Health
Justice Health &
Forensic Mental Health Network

Justice Health & Forensic Mental Health Network
PO BOX 150 Matraville NSW 2036
Tel (02) 9700 3000
http://www.justicehealth.nsw.gov.au

Clinical Applications Access and Security

Policy Number 2.125

Policy Function Leadership and Management

Issue Date 27 July 2018 (*minor change on section 3.2 Acess on 7 February 2020*)

Summary The information contained within the Justice Health & Forensic Mental Health Network (JH&FMHN) Clinical Applications is considered an integral part of the patient's Health Record and is used for the provision of direct care, research, quality improvement, education, analysis of data, health service evaluation, planning, workplace health/safety and legal purposes.

This policy provides a standardised approach explicitly to accessing the patient's electronic health records, with access granted only after it has been appropriately authorised, users have been adequately trained and are aware of their responsibilities relating to access, privacy and security.

Responsible Officer Executive Director Corporate Services

Applicable Sites

☒ Administration Centres (Inc. Joint Records Centre)
☒ Community Sites (e.g. Court Liaison Service, Community Integration Team, etc.)
☒ Health Centres (Adult Correctional Centres or Police Cells)
☒ Health Centres (Juvenile Justice Centres)
☒ Long Bay Hospital
☒ Forensic Hospital

Previous Issue(s) Policy 2.125 (May 2010)

Change Summary

- Addressed any requirements following updates to JH&FMHN policies, forms, NSW Ministry of Health Policy and NSW Legislation. In addition a few minor procedural changes occurred. Addition of CHIME. Updated hyperlinks.

TRIM Reference POLJH/2125

Authorised by Chief Executive, Justice Health & Forensic Mental Health Network

1. Preface

The policy applies to all Justice Health & Forensic Mental Health Network (JH&FMHN) staff, including agency staff, contractors, vendors and other persons who have access to electronic personal health information of the patient's Health Record stored in JH&FMHN Clinical Application Systems, iPM Patient Administration System (PAS), the Justice Health electronic Health System (JHeHS) and Community Health Information Management Enterprise (CHIME). This includes those users who are authorised to access the system remotely.

2. Policy Content

2.1 Mandatory Requirements

Compliance is mandatory under NSW Ministry of Health (MoH) PD2013_033 *Electronic Information Security – NSW Health*, the *Health Records and Information Privacy Act 2002* (HRIPA), the *Privacy and Personal Information Protection Act 1998* (PPIPA) and JH&FMHN policy 2.156 *Information Security Management System (ISMS)* for management, personnel and all persons handling electronic health information, whether directly or indirectly, involved in patient care.

The NSW public health sector, as with all public sector agencies in NSW, is required to comply with the HRIPA and PPIPA. Both specify a series of rules designed to protect the privacy of personal information, including personal health information, in NSW.

As per PD2013_033, *NSW Government Digital Information Security Policy* and *NSW Health Privacy Manual for Health Information* all personnel and organisations must be aware of their legislative confidentiality obligations and that the breach of those obligations may result in prosecution and the imposition of a penalty.

2.2 Implementation – Roles & Responsibilities

All JH&FMHN Clinical Application System users must ensure they follow required procedures relating to Clinical Applications access and security and ensure they understand their responsibilities under policy and legislation.

Manager is responsible for:

- Identifying and approving access for direct reports to the relevant Clinical Application System/s.
- Ensuring direct reports attend mandatory Clinical Application Systems training and are compliant with all processes.
- Advising Information Communications Technology (ICT) the level of access to be granted to a user.

User is responsible for:

- The information recorded within the Clinical Application Systems.
- Attending Clinical Application Systems training and being compliant with all access and security processes.

Information and Communications Technology (ICT) is responsible for:

- Ensuring correct configuration of systems such as servers, networks, firewalls and routers to allow users secure, efficient and effective access as required to Clinical Applications.

- Ensuring that access to the appropriate Clinical Application is granted only after the user has received appropriate training;
- Determining the level of access granted to a user, in consultation with the user's line manager;
- The provision of training and for assisting line managers with the determination of necessary competencies / training requirements for personnel performing work that requires them to use the Clinical Application.
- Ongoing management and maintenance of user accounts and access levels to ensure the effectiveness and efficiency of implemented controls, to assess whether controls are being adhered to and check compliance against policy and legislative requirements including those set out in PD2013_033, JH&FMHN policy 2.156 *Information Security Management System (ISMS);* and
- Reporting any security incident or privacy breach to the Chief Information Officer (CIO) and Information Management (IM).

Clinical Applications Advisory Group (CAAG) is responsible for:

- Approving changes made to role-based access levels within the Clinical Applications to assist ICT in its configuration.

3. Procedure Content

3.1 Reportable Security Incidents

Reportable Security Incidents include, but are not limited to:

- A breach by JH&FMHN staff of any of the 15 Health Privacy Principles (HPPs) under HRIPA. These HPPs are detailed in the *NSW Health Privacy Manual for Health Information* section 2.2 and fall under 7 principle categories of:
    - Collection, Security, Access and Amendment; Accuracy; Use; Disclosure; Other.
- Compromised confidentiality of personal health information, including unauthorised access to personal health information stored within the Clinical Applications;
- Compromised confidentiality of passwords, and/or staff logging activity using another staff member's username and password;
- Compromised confidentiality and integrity of the Clinical Applications; and,
- Attempts to bypass security systems or to gain unauthorised access to any of the Clinical Applications.

If a JH&FMHN staff member suspects any type of reportable security incident to have occurred they must log an incident on the *Incident Information Management System* (IIMS) and advise their line manager or After Hours Nurse Manager (AHNM), if outside of business hours as soon as practicably possible. It is the responsibility of the line manager to report the incident as soon as practicable to their Director, CIO and/or IM.

3.2 Access

Access to personal health information is only possible via a secure logon process designed to minimise the opportunity for unauthorised access. Access to Clinical Applications will not be approved unless the staff member's line manager has completed the online *Network Access - New Account.*

All JH&FMHN Clinical Application users, including agency staff, contractors, students, vendors and other persons will have a unique system logon with an associated password that identifies the individual on the system. A stafflink number must be assigned to the individual prior to Clinical Application Access being provided. Management should liaise with Workforce to provide relevant details for a stafflink number to be assigned.

If changes are required to a staff member's access to Clinical Applications due to a change in role or responsibility, it is the responsibility of the user and the line manager to complete a *Change of Access & Termination* form.

If the user requires a level of access higher than that which they previously had, a training analysis for the additional functionality is required before the access can be changed.

Upon completion of any required training, the user's access is updated. Users will be required to log out of the system and back in to see any changes made to their account.

3.3 Permissible and Appropriate Use of Clinical Applications

All Clinical Applications must be used in a manner that complies with all security requirements such as user account and data security as outlined in JH&FMHN policy 2.002 *Acceptable Use of Communication Systems*.

All JH&FMHN Clinical Applications users must ensure they follow required procedures for maintaining data security, as described in the *Network Account Request* and ensure they understand their responsibilities under Security and Privacy legislation. Computers must not be left unlocked or unattended when staff are logged into a Clinical Application. Screen lock and logout features must be used if a computer is to be left unattended.

Clinical documentation within the Clinical Applications must also comply with the principles and standards outlined in JH&FMHN policy 4.020 *Implementation Guide to NSW Health Policy: Health Records*. Users must ensure only valid information is entered.

3.4 Monitoring

JH&FMHN will monitor the use of the Clinical Applications (including when the person is working offsite). For further details refer to JH&FMHN policy 2.002 *Acceptable Use of Communication Systems*.

3.5 Official Records

As noted earlier, a patient's Health Record's nature and content within the Clinical Applications and its use constitutes a JH&FMHN record, which may be subject, to the *State Records Act* (1988), the *Government Information Public Access Act 2009* (GIPA) and the HRIPA.

3.6 Management of Forms

The *Network Account Request* and *Change of Access & Termination* forms are retained electronically.

4. Definitions

Must

Indicates a mandatory action to be complied with.

Patient Health Record

Indicates a patient has a paper-based and electronic health record.

Should

Indicates a recommended action to be complied with unless there are sound reasons for taking a different course of action.

5. Legislation and Related Documents

Legislation	*Commonwealth Privacy Act (1988) (Cth)* *Government Information (Public Access) Act 2009* *Health Services Act 1997* *Health Records Information and Privacy Act 2002* *Health Records and Information Privacy Regulation (2002)* *Independent Commission Against Corruption Act 1988* *Privacy and Personal Information Protection Act 1998* *State Records Act 1998*
NSW MoH Information Bulletins and Policy Directives and Manuals	*NSW Government Digital Information Security Policy* *NSW Health Privacy Manual for Health Information* PD2009_057 *Records Management - Department of Health* PD2012_069 *Health Care Records – Documentation and Management* PD2013_033 *Electronic Information Security Policy – NSW Health*
JH&FMHN Policies, Forms and Guidelines	2.002 *Acceptable Use of Communication Systems* 2.156 *Information Security Management System (ISMS)* 4.020 *Implementation Guide to NSW Health Policy: Health Records* *Network Account Request* *Change of Access & Termination*