal device.

3.6.6 All private data that is acquired after enrolment is removed when a user retires a device or unsubscribes from the service.

For information about how the Department of Health protects your personal information, or to learn about your right to access your own personal information, please see www.health.qld.gov.au.

Note: To protect the personal information of your contacts, it is important that you change the default for your contacts and calendar to your personal email accounts as per the below instructions:

Settings > Contacts > Default Account (for Contacts) or Settings > Calendar > Default Calendar (for Calendar) and choose your personal email account as the default for synchronising your contacts and calendar. For more information please refer to the FAQ & Help Guide

http://qheps.health.qld.gov.au/byod/docs/byod-faq_and_help_guide.pdf

3.7. Recordkeeping

3.7.1 Staff who copy and edit documents on smart devices must reintroduce those documents back into the enterprise repositories at the earliest opportunity in order to prevent loss.

4. Legislation

- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2019*
- *Hospital and Health Boards Act 2011*
- *Human Rights Act 2019*
- *Information Privacy Act 2009*
- *Privacy Act 1988 (Cth)*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*
- *Right to Information Act 2009*
- *Work Health and Safety Act 2011*

5. Supporting documents

- Queensland Health:
    - 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 email standard
    - Use of ICT services and devices standard
  - Information Security Policy
    - Information Security User responsibilities standard
  - Data and application custodianship Policy
    - Data and application custodianship Standard
  - Data Management Policy
  - Discipline HR Policy E10
  - Financial Management Practice Manual
  - Health Service Directive – Enterprise Architecture
  - Corporate Records Management Policy
  - Requirements for Reporting Official Misconduct HR Policy E9
  - Separation of Employment H1
- Code of Conduct for the Queensland Public Service

6. Definitions

Term	Definition
Administrator	An individual responsible for delivering the service in accordance with business requirements.
Apps	A self-contained program or piece of software designed to fulfil a particular purpose, especially as downloaded to a Smart Device.
Authentication	Access control process that verifies the claimed identity of an individual as established by an identification process to prevent unauthorised persons using services or accessing particular content.
Authorised User	An employee, contractor, student, volunteer or consultant of Queensland Health who has a Queensland Health login and has received authorisation before operating the relevant BYOD or BYOD Service and agreed to abide by the policies, guidelines and local practice arrangements for use of the BYOD or BYOD Service and agreed to be bound by the BYOD Agreement when signing up for the BYOD service.
BYOD/Bring Your Own Device	The electronic device, including a Smart Device, owned, leased or operated by an Authorised User which is capable of storing information and connecting to the

Term	Definition
	Queensland Health network for the purpose of accessing the BYOD Service.
BYOD Service	The BYOD self-managed services offered by eHealth Queensland
Custodian	The recognised officer of the Department of Health responsible for implementing and maintaining ICT services and applications according to the rules set by the owner – to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility throughout its lifecycle.
ICT Service Provider	The individual taking primary accountability for an ICT service including its design, objectives, delivery & progression. This is generally an eHealth Queensland technical coordinator role.
Jailbroken	In relation to iOS systems only, the process of bypassing software restrictions put into place by Apple on devices that run the iOS operating system to allow down-loading of non-App Store Apps not supported or authorised by Apple. The process may introduce security threats to the Smart Device and any connected services.
Malware	Software which is specifically designed to disrupt or damage an ICT system, includes computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.
Queensland Health Information	Information, in any form, transmitted to a BYOD by way of the BYOD Service. Information is any collection of data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form.
Rooted	In relation to Android systems only, a modification which allows privileged control (root access) of the Smart Device operating system with administrative access to alter or replace system applications and settings, run specialised Apps and perform operations otherwise inaccessible

Term	Definition
	without the modification. The modification may introduce security threats to the Smart Device and any connected services.
ServiceNow	The online facility for Authorised Users to request access to ICT services, log support requests and maintain their contact details.
Service Manager	An individual who has accountability for managing the service in accordance with business requirements.
Smart Device	An electronic device that offers more advanced computing ability, connectivity and features than a basic phone or device.
Suspended	In the context of the BYOD Service, the record of enrolment of the Authorised User being retained on the BYOD Service portal and the ability to connect to the BYOD Service being disabled for that Authorised User.
Third Party	An individual or an organisation outside of the individual agency that provides labour or services.

Version Control

Version	Date	Comments
1.0	10 May 2016	Approved by Chief Executive
2.0	6 September 2017	Approved by the Architecture and Standards Committee
2.1	18 September 2018	Schedule 1 - User agreement form removed and references to Schedule 1 removed from the body of the standard. Users should always refer to the online form located on ServiceNow - BYOD Self-managed service for the latest version of the BYOD User Agreement Form. 3.4.2 ‘erased’ replaced with ‘removed’. Self-service Centre replaced with ServiceNow.
2.2	9 March 2021	Transferred to new template and repositioned as a standard under the new Use of ICT services and devices Policy.