Remote Access

Summary The NSW Health Remote Access Policy Directive defines the principles for authorised and secured connection to the NSW Health network from a remote location.

Document type Policy Directive

Document number PD2020_036

Publication date 13 October 2020

Author branch eHealth & ICT Strategy Branch

Branch contact (02) 8644 2213

Review date 13 October 2023

Policy manual Not applicable

File number H20/70765

Status Active

Functional group Clinical/Patient Services - Information and Data
Corporate Administration - Information and Data, Security
Personnel/Workforce - Security, Workforce planning

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

Distributed to Ministry of Health, Public Health System, Government Medical Officers, NSW Ambulance Service

Audience All Staff of NSW Health

Secretary, NSW Health

This Policy Directive may be varied, withdrawn or replaced at any time. Compliance with this directive is mandatory for NSW Health and is a condition of subsidy for public health organisations.

REMOTE ACCESS

POLICY STATEMENT

This Policy Directive defines the principles for the authorised and secured connection to the NSW Health network from a remote location that minimises the potential exposure to NSW Health from damages, destruction, misuse and theft.

NSW Health Organisations are committed to provide flexible working arrangements that allows users to remotely connect to NSW Health systems from locations not within the physical control of NSW Health. This remote access allows authorised users to perform work processes efficiently and effectively.

Authorised users of NSW Health Organisations remote access solutions are employees, contractors, service providers, third parties and other persons who have successfully completed the Remote Access application process.

SUMMARY OF POLICY REQUIREMENTS

Remote access to NSW Health networks must only be through authorised solutions and systems.

The remote access solution must be configured so that it only facilitates access to information systems and assets within NSW Health for which the user is authorised to access.

Remote access users must only remain connected for as long as they are conducting business related work for NSW Health and must disconnect as soon as that work is completed.

All users remotely accessing NSW Health must take all reasonable steps in ensuring that the organisations' assets, and non-organisation computer systems used for this purpose, are free from malicious software and are not available for unauthorised use.

When using the authorised remote access solution, all policies related to connection to the NSW Health network must be followed. This includes the *NSW Health Policy Directive Communications - Use & Management of Misuse of NSW Health Communications Systems (PD2009_076).*

REVISION HISTORY

Version	Approved by	Amendment notes
October-2020 (PD2020_036)	Secretary, NSW Health	Initial Document

ATTACHMENTS

1. Remote Access: Procedures.

CONTENTS

1 BACKGROUND

Remote Access is required when a user is physically distanced from the office and needs to access the information systems and assets within NSW Health's secure networks. Remote Access presents a greater risk to NSW Health as the electronic device used is working in an unprotected environment with unprotected network facilities.

In addition, protection of Remote Access connections is especially critical since communications can be transmitted using media that cannot be assumed to be secured. Therefore, Remote Access requires additional protections and precautions to be applied to ensure the security and safeguarding of the organisations' assets, information and resources.

Confidentiality, integrity and availability are the security objectives that must be applied to Remote Access when connecting to NSW Health information systems and assets. These objectives will uphold on access to and disclosure of information, ensure data is protected against unauthorised alteration or destruction and authorised users are provided with timely and reliable access to information systems and assets.

It is also a legislative requirement to maintain the privacy of records containing personal information and personal health information about employees and members of the public and prevent unlawful access, use and disclosure of such information.

1.1 About this document

This document establishes the provision of appropriate levels of security for the authorised and secured connection to the NSW Health network from a remote location.

1.2 Key definitions

Availability

Ensuring timely and reliable access to and use of information.

Confidentiality

Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Dual homing

Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being on one of the organisations provided Remote Access networks and connecting to another network.

Electronic device

Workstation, laptop, tablet, smartphone and any other computing device which is capable of remote access to the NSW Health network.

Information systems and assets

Refer to any information or communication infrastructure used by NSW Health Organisations and all personnel that work with it. This includes computer hardware and software, to create, process, hold, maintain or transmit electronic information.

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Personal health information

Personal Information which concerns a person/client's health, medical history or past or future medical treatment. It also includes other Personal Information collected in the course of providing a health service or information collected in relation to donation of human tissue.

Personal Information

Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion.

Remote Access

Authorised access to a system from outside of a security domain and/or access to a system from a location not within the physical control of the system owner.

Third Party Organisations

Third Party Organisations are used to collectively refer to Affiliates and other organisations who, while not specifically named in the Act, participate in the use of NSW Health ICT systems. Third Party Organisations includes but is not limited to:

- Affiliated health organisations under Schedule 3 of the Health Services Act
- Any other organisations contracted by NSW Health or its entities to deliver clinical services, which require the organisation to routinely access NSW Health applications such as:
    - Private Hospitals contracted by NSW Health to provide public health services,
    - Private pathology and radiology services,
    - University and education providers,
    - Royal Flying Doctor Service and Careflight, etc.
    - Third Party Vendors.

Third Party Organisations do not include private GP practices, patients or carers.

Third Party Users

Third Party Users are the staff engaged by Third Party Organisations and have access into NSW Health Systems and/or software.

Split-tunnelling

Simultaneous direct access to an external network (such as the Internet) while connected into the NSW Health's corporate networks via a VPN tunnel.

Two-factor authentication

System wherein two different factors are used in conjunction to authenticate. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance. Two-factor authentication typically is a signing-on process where a person proves his or her identity with two of the three following methods: "something you know" (e.g. password or PIN), "something you have" (e.g. smartcard or token), and "something you are" (e.g., fingerprint or iris scan).

1.3 Legal and legislative framework

NSW Health Organisations and people who work within the NSW public health system must comply with the legislative obligations contained in the:

- Health Records and Information Privacy Act 2002 (NSW);
- Privacy and Personal Information Protection Act 1998 (NSW); and
- State Records Act 1998 (NSW)

Additionally, staff must comply with privacy and confidentiality obligations contained in the NSW Health Code of Conduct.

2 IMPLEMENTATION OF REMOTE ACCESS

2.1 Remote Access solution

Remote Access to NSW Health networks must only be through authorised solutions and systems. The authorised Remote Access solution must allow access to the NSW Health network in a controlled and administered service to all authorised users.

The Remote Access solution must be configured so that it only facilitates access to information systems and assets within NSW Health for which the user is authorised to access.

No individual, division, group or third party shall provide or setup any device or service that allows remote access to NSW Health's network or to information systems or assets on the NSW Health network without documented approval for an exception.

2.2 Authorisation

Authorisation for remote access must be obtained through the approved Remote Access Request Form in place locally. This will ensure that access is provided according to business needs and the role of the user.

Users changing job roles within NSW Health Organisations must have their Remote Access reviewed. If Remote Access is no longer required, then it must be revoked immediately.

Remote Access from overseas must be considered on a case-by-case basis, approved prior to travel and with a defined time limit. This access may also be immediately revoked if any security alerts are raised.

2.3 Authentication and access control

NSW Health organisations must be able to positively identify who is connecting remotely, and verify what access levels are required. This is achieved by user authentication and identification.

All NSW Health Organisations must use a minimum of two-factor authentication when connecting using remote access. Using only a username and password is not an acceptable means of authentication for Remote Access. Two-factor authentication requires users to validate their credentials using two separate methods; in essence this represents something you know (username/password) and something you have (token passcode).

Inactive sessions should be shut down after a defined period of inactivity of 1 hour. This will ensure that devices are not left exposed whilst connected to the NSW Health information systems and assets.

NSW Health Organisations reserve the right to revoke Remote Access in the case where a designated connection is causing any threat to the organisations' information systems and assets.

2.4 Audit log

Any device using Remote Access to connect to NSW Health information systems and assets is subject to monitoring, which may include but is not limited to date, time, duration of access, identification of endpoint and all traffic which traverses the NSW Health network.

2.5 Remote access for third parties

Remote Access by Third Party users needs to be considered separately from remote access by employees and contractors hired by NSW Health Organisations. It must be possible to clearly differentiate Third Party users from NSW Health employees and contractors.

Third Party organisations must agree to NSW Health's terms and conditions for access to information systems and assets prior to the access being granted. The terms and conditions shall be clearly documented within the Third Party Agreement, Service Partnership Agreements and/or Service Level Agreements (SLA).

In providing Remote Access to Third Parties, consideration must be given to:

- Limiting access to specific time windows only and to explicit resources only;
- Removing access immediately after access is no longer required;
- Reviewing the Third Party access accounts in a timely manner; and

- Automatic expiration rights on a set date and time or after a specified number of sessions has been reached or exceeded.

2.6 Protection from malicious activity

All NSW Health owned and personally owned devices used for Remote Access to NSW Health information systems and assets must use the most up-to-date end point protection software and appropriate operating system security patches. Users of personal devices are encouraged to ensure operating systems and end-point-protection software are configured for automatic refresh and updates. Users of NSW Health owned devices must contact the State-Wide Service Desk or lodge a ticket on SARA if software is out of date.

3 REMOTE ACCESS USER RESPONSIBILITIES

Remote Access users must ensure that the security of their Remote Access connection is given the same consideration as their on-site connection to the NSW Health network.

At no time is a remote user to connect NSW Health's network to any other network. This includes, but is not limited to split-tunnelling, dual homing, or otherwise rerouting NSW Health traffic beyond the intended endpoint.

Remote Access users are not permitted to download or otherwise store NSW Health data which is considered sensitive, contains personal information or personal health information on their personally owned electronic devices. This includes the transfer of such data to a personal cloud service, or printing outside the office. If any NSW Health owned device used for Remote Access is lost, stolen, or otherwise removed from the user's control, the user will be responsible for notifying the State Wide Service Desk immediately.

Remote Access users agree to immediately notify the State Wide Service Desk of any incident or suspected incidents of unauthorised access and/or disclosure of NSW Health resources or information.
Personal devices must not be used for Remote Access when the appropriate security measures cannot be applied.

4 EXCEPTIONS

Any exceptions to this Policy Directive must be appropriately documented and approved. Exemptions will only be granted on the basis of a strong business and/or technical need and must include:

- a detailed and balanced assessment of the exception
- a timeframe associated with the proposed exception
- detailed risks assessment associated with the proposed exception
- costs associated with the proposed exception, and
- evidence of awareness and approval from senior executives

5 REFERENCES

5.1 NSW Health policy directives

NSW HEALTH POLICY DIRECTIVES	
PD2013_033	NSW Health Electronic Information Security Policy
PD2015_036	NSW Health Privacy Management Plan
PD2009_076	NSW Health Communications – Use & Management of Misuse of NSW Health Communication Systems
PD2015_049	NSW Health Code of Conduct
PD2015_043	NSW Health Risk Management – Enterprise-Wide Risk Management Policy and Framework

5.2 NSW government policies and directives

NSW GOVERNMENT POLICIES AND DIRECTIVES	
https://www.digital.nsw.gov.au/policy/cyber-security-policy	NSW Government Cyber Security Policy
https://www.digital.nsw.gov.au/policy/managing-data-information/information-classification-handling-and-labeling-guidelines	NSW Government: Information Classification, Labelling and Handling Guidelines