Bring Your Own Device and NSW Health Smart Devices

Summary The Bring Your Own Device (BYOD) and NSW Health Smart Devices policy enables staff to use NSW Health owned mobile and smart devices (NSW Health Smart Devices) and / or approved personal devices to access NSW Health ICT systems, and establishes a baseline of security requirements for all mobile and smart devices used within the NSW Health network.

Document type Policy Directive

Document number PD2022_011

Publication date 31 March 2022

Author branch eHealth & ICT Strategy Branch

Branch contact (02) 8644 2213

Replaces PD2020_037

Review date 31 March 2025

Policy manual Not applicable

File number H22/19823

Status Active

Functional group Corporate Administration - Asset Management, Communications
Personnel/Workforce - Conduct and ethics, Security

Applies to Ministry of Health, Local Health Districts, Board Governed Statutory Health Corporations, Chief Executive Governed Statutory Health Corporations, Specialty Network Governed Statutory Health Corporations, NSW Health Pathology, Public Health System Support Division, NSW Ambulance Service

Distributed to Ministry of Health, Public Health System, NSW Ambulance Service

Audience All Staff of NSW Health

Secretary, NSW Health

NSW Health

POLICY DIRECTIVE

Bring Your Own Device and NSW Health Smart Devices

POLICY STATEMENT

NSW Health staff can use NSW Health owned mobile and smart devices (NSW Health Smart Devices) and/or approved personal devices to access NSW Health Information and Communications Technology (ICT) systems.

Staff must have appropriate approval to use personal and NSW Health smart devices to access sensitive and security classified information contained within corporate and clinical applications and NSW Health systems.

SUMMARY OF POLICY REQUIREMENTS

This Policy applies to all NSW Health staff, including employees, contractors, service providers, third parties and other persons who have a justified business need to access NSW Health information systems and assets and associated information.

NSW Health provides technical support for NSW Health smart devices via the State-Wide Service Desk (SWSD).

NSW Health does not provide technical support, advice, or consulting services for personal devices, except to enable users to access corporate and clinical applications on NSW Health ICT systems for business purposes.

All mobile devices owned by NSW Health organisations must be managed and administered through a NSW Health mobile device management platform.

NSW Health organisations must establish a process for reviewing applications for staff to bring and use their own personal devices to access sensitive and security classified information contained within corporate and clinical applications.

NSW Health organisations must not allow personal devices to be connected to its corporate network if a mobile device management platform does not manage the personal device.

NSW Health organisations must also deny access to systems if the personal device does not meet local requirements.

NSW Health staff must follow the minimum-security requirements for all devices accessing NSW Health systems that hold sensitive and security classified information:

- Password must meet complexity requirements
- Auto-lock feature enabled
- Devices must be free of malware
- Only install apps from a trusted source
- Remote wipe function enabled

- Encrypted backups enabled
- Minimal information must be shown on lock screens
- Devices must be kept physically secure
- Devices must not connect to unsecure Wi-Fi networks.
- The most up to date operating system and security updates must be installed.
- The device operating system must not be modified.

Users must notify the State-Wide Service Desk (SWSD) and/or local NSW Health organisation ICT department if a NSW Health smart device or personal device being used to access NSW Health ICT systems has been lost, stolen or compromised.

REVISION HISTORY

Version	Approved By	Amendment Notes
PD2022_011 March-2022	Secretary, NSW Health	Amended to include bring your own device requirements.
PD2020_037 October 2020	Secretary, NSW Health	New Policy Directive

CONTENTS

1. BACKGROUND

This Policy sets the responsibilities of NSW Health staff who use NSW Health owned mobile and smart devices (NSW Health smart devices) to access NSW Health Information and Communications Technology (ICT) systems. It also sets the responsibilities of NSW Health organisations' in the provision of bring your own device (BYOD) access and the responsibilities of persons using a personal device to access NSW Health ICT systems.

Risks arise from the possibility that devices can be stolen, lost or compromised and lead to systemic risk exposures such as a large-scale cyber-attack, data leak, exploitation and other malicious activities from interaction with third-party ICT systems. This Policy aims to reduce these risks.

The *NSW Government Information Classification, Labelling and Handling Guidelines* defines sensitive and security classified information, including personal and health information, as information that is in any format, including records in physical and digital format, data sets and physical records.

Any person accessing NSW Health information using mobile and smart devices has a responsibility to maintain the security of sensitive information, including personal health information.

1.1. About this document

This Policy applies to NSW Health staff, including employees, contractors, service providers, third parties and other persons who have a justified business need to access NSW Health information systems and assets, who use issued NSW Health smart devices. It also applies to NSW Health staff who may choose to bring personal devices to access NSW Health ICT systems. NSW Health staff should not download, store or transfer NSW Health sensitive data or information to a personal device that is not enrolled to the NSW Health Mobile Device Management platform.

NSW Health staff requiring remote access to information systems and assets within NSW Health's secure network must refer to NSW Health's Remote Access Policy (PD2020_036).

All NSW Health organisations must have appropriate systems and processes to adequately and appropriately protect their information systems and assets. These systems and processes include, but is not limited to, information security measures and controls and continual improvement processes referred to in the NSW Health Electronic Information Security Policy (PD2020_046).

1.2. Key definitions

Bring your own device	Refers to any smartphone, tablet or laptop device that is not owned or leased by NSW Health—referred to as personal devices.
Mobile device	Mobile handsets, smartphones, tablets and other mobile devices that have similar functions and mobility.

Mobile device management platform	A platform that provides software distribution, policy compliance, inventory management, security management and service management for mobile devices. An example Mobile Device Management (MDM) platform is the NSW Health Mobility Platform.
NSW Health information and communications technology (ICT) systems	NSW Health ICT systems refer to the hardware, software and communication technologies used by NSW Health.
NSW Health mobility platform	Refers to the NSW Health State-Wide mobile device management platform that provides a mechanism for managing, securing and administrating NSW Health smart devices and personal devices.
Smart device	Refers to any smartphone, tablet, laptop, personal computer device or other hybrid devices.

1.3. Legal and legislative framework

NSW Health organisations and staff must meet the requirements of the following:

- *Government Sector Employment Act 2013 (NSW)*;
- *Health Records and Information Privacy Act 2002 (NSW);*
- *Health Records and Information Privacy Regulation 2017* (NSW);
- *Privacy and Personal Information Protection Act 1998 (NSW);*
- *Privacy and Personal Information Protection Regulation 2019* (NSW);
- *State Records Act 1988 (NSW);* and
- *Workplace Surveillance Act 2005 (NSW)*.

2. ELIGIBILITY FOR THE USE OF PERSONAL DEVICES

NSW Health staff can use personal devices to access sensitive and security classified information held on NSW Health corporate and clinical applications on NSW Health ICT systems.

An access form to use a personal device to access specific NSW Health corporate and clinical applications must be submitted in Search and Request Anything (SARA). eHealth NSW or the NSW Health organisations' Information Technology (IT) Team will action the request and enable access if approved. Information on what applications require approval and security requirements can be found on SARA for each application.

NSW Health organisations have specific rules to determine if personal devices may connect to the local NSW Health organisation's network on-site and if this connection is limited in any way. This can include limitations to any access point to NSW Health data and services, not just an on-site or Virtual Private Network (VPN) connection.

NSW Health organisations must not allow personal devices to be connected to its corporate network if a mobile device management platform does not manage the personal device. NSW Health organisations must also deny access to systems if the personal device does not meet local requirements.

Users of a personal device must also comply with the requirements in Section 7 for disposal and ensure they have removed all NSW Health data from the device when they leave the organisation.

Non-compliance with the policy requirements may result in loss of privilege to enrol and access sensitive and security classified information contained within NSW Health ICT systems with a personal device.

2.1. Approval Process for Using Personal Devices

NSW Health organisations must establish a process for reviewing and approving applications requesting to use personal devices for business purposes that require access to specific NSW Health corporate and clinical applications. NSW Health organisations are to follow local approval processes, which must be appropriately documented in SARA.

The use of approved personal devices must comply with the security requirements outlined in Section 6 of this Policy.

All costs associated with the use of personal devices are the sole responsibility of the device owner.

3. TECHNICAL SUPPORT

NSW Health provides technical support for NSW Health smart devices via the State-Wide Service Desk (SWSD).

NSW Health does not provide technical support, advice, or consulting services for personal devices, except to enable users to access corporate and clinical applications on NSW Health ICT systems for business purposes.

4. TRANSFERRING A PERSONAL MOBILE NUMBER TO A NSW HEALTH ACCOUNT

Staff can choose to transfer their personal number to a NSW Health account subject to contract arrangements with the vendor. However, when staff leave NSW Health, they must submit a request form in SARA or to their local NSW Health organisation ICT team to transfer back their number before leaving the organisation. If a request form is not submitted, then the number remains with NSW Health.

5. MOBILE DEVICE MANAGEMENT AND THE NSW HEALTH MOBILITY PLATFORM

All NSW Health smart devices used to access sensitive and security classified information owned by NSW Health must be enrolled in a NSW Health Mobile Device Management platform, such as the NSW Health Mobility Platform.

Staff can choose to enrol personal devices in a NSW Health Mobile Device Management platform and the NSW Health Mobility Platform. NSW staff may not be able to access all clinical and corporate applications and NSW Health organisation specific sites if their personal device is not enrolled.

The NSW Health Mobility Platform facilitates governance and compliance through configuration settings and policy enforcement for mobile devices by:

- Providing secure access to NSW Health resources such as clinical systems and corporate information and organisation-specific Intranet sites.
- Enabling and assisting staff when bringing personal mobile devices to access sensitive and security classified information stored on NSW Health systems.
- Managing and controlling application installation on mobile devices. The Mobility Platform restricts installation of applications that can pose a risk to data security or productivity. In addition, the Platform publishes recommended apps for NSW Health organisations via a customisable 'Health Store'.
- Monitoring for security vulnerabilities and compliance checking mobile devices to ensure software and enrolled devices are up-to-date, minimising exposure to security threats.
- Providing automated and centralised configuration and management of mobile devices at the time of enrolment (fast device set-up).
- Assisting users experiencing issues with enrolled devices by allowing support staff to remotely inspect the device's configuration and help troubleshoot.
- Enhancing mobility for an increasingly agile workforce enabling collaboration while 'roaming' across NSW Health organisations or working remotely.
- Improving asset control and device lifecycle management for NSW Health mobile devices.

The NSW Health Mobility Platform does not store or collect any tracking information for any personal enrolled devices. It only tracks information on corporate and clinical applications stored on the device, not personal use applications.

The NSW Health Mobility Platform also can remotely delete corporate and clinical applications holding sensitive NSW Health information but will not remove any personal information and applications held on the personal device. A factory reset or complete device wipe will only be performed in consultation with the device owner.

6. SECURITY REQUIREMENTS

The following table outlines security requirements for NSW Health smart devices and personal devices.

All NSW Health smart devices and personal devices must have their operating system patched with the latest appropriate software and security updates per their vendor. This is in line with recommendations from the Australian Cyber Security Centre, their website has additional regularly updated resources.

NSW Health staff must also complete Cyber S.A.F.E (Security Awareness for Everyone) Training, available via My Health Learning. Completing the training will ensure that staff are aware of their responsibilities regarding information security and protect them and NSW Health information from malicious attacks.

Security Feature	Security Requirement	Device Requirements
Passcodes and complexity	A password or passcode must be enabled on devices to unlock the device when not in use. Biometric features such as fingerprint scanners can be used and enabled by default, but a backup password or passcode is still required to leverage any biometric features. Simple passwords must be disabled across the NSW Health systems and networks. Users will be prompted to create stronger passwords to protect against the risks of disclosing sensitive and confidential NSW Health information. NSW Health organisations must have guidelines to advise staff on creating strong passwords.	NSW Health smart devices and personal devices must meet length and complexity requirements.
Appropriate anti-malware protection	All computers should have approved anti-malware software installed where appropriate. This software should be active, be scheduled to perform checks at regular intervals. A device suspected of having malware installed must not be used to access NSW Health information.	NSW Health smart devices and personal devices must meet this requirement.
Auto-lock	Devices must have the auto-lock feature enabled and set to auto-lock. The auto-lock feature protects the information on the device by automatically locking the device after the specified time.	NSW Health and personal computers must auto-lock after ten minutes. NSW Health and personal mobile devices must auto-lock after three minutes, including smartphones and tablets.
Password attempt lockout	Account lockout means locking out any account after a defined number of unsuccessful login attempts. At a minimum, the device should be enabled so that after six invalid password attempts, the device will remain locked out for a minimum of 15 minutes.	NSW Health smart devices and personal devices must meet this requirement.

Security Feature	Security Requirement	Device Requirements
Trusted Applications (Apps)	Devices must only install apps from a trusted source, including the NSW Health Store, Google Play with play protect, and Apple Store, to ensure that the developer has validated and properly signed. Devices must not install apps from unknown sources, and where possible, installing apps from unknown sources must be disabled.	NSW Health smart devices and personal devices must meet this requirement.
Remote Wipe	Devices must have the remote wipe function enabled. The remote wipe function allows the device to be wiped of data if lost, stolen or misplaced. This data includes any personal information stored on the device. Further information on remote wipe and device disposal is in section 7.	NSW Health smart devices must meet this requirement. This must be enabled on personal devices that have NSW Health information stored on the device.
Protected backups	Device data backups must be kept secure to ensure that information backed up is not easily accessible. Regularly backing up your device means your information can be recovered if your device is ever lost, stolen or damaged. The Australian Cyber Security Centre website has resources to enable this on devices.	NSW Health smart devices must meet this requirement.
Minimum device operating system level	The NSW Health organisations' ICT Team will define the device's minimum operating system level during the approval process to bring a Personal Device or through the NSW Health Mobility Platform. Any device that does not meet this requirement will not be able to access sensitive and security classified information on NSW Health ICT systems.	NSW Health smart devices and personal devices must meet this requirement.
Information visible on locked screens	When devices are locked, minimal information must be shown on the display screen. This includes (but is not limited to) disabling mail and message previews and notification messages.	NSW Health smart devices and personal devices must meet this requirement.
Physical security of a device	The loss or theft of any device containing information or data owned by NSW Health organisations must be reported immediately to SWSD, through SARA or the local organisation ICT department. A report must be made for NSW Health smart devices and personal devices.	NSW Health smart devices and personal devices must meet this requirement.
Network security of a device	Users must ensure all Bluetooth communications use a unique passcode. Users must not connect to unsecured Wi-Fi access points. Networks in coffee shops and public places are frequently unsecured and are frequent targets of hackers.	NSW Health smart devices and personal devices must meet this requirement.

6.1. Operating System Modifications

The device operating system must not be modified. Any device suspected to have had unauthorised changes to its operating system must not be used to access NSW Health systems. In addition, devices must not be "jailbroken", which is the process of removing the limitations imposed on devices through the use of hardware or software exploits.

Jail breaking allows users to gain root access to the operating system, allowing them to download additional applications, extensions, and themes that are unavailable through the official application stores.

7. LOST AND STOLEN DEVICES AND DISPOSAL OF DEVICES

NSW Health staff must report device loss or theft to the SWSD or local organisation ICT department or lodge a ticket in SARA. Staff must also notify the SWSD, ICT department or lodge a ticket in SARA if they believe their device has had its security compromised.

The remote wipe feature of the NSW Health Mobility Platform is used to delete NSW Health data from the device.

A factory reset or complete device wipe will be performed on devices in consultation with the device owner and only performed if necessary if the device has been lost, stolen or had its security compromised. This data includes any personal information stored on the device. NSW Health organisations take no responsibility for any personal or non-NSW Health information data that is stored on these devices that may be lost or deleted. NSW Health staff are encouraged to regularly backup their personal data held on the device.

In cases where NSW Health smart devices are faulty, and data cannot be removed from the device via its feature set or remotely wiped by the NSW Health Mobility Platform, the device will be physically destroyed to ensure all NSW Health information and data are disposed of completely.

NSW Health smart devices that are no longer needed must be returned to the NSW Health organisation for disposal or to be re-assigned in the asset register. NSW Health smart devices must be reset and wiped before being re-assigned in the asset register.

It is the responsibility of each NSW Health organisation to ensure managed devices are disposed of correctly. This also includes the remote wipe of all corporate and personal information from the device.

If a device is destroyed, the approved destruction of the hardware is to be updated in the asset register. In addition, where third-party vendors have been engaged to perform the destruction, a certificate of destruction must be obtained from the vendor and filed appropriately within the organisation.

If the owner intends to change or dispose of their personal device that is enrolled in a NSW Health mobile device management platform or has NSW Health corporate or clinical applications installed, it is their responsibility to notify the SWSD and their manager of the change immediately. The device owner must verify with NSW Health via the state-wide service desk, SARA or with their NSW Health organisation ICT team that they have removed all NSW Health data from the device as required.

8. RELATED DOCUMENTS

8.1. NSW Health policy directives, guidelines, and frameworks

NSW HEALTH POLICY DOCUMENTS	
(PD2020_046)	NSW Health Electronic Information Security Policy
(PD2015_036)	NSW Health Privacy Management Plan
(Manual)	Privacy Manual for Health Information
(PD2009_076)	NSW Health Communications – Use & Management of Misuse of NSW Health Communication Systems
(PD2015_049)	NSW Health Code of Conduct
(PD2019_028)	NSW Health Goods and Services Procurement Policy
(PD2015_043)	NSW Health Risk Management – Enterprise-Wide Risk Management Policy and Framework
(PD2020_036)	Remote Access Policy
(GL2005_045)	Mobile Phones and Wireless Communication Devices - Interference with Medical Equipment - Use of
(PD2015_036)	NSW Health Privacy Management Plan
(PD2009_057)	NSW Health Records Management
(PD2018_031)	NSW Health Managing Misconduct
(GL2019_002)	NSW Health Data Governance Framework
(HD21/9532)	NSW Health Information Security Management Standards

8.2. NSW Government policies and directives

NSW GOVERNMENT POLICIES AND DIRECTIVES	
(Policy)	NSW Government Cyber Security Policy
(Guideline)	NSW Government: Information Classification, Labelling and Handling Guidelines
(Framework)	NSW Government Intellectual Property Framework 2020

8.3. Whole of Government Guidelines

Risk Management of Enterprise Mobility including Bring Your Own Device	Australian Cyber Security Centre – Risk Management of Enterprise Mobility including Bring Your Own Device

8.4. Standards

ISO/IEC 27001	Information Security Management – ISO/IEC 27001