Health
Justice Health and
Forensic Mental Health Network

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

Health Records

Implementation Guide to NSW Health PD2012_069 Health Care Records – Documentation and Management and PD2009_057 Records Management – Department of Health

Policy Number 4.020

Policy Function **Clinical Information Management**

Issue Date 10 January 2019 *(Minor update on 28 February 2020 on the procedures for the storage of progress note)*

Summary The maintenance of an accurate and comprehensive Health Record is an essential element of patient care. The Health Record is compromised of the paper-based and electronic Health Record.

This document provides guidance to all Justice Health and Forensic Mental Health Network staff, for specific policies and procedures on clinical documentation and the Health Record, when implementing relevant NSW Health policies. Staff must read this document in conjunction with the following overarching NSW Health policies:

1. PD2012_069 *Health Care Records – Documentation and Management*
2. PD2009_057 *Records Management – Department of Health*

Responsible Officer Executive Director Corporate Services

Applicable Sites

☒ Administration Centres
☒ 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 4.020 (Jul 2015; May 2010)

Change Summary

- Revised Section 3.3 Monitoring to include the QARS audit and JHeHS audits
- Updated Network branding
- Hyperlinks updated
- Clinical Applications updated throughout document

TRIM Reference POLJH/4020

Authorised by Chief Executive Justice Health and Forensic Mental Health Network

1. Preface

This policy applies to all Network staff, including agencies, contractors, vendors and other persons who have access to the Network's patient Health Records, including those who access the system remotely. The combination of a paper-based and electronic Health Record may be referred to as a hybrid health record, however for the purpose of this policy the term 'Health Record' will be used to refer to the hybrid Health Record. The Networks Health Record includes and comprises of the:

- Paper-based Health Record; and,
- Network's Clinical Applications Systems (electronic Health Record):
- Patient Administration System (PAS);
- Justice Health electronic Health System (JHeHS);
- Community Health Information Management Enterprise (CHIME);

The maintenance of an accurate and comprehensive patient Health Record is an essential element of patient care. A patient's Health Record is a documented account of a patient's health and treatment during each encounter with a health care professional and serves as a basis for review, study and evaluation of the care given to the patient. It also provides a means of communication regarding episodes of illness for all clinicians and will serve as a basis of maintaining continuity of patient care.

The patient's Health Record, with the appropriate authorisation, may also be used for communicating with regulatory bodies, planning, research, education, financial reimbursement, quality improvement, public health, complaints' management, medico-legal and statutory requirements.

The objectives of this policy are to ensure that:

- The patient's Health Record provides complete and comprehensive documentation of all aspects of patient care;
- The patient's Health Record is used to promote continuity of a person's care across time and service boundaries:
    - Provide effective communication to the health care team;
    - Provide for a person's safe and appropriate continuing care;
    - Enable the evaluation of a person's progress and health outcome; and,
    - Retain its integrity over time.

All information in a patient's Health Record is managed in a confidential and secure manner;

- The patient's Health Record complies with the *State Records Act 1998*, privacy legislation and NSW Health standards; and,
- Improved clinician awareness and access to patient health information is available at the point of care.

2. Policy Content

2.1 Mandatory Requirements

The Network staff must comply with this policy in conjunction with the following overarching policies relating to the creation and management of a patient's Health Record. This extends to Privately Operated facilities:

- PD2012_069 *Health Care Records – Documentation and Management*; and,
- PD2009_057 *Records Management – Department of Health.*

The NSW public health sector, as with all public sector agencies in NSW, is required to comply with the *Health Records and Information Privacy Act 2002* (HRIPA) and *Privacy and Personal Information Protection Act 1998* (PPIPA). Both specify a series of rules designed to protect the privacy of personal information, including personal health information, in NSW.

It is the responsibility of all NSW Ministry of Health (the Ministry) personnel and their contractors to be aware of and comply with the requirements outlined in the *NSW Health Privacy Manual for Health Information* and PD2015_036 *Privacy Management Plan – NSW Health*.

2.2 Implementation – Roles & Responsibilities

In accord with the principles set out in PD2012_069 *Health Care Records – Documentation and Management,* all Network clinicians who provide a person with care, assessment, diagnosis, management and/or professional advice are responsible for legibly documenting and dating this activity in the patient's Health Record. The Ministry periodically updates its policies and guidelines. The Network's staff should regularly check the NSW Health *Policy Directives and Guidelines internet page* for the most current policies and guidelines on patient Health Records.

Managers are responsible for:

- Ensuring the requirements of this policy are disseminated and implemented in their facility / service;
- Ensuring clinicians within their facility / service have timely access to the patient's Health Record;
- Ensuring clinicians within their facility comply to any Health Record related business processes; and
- Monitoring compliance with this policy, including health record audit programs, and acting on the audit results.
- Ensuring Clinicians have the appropriate Network Access for Clinical Application Systems

Clinicians are responsible for:

- Maintaining their knowledge, documentation and management of Health Records consistent with the requirements of this policy;
- Ensuring they are aware of current information about the patient under their care, including where appropriate reviewing entries in paper and electronic patient's Health Record; and
- Complying with all Health Record related Business Processes.
- Completing the appropriate elearning modules relevant to the patient Health Record

Clerical staff are responsible for:

- Document tracking the Health Record across Health Centres.
- Ensuring all Downtime packages are available at the Health Centre for use when required.
- Any other admin related duties in the preparation and maintenance of the Health Record.

Health Information and Record Service (HIRS) is responsible for:

- The ongoing review and maintenance of the patient Health Record;
- Storage of paper Health Records of patients who have been released from custody; and
- Auditing compliance and data integrity through reports.
- Quality checking Downtime forms within Clinical Application Systems.

Failure to maintain appropriate Health Record entries – in either paper or electronic format - may jeopardise continuity of care, patient safety and as well as the professional indemnity and/or registration of staff.

3. Procedure Content

3.1 Ownership

The Network's patient Health Record is the property of the Network and not individual clinicians. Health Records must not be removed from Network facilities. The only exceptions when the record may be removed are:

- When subpoenaed by a Court (and a photocopy is not acceptable);
- When required for the Coroner (and a photocopy is not acceptable);
- When required by the Forensic Mental Health medium secure units for a time-limited loan; and
- At the discretion of the HIRS Manager.

3.2 Documentation

A uniquely identifiable patient's Health Record must be created at the time of a patient's first contact with the Network. Clinicians are required to document in the patient's Health Record and must access both paper and electronic formats of the Health Record to obtain a complete and accurate assessment of the health status of a patient.

Clinicians must utilise the Clinical Application Systems in accordance with their intended purpose. Paper records must not be used as an alternative to the Clinical Application Systems where there is functionality in the systems to record the intervention or planned action, with the exception documentation during down time periods.

All documentation made in the patient's Health Record must comply with the standards set out in PD2012_069 *Health Care Records – Documentation and Management*. Further to the standards outlined, the following standards must also be followed within the Network:

- Clinicians must ensure documentation is recorded against the correct patient.
- Clinicians must check the patient ID (MIN, CIMS, MRN or AUID) and the name on the patient's Health Record prior to making an entry in the Health Record.

- Clinicians must not make an entry in the patient's Health Record on behalf of another person, especially where the episode of care or procedure is performed by another clinician. This includes the usage of another clinician's user credentials in JHeHS, PAS, CHIME and/or Titanium.
- Approved Network *Clinical Abbreviations* and *Non-Clinical Abbreviations* should be documented in a patient's Health Record.
- The Health Record may consist of multiple volumes. Staff must not maintain a secondary Health Record for their own purposes, including electronic storage of data on network drives in MS Office applications. All documentation regarding the patient must be filed within the patient's Health Record.
- Every patient contact, intervention or service provided must be recorded in the patient's paper-based Health Record and/or the patient's electronic Health Record. All entries in the Health Record are arranged in chronological order and, in the case of electronic records, are accessible and linked to the individual paper-based record.
- An incident should also be logged in the *Incident Information Management System (IIMS)* for all documentation incidents identified within the patient's Health Record.
- The Network staff creating new Health Record volumes must follow the *Health Records Procedure Manual HIRS Staff* or *Health Records Procedure Manual Health Centre Clerks.*
- All Clinical Applications used by the Network staff must have the capacity to enable identification of individual health personnel who have entered the information.
- An Integrated Care Service/Medical Appointments Unit satellite record may exist for the patient but must be approved by the HIRS Manager and electronically linked with the patient's Health Record within PAS.

3.2.1 Paper-Based Records

The standardised approach to documentation is outlined in PD2012_069 *Health Care Records – Documentation and Management*. The following must also occur when documenting in a paper based Health Record:

- Each entry into the paper Health Record must be in English, using a black pen and be legible. It must include the name, designation of the author, date (day, month and year), and time (HH:MM using 24 hour clock) in which the entry was made. The professional discipline (for example Physiotherapy, Psychiatry, Primary Health) should be recorded at the beginning of the entry.
- The patient's printed PAS label should be placed on the top right hand corner of every paper-based Health Record and Clinical Form, including double sided forms. If a PAS label is unavailable the following must be recorded by clinicians in the place of the PAS label:
    - Patient number (MIN, CIMS, MRN or AUID);
    - Family name/Surname;
    - Given name;
    - Date of Birth; and,
    - Sex.
- For privacy and confidentiality reasons, Corrective Services NSW (CSNSW) inmate labels must not be used in the Health Record – only PAS printed labels are to be used.

- All progress note entries must be recorded within JHeHS using the patient's electronic Progress Notes. The exception to the rule is when there is a confirmed JHeHS downtime, and paper-based progress notes should be used and then either retrospectively typed into JHeHS as an electronic Progress Note or scanned into the Progress Notes tab within JHeHS.
- If an entry omits details which are subsequently documented, a heading 'ADDENDUM' must be made with the date and the time of the omitted event recorded as well as the date and time of the ADDENDUM. The ADDENDUM must also capture the clinician's details.
- All 'in error' documentation must have a single black line crossed through the in error entry and initialled by the clinician.
- All paper-based forms must be filed into the patient's paper-based Health Record as soon as practical to ensure the validity, reliability and completeness of the Health Record.
- Original notes are not to be removed or destroyed. Interim diagnostic results or faxed/photocopied documents must be removed and destroyed when the final diagnostic results or original documents are available.
- If a page in the health record is not completed and a new page is commenced a single black line is to be made through the rest of the page to prevent further entries being made.
- Network policy 2.027 *Forms Management* must be complied with in relation to Health Record and Clinical Forms.

3.2.2 Electronic Health Record (Clinical Application Systems)

It is important that clinicians are aware that patient health information is recorded within the Clinical Application Systems (PAS, JHeHS, CHIME and Titanium). To obtain a full clinical **picture** of a patient's health status, clinicians must review the electronic Health Record in conjunction with the paper-based Health Record. Clinicians must not assume that the paper Health Record holds all patient health information. Information contained within the electronic Health Record is considered an integral part of the patient's Health Record. Staff must comply with the Network policy 4.014 *Clinical Application Systems – Alerts, Health Conditions, Allergies or Adverse Drug Reactions* when recording the following information within the Clinical Applications.

The standardised approach to documentation within an electronic Health Record must also comply with the standards that are outlined in PD2012_069 *Health Care Records – Documentation and Management*. The following must also occur when documenting in an electronic Health Record:

- In accordance with Network policy 2.125 *Clinical Applications Access and Security*, each Clinical Application user is allocated a unique username and login credentials following the completion of Clinical Application training. The sharing of logon credentials must not occur under any circumstances.
- Each clinician is accountable for the care they provide and for the activity recorded under their username within the Clinical Application systems. All activity recorded against a username can be used as evidence in a Court of Law.
- All progress notes must be recorded in the patient's electronic Progress Notes within JHeHS
- All users must only record their own activities within the Clinical Application Systems. Information should not be entered on behalf of anyone else. Limited exemption to this requirement is granted to agency

locum/casual/VMO leave relief Medical staff, who attends for less than one, four (4) hour session per month.

- Staff must ensure that all newly created electronic forms (e-forms) in JHeHS for a patient are finalised upon completion and not left as in interim e-form. If an amendment or update needs to be made to a finalised e-form, this must be made via the amendment button, which will create a new version of the e-form.
- All mandatory items must be completed prior to finalisation. All other fields should be completed to the best of the clinician's ability where clinically appropriate.
- All relevant paper forms that are to be scanned into the patient's electronic JHeHS record must be added with the following details completed. Please refer to the *JHeHS Scanning Categories of Scanned Documents in JHeHS* document for further information.
    - Category;
    - Title of Document;
    - Date of Document; and
    - Service Provider.
- There are identified scanned documents in a patient's JHeHS record that must be reviewed and/or signed off using the scanned documents dashboard. Please refer to the *Scanned Documents Dashboard Business Process* for further information.
- All pathology results received electronically into the patient's JHeHS Health Record must be signed off by Medical Officers, Public Sexual Health Nurses, Nurse Practitioners, or Midwives. Please refer to the *Pathology Results Management Procedure* for further information.

3.3 Downtime

In the event of an unplanned Downtime, the individual must confirm with myIT prior to reverting to Downtime processes. Please refer to the myIT Downtime intranet page to access the Downtime Forms, Business Processes and further guidance.

Downtime forms must be made available within all clinical areas. All downtime forms can be accessed and printed via the intranet. There are paper Downtime forms available to document patient Alerts, Health Conditions, Allergies or Adverse Drug Reactions. It is the responsibility of all clerical staff to ensure that there are numerous forms available in the event of a Clinical Application System being unavailable. These forms must be made available for clinical and clerical staff to capture information before the individual that completes it then retrospectively updates the patient's Health Record within the correct Clinical Application System when Downtime has ended. If required, this should also be communicated via Clinical Handovers.

Following downtime, all Downtime forms must be sent to the Health Information and Record Service for quality checking and appropriate destruction.

3.4 Monitoring and Audits

The Governance Unit coordinates and overseas the Clinical Documentation and Health Record Audit in the Quality Audit Reporting System (QARS) to support evidence for The National Safety and Quality Health Service

(NSQHS) Standard 1 Governance for Safety and Quality in Health Services Organisations. Audit results are monitored and reported to the Directorates, the Clinical Governance Committee and the Quality Council. There are separate audits for Custodial Health (adult and adolescent), Long Bay Hospital (LBH) and the Forensic Hospital. The NUM or Nurse in Charge (NIC) is responsible for addressing any identified documentation issues with individual clinicians.

The JHeHS Quality Assessment and Audit Officer coordinates and oversees the monitoring and auditing of:

- Pathology mismatches;
- Preliminary pathology result reconciliation;
- Unsigned pathology results;
- Interim e-forms and eprogress notes
- Student eProgress notes not countersigned;
- Allergies and Health Conditions recorded in JHeHS against e-forms; and,
- Scanned Documents Dashboard.

The results are reported to the Manager, Information Management, Nurse Unit Managers (NUMs), other Network managers, the Clinical Application Advisory Group (CAAG), and the pathology labs where relevant.

3.5 Privacy and Confidentiality

All information in a patient's Health Record is confidential. Disclosure of this information is only permissible under certain conditions. For further information staff should refer to the Network policy PD4.030 *Implementation Guide to NSW Health Policy: Releasing and Requesting Health Information* and the *NSW Health Privacy Manual for Health Information*. As a general rule, a patient's Health Record is only available to:

- The person to whom the record relates;
- Health care professionals and clerical staff currently involved in the continuing care, observation, assessment, diagnosis, management/treatment, record management and professional advice; and,
- Health care professionals and clerical staff in other limited circumstances in accordance with legislation and common law.

3.6 Storage and Security

All patient Health Records must be stored in environmental conditions that are appropriate to their format and retention period according to State Records Act 1998. Further to the conditions set out in PD2009_057 *Records Management – Department of Health,* the Network's staff must adhere to the following to ensure the safe storage of Health Records:

- Paper based Health Records must be kept in lockable storage or secure access areas when not in use, that is, lockable record rooms, lockable cabinets and filing shelves.
- Documents containing personal health information must not be left unattended on workbenches or anywhere they might be visible to unauthorised persons.
- Electronic documentation must be protected against unauthorised use and access. All staff must logout or utilise screen lock features when leaving a workstation unattended.

Further information on electronic record access, storage and security can be found in the Network policy 2.125 *Clinical Applications Access and Security*.

3.7 Transport of Health Records

Staff who prepare a patient's Health Record for transportation, must ensure the Health Record is correctly assembled and any loose clinical documentation is correctly filed in accordance with the Network *Order of Forms*.

Information and e-forms recorded within Clinical Application Systems should not be printed except for the following purposes:

- Medico-legal requests;
- Providing Local Health Districts (LHDs) and other health care providers with the Clinical Summary Transfer to External Hospital e-form for external appointments and/or admissions to other LHDs, where the paperwork must accompany the patient and the patient is in custody at the time of the appointment and/or admission;
- Providing the patient with the Release Summary and Transfer of Care e-form upon release;
- Providing Corrective Services NSW (CSNSW) with the Drug and Alcohol and Mental Health Summary of Reception Screening Assessment e-form;
- Providing CSNSW with the Health Problem Notification Form (HPNF) from PAS; and
- Other clinical reason as appropriate.

If information is printed from Clinical Application Systems for a reason other than stated above, the printed information must be destroyed securely in a secure destruction bin. The printed information must not be filed within the patient's paper Health Record as it is not the source of truth.

All paper-based health documentation must be transferred in a sealable/lockable Health Record transport satchel clearly marked as confidential.

The Health Record must only be transported by a CSNSW escort vehicle, Juvenile Justice NSW (JJNSW) Transport vehicle or an approved courier. Health Records must not be transferred by private vehicles or by Australia Post. Staff who are working in Community Forensic Mental Health, Community Integration Team or the Connections Project Team, are permitted to transport health records for work related purposes only. Health records must not be stowed in vehicles when not in use.

It is the responsibility of all Network staff to ensure the security and confidentiality of the patient's Health Record. Care must be taken to ensure paper Health Records are not damaged or compromised in any way. An IIMS Incident Report must be logged if any security breaches are identified.

All movements of Health Records must be correctly tracked on PAS.

3.8 Retention and Destruction

The patients paper-based Health Records will be retained for a period of 30 years as per *General Disposal Authority 17 Public Health Services: Patient/Client Records* following:

- the last attendance in either the custodial or community setting;

- the last official contact;
- the last legal request made for the Health Record; or
- the individual attaining the age of 18.

Following Chief Executive and State Records approval, HIRS Management is responsible for the secure destruction of sentenced Health Records that meet the retention period. All destruction activity must be recorded within PAS.

All scanned health record forms into the electronic health record must be forwarded to HIRS. HIRS will quality check the form within the electronic health record and retain the forms for a minimum of 6 months before destroying.

4. Definitions

Must

Indicates a mandatory action required to be complied with.

Patient Health Record

Indicates the patient's paper-based and electronic Health Record combined.

Should

Indicates a recommended action to be followed 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 and Information Privacy Act 2002* *Privacy and Personal Information Protection Act 1998* *State Records Act 1998* *General Disposal Authority 17 (GDA17) Health Services, Public: Patient/Client Records*
Standards	*AS 2828-1999 Paper Based Health Care Records* *AS 2828.2-2012 Health Records Digitized (scanned) health record system requirements*
NSW Health Policy Directives, Guidelines and Manuals	PD2015_036 *Privacy Management Plan – NSW Health* PD2009_057 *Records Management - Department of Health* PD2015_049 *NSW Health Code of Conduct*

	PD2012_069 *Health Care Records – Documentation and Management* PD2013_033 *Electronic Information Security Policy - NSW Health* *NSW Health Privacy Manual for Health Information*
Network Policies, and Forms	2.027 *Forms Management* 2.125 *Clinical Applications Access and Security* 4.030 *Requesting and Disclosing Health Information* 4.014 *Clinical Application Systems – Alerts, Health Conditions, Allergies or Adverse Drug Reactions* *Health Record Procedure Manual HIRS Staff* *Health Record Procedure Manual Health Centre Clerk* *JHeHS Scanning Categories of Scanned Documents in JHeHS* *Pathology Results Management Procedure* *Scanned Documents Dashboard Business Process* *Order of Forms*