NSW Health My Health Record Security and Access

Summary This Policy Directive outlines the obligations and responsibilities of all individuals and organisations who use the NSW Health HealtheNet Clinical Portal (HealtheNet) to access the national My Health Record System. The Policy is intended to ensure that all NSW Health employees and contractors comply with all legislation and policies that govern the use of HealtheNet and My Health Record.

Document type Policy Directive

Document number PD2019_054

Publication date 07 November 2019

Author branch eHealth & ICT Strategy Branch

Branch contact (02) 8644 2213

Review date 07 November 2024

Policy manual Not applicable

File number

Status Active

Functional group Clinical/Patient Services - Governance and Service Delivery, Information and Data
Corporate Administration - Governance, Information and Data, Records, Security

Applies to Ministry of Health, Local Health Districts, Specialty Network Governed Statutory Health Corporations

Distributed to Ministry of Health, Public Health System

Audience All Staff of NSW Health

Secretary, NSW Health

POLICY STATEMENT

NSW HEALTH MY HEALTH RECORD SECURITY AND ACCESS

PURPOSE

This Policy Directive outlines the obligations and responsibilities of all individuals and organisations who use the NSW Health HealtheNet Clinical Portal (HealtheNet) to access the national My Health Record system.

This Policy is to ensure that all NSW Health employees and contractors comply with all legislation and policies that govern the use of HealtheNet and My Health Record.

The national My Health Record system is designed to provide a secure online summary of an individual's health information. The HealtheNet portal enables NSW Health to upload a copy of clinical information which sits within NSW Health ICT systems into the My Health Record system and facilitates NSW Health personnel access into the My Health Record system.

There are mechanisms in place to allow patients to control which information is uploaded and stored in the My Health Record system.

MANDATORY REQUIREMENTS

All NSW Public Health Organisations must ensure that their local processes comply with and support this Policy in relation to the following:

- Adherence to all policy and legislative requirements relating to information security, privacy, and access controls.
- Access to the My Health Record System must only occur through the NSW Health HealtheNet Clinical Portal.
- Maintain records of the individuals who have access to and/or received training to access the My Health Record system.
- If a patient requests that the documents relating to the particular episode of care not be uploaded to the My Health Record, these documents must not be uploaded.

IMPLEMENTATION

This Policy covers the requirements relating to accessing the My Health Record system on behalf of NSW Health and applies to all employees, contractors and other persons connected to NSW Health.

Compliance with this Policy and all relevant acts and regulations as they relate to the My Health Record system is mandatory for all NSW Health personnel who come into contact with clinical information which could potentially be uploaded to the My Health Record system.

All personnel and organisations should be aware of their legislative obligations and that the breach of those obligations may result in prosecution and the imposition of a penalty or disciplinary actions.

REVISION HISTORY

Version	Approved by	Amendment notes
November-2019 (PD2019_054)	Secretary, NSW Health	New Policy Directive

ATTACHMENTS

1. My Health Record Security and Access: Procedures.

NSW Health My Health Record Security and Access

PROCEDURES

Issue date: November-2019

PD2019_054

CONTENTS

1 BACKGROUND

1.1 Summary

My Health Record is a secure online summary of a patient's health information operated by the Australian Commonwealth Government. Information included in My Health Record is controlled by the patient, and the patient determines which healthcare organisations are able to access it.

My Health Record enables health information – summaries of medical conditions and treatments, allergies, medicines details, pathology test or medical imaging reports – to be shared across health care providers including General Practitioners (GPs), hospital staff and available to the patient.

The *My Health Records Act 2012,* together with the NSW and the Commonwealth Privacy legislation provide the legislative framework for the My Health Record system and NSW Health systems.

1.2 Purpose

NSW Health is committed to ensuring the security and integrity of the My Health Record system, and the personal and health information that it holds. This Policy Directive outlines NSW Health's obligation and responsibilities in participating in the My Health Record system.

My Health Record system provides an opportunity for NSW Health to share information about patient encounters in the NSW public health system with the patient, their carers, and any other healthcare providers who are authorised to access the patient's My Health Record. Any NSW Health data that is uploaded into the My Health Record system will be a copy of health information that currently sits within NSW Health systems.

1.3 Scope

This Policy Directive applies to all staff (employees and contractors) of NSW Health and any healthcare provider that NSW Health supplies services to under contract, who access, and use, the HealtheNet Clinical Portal to gain access to a patient's My Health Record.

1.4 Mandatory requirements

The *NSW Health My Health Record Security and Access Policy* is a mandatory Policy Directive across all NSW Health Organisations. All NSW Health Organisations must enforce the requirements of this Policy within their organisation as this applies to all employees, person or contractor who is authorised to access and use the My Health Record system.

2 NSW HEALTH STAFF RESPONSIBILITIES AND OBLIGATIONS

All access to My Health Record needs to be lawfully authorised and conducted in the normal course of employment.

2.1 Legislative obligations

NSW Health staff are bound by legislative privacy obligations and are subject to sanctions applicable under the *Health Records and Information Privacy Act 2002* (HRIP Act) and the *My Health Records Act 2012*. Any access to the My Health Record may also be subject to sanctions under the *Privacy Act 1988* (Cth).

NSW Health staff access to the HealtheNet Clinical Portal and the My Health Record system is aligned to the following polices and legislation:

- *Health Records and Information Privacy Act 2002* (HRIP Act)
- *My Health Records Act 2012*
- *My Health Records Amendment (Strengthening Privacy) Act 2018*
- NSW Health Privacy Manual for Health Information
- NSW Health Code of Conduct
- The NSW Health Electronic Information Security Policy
- Communications - Use & Management of Misuse of NSW Health Communications Systems

It is essential that staff be made aware of their individual rights and responsibilities in respect of safeguarding information privacy.

NSW Health staff must also be aware that where an intentional breach occurs they may also be subject to provisions under the My Health Records Act, Independent Commission Against Corruption (ICAC) Act 1988 and the Crimes Act 1900.

Staff must sign an undertaking to ensure that they are aware of their obligations and responsibilities in using electronic Medical Records (eMRs), which includes the My Health Record system, before they access the system.

2.2 NSW Health staff access to the My Health Record system

NSW Health staff must only access My Health Record system for the purpose of providing healthcare or other limited purposes set out in the My Health Records Act.

Within NSW Health, staff can only access the My Health Record system through the HealtheNet Clinical Portal. The HealtheNet Clinical Portal is accessed through a link within a patient's record in a NSW Health eMR. All employees of NSW Health, including temporary and casual staff, whose role requires them to access the My Health Record system will be provided with a unique eMR user account, with an individual login name.

All NSW Health staff are required to sign an undertaking as part of their eMR Network Access terms and conditions in order to access My Health Record and other NSW Health systems. All NSW Health staff have agreed that they will be accountable for all actions performed using their user ID and that any records that have been accessed from a patient's My Health Record can be audited.

User accounts should only be accessed by the individual the account is assigned to and will not be used by multiple staff members. All users must ensure that they log out of the system when they are not using their account to prevent unauthorised access.

The HealtheNet Clinical Portal will automatically log a user out of an active open session:

- Where a user has opened another window and has not returned to the HealtheNet Clinical Portal window for 2 minutes
- Where a user has the HealtheNet Clinical Portal window open as the main window on their desktop, but has not actively used the Portal for 2 minutes

NSW Health staff are not permitted to access the My Health Record system through the national Provider Portal as NSW Health is obliged to maintain a record of all its healthcare providers' interactions with the My Health Record System.

Some specialists, in their capacity as a private health provider, may want to register to participate in the My Health Record system and access within their own private rooms/organisations. This access should be separate to NSW Health.

2.3 Reporting security and privacy breaches

A security breach is when any unauthorised person accesses the My Health Record system, for example a staff member with access to the My Health Record system discovers that someone else has gained access to their eMR user account/login and has inappropriately accessed a person's My Health Record using their credentials.

If any staff member becomes aware of an actual, or potential, security breach in the My Health Record system, it is their responsibility to follow their local reporting procedure to ensure the breach is notified to their manager or respective senior management.

Guidance on privacy breaches can be found in the Privacy Manual for Health Information, and all related concerns and incidents on information security can be found in *PD2013_033: Electronic Information Security Policy – NSW Health*

Staff are to also be reminded that their approval to access and use of eMR does not extend to accessing their own or their families' health information. Such access is potentially a privacy breach unless it specifically relates to their employment or role.

Staff wanting to access their own My Health Record should do so through the MyGov portal and not through the HealtheNet Clinical Portal.

2.4 Emergency Access

Section 64 of the *My Health Records Act 2012* allows a healthcare provider to override advanced access controls where they believe access to the information is necessary to lessen or prevent a serious threat to an individual's life, health or safety and it is unreasonable or impracticable to obtain the patient's consent (for example, if the patient is unconscious); or to lessen /prevent a serious threat to public health or public safety.

Staff who use Emergency Access must be able to justify the circumstances during any audit by the System Operator and all access will be documented in the patient's My Health Record. NSW Health staff must be aware that any access to the My Health Record system is to be lawfully authorised as it is an offence to collect, use or disclose information in the My Health Record system that is not authorised by the My Health Record Act. Significant penalties apply, including fines and imprisonment.

2.5 Uploading clinical information to a My Health Record

Healthcare providers are authorised by the My Health Records Act to upload clinical documents to the My Health Record without relying on the patient providing consent on each and every occasion subject to any express advice given by the patient that their records should not be uploaded.

NSW Health has built an 'exclusion flag' in the Patient Administration System (PAS) to capture the patient's withdrawal of consent for clinical information to go to their My Health Record for that single encounter. The field is set by default to share patient information with the My Health Record system.

2.6 Patient requests to access their My Health Record information

NSW Health does not need to show a patient the contents of their My Health Record component in the HealtheNet Clinical Portal as the patient can view the information themselves online.

Patients should be directed to view their My Health Record through the online consumer portal (www.my.gov.au), or to contact the My Health Record System Operator on: 1800 723 471.

2.7 Training

Staff must receive training on an ongoing basis to understand their privacy obligations, and how to access and use of the NSW Health's systems and My Health Record system.

Admissions teams and any other relevant staff must be trained in the use of the My Health Record 'exclusion flag' to exclude a patient's information going to their My Health Record, if asked to do so.

3 NSW HEALTH ORGANISATIONS' RESPONSIBILITIES AND OBLIGATIONS

All NSW Health Organisations must enforce all legislative and policy obligations within their organisation.

3.1 My Health Record system roles

The following eHealth NSW roles and responsibilities for implementation and compliance monitoring of the My Health Record Policy in NSW Health are:

- Responsible Officer (RO): Oversees NSW Health's legal compliance with participation requirements in the My Health Record system.
- Organisational Maintenance Officer (OMO): Responsible for implementation and compliance monitoring of the My Health Record Policy, and for the maintenance of the policy within NSW Health.

3.2 NSW Health staff access to the My Health Record system

The healthcare provider organisation must maintain records linking user accounts to individual staff for auditing purposes.

All NSW Health organisations must comply with the NSW Health Electronic Information Security Policy (PD2013_033) which states the following:

- A unique user identifier is assigned to all users
- Passwords used for authentication must be kept secret and should align with appropriate policies and standards for the NSW Health Organisation
- User ID's should be unique to each user to ensure audit and control over permissions
- Users are accountable for actions performed using their user ID's.

NSW Health organisations must ensure that they immediately suspend or deactivate individual user accounts in cases where a user:

- leaves the organisation
- has the security of their account compromised
- has a change of duties so that they no longer require access to the HealtheNet Clinical Portal and My Health Record system.

3.3 Uploading clinical information to a My Health Record

In uploading clinical documents to the My Health Record system, NSW Health organisations will:

- maintain a local copy of every document uploaded to the My Health Record
- not infringe intellectual property or moral rights
- not upload documents that contain defamatory material
- only upload content for registered consumers
- only upload documents approved by an authorised clinician, and
- take appropriate measures to ensure data quality and accurate identification of the consumer.

3.4 Local changes to clinical documents and notifying HealtheNet

If any Discharge Summaries, Pathology Results, Diagnostic Imaging Reports or Dispense Records have been submitted to HealtheNet under the incorrect encounter they will not automatically be moved or merged in HealtheNet and My Health Record.

Where clinical documents have been submitted to HealtheNet, and an encounter combine/move is required, the Local Health Districts must mitigate any impact to downstream systems. Any changes to local systems made by the LHD must be notified to the impacted teams, including the HealtheNet Application Support team.

3.5 Identification of staff members with authorised access to the My Health Record

NSW Health organisations must maintain a record of healthcare providers authorised to access the My Health Record system within eMR and in the organisation's internal records. These records must be maintained to allow audits to be conducted by the System Operator.

eMR will be used to assign and record a unique internal staff member identification code. This unique identification code will be automatically recorded in the HealtheNet system against any My Health Record system access.

3.6 Staff training and obligations

NSW Health is bound by legislative privacy obligations and is subject to sanctions applicable under the *Health Records and Information Privacy Act 2002* (HRIP Act) and the *My Health Records Act 2012*. It is an offence to collect, use or disclose information in the My Health Record system that is not authorised by the My Health Record Act. Significant penalties apply, including fines and imprisonment.

NSW Health must ensure that staff are appropriately trained on how to use the My Health Record, that they are aware of their legal obligations and the consequences of any breach. Healthcare provider organisations must maintain a register of staff training as it relates to accessing and using NSW Health eMRs, including use of the My Health Record system.

4 DEFINITIONS

My Health Record	Formerly known as the Personally Controlled Electronic Health Record.
System Operator	The Australian Digital Health Agency

5 RELATED DOCUMENTS

- NSW Health Privacy Manual for Health Information
- My Health Records Act 2012
- PD2013_033: Electronic Information Security Policy – NSW Health
- PD2012_069: Health Care Records – Documentation and Management
- Health Records and Information Privacy Act 2002 (HRIP Act)
- NSW Health Privacy Leaflet for Patients
- NSW Health Privacy Leaflet for Staff
- Health Records and Information Privacy Regulation 2012
- NSW Health Code of Conduct
- Communication - Use & Management of Misuse of NSW Health Communication Systems
- MHR Incident Management Framework

Appendix A: Implementation checklist

LHD/Facility:			
Assessed by:		**Date of Assessment:**	
IMPLEMENTATION REQUIREMENTS	**Not commenced**	**Partial compliance**	**Full compliance**
1. Local policies relating to the management of staff access to the eMR including My Health Record	❑	❑	❑
	Notes:		
2. Register of eMR and My Health Record training activities	❑	❑	❑
	Notes:		
3. PD2013 033 – Electronic Information Security Policy – NSW Health	❑	❑	❑
	Notes:		
4. PD2012 069: Health Care Records – Documentation and Management	❑	❑	❑
	Notes:		
5. Communication – Use & Management of Misuse of NSW Health Communication Systems	❑	❑	❑
	Notes:		
	❑	❑	❑
	Notes:		