SESLHD PROCEDURE COVER SHEET

NAME OF DOCUMENT	Managing Chart Access Audits in Electronic Health Records
TYPE OF DOCUMENT	Procedure
DOCUMENT NUMBER	SESLHDPR/522
DATE OF PUBLICATION	September 2023
RISK RATING	Low
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standard: Standard 1 - Clinical Governance
REVIEW DATE	September 2028
FORMER REFERENCE(S)	N/A
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Director, Clinical Governance and Medical Services
AUTHOR	SESLHD Health Records & Medico-Legal Committee
POSITION RESPONSIBLE FOR THE DOCUMENT	Co-Chairs, Health Records & Medico-Legal Committee
FUNCTIONAL GROUP(S)	Records Management – Health
KEY TERMS	Audit, proactive, reactive, Powerchart, chart access, privacy, confidentiality, eMR, Health Records, eMR, Medical Records
SUMMARY	This procedure provides a framework for managing access audits within electronic health records.

Managing Chart Access Audits in Electronic Health Records

SESLHDPR/522

1. POLICY STATEMENT

Personal health information may only be accessed by users in relation to their official work duties. This procedure has been developed to outline processes for auditing access to health information to ensure that access to the eMR is in line and compliant with NSW Health Policy.

2. BACKGROUND

Personal health information may only be accessed by users in relation to their official work duties.

This procedure outlines the steps required to manage chart access audits within electronic health record systems. Specifically, it aims to:

- Maintain a process for auditing all access to electronic health records in accordance with privacy requirements
- Identify irregularities in access to health information and outline actions for management and referral of such matters
- Foster awareness of the auditing process privacy requirements which will assist in preventing the improper access, misuse and/or disclosure of personal health information.

3. DEFINITIONS

Affiliated/external electronic health record user: Person with access to the electronic health record who is not a direct employee of SESLHD. For example, Medical Students, Staff of War Memorial and Calvary Hospitals, etc.

Audit by patient: An audit run against an individual *patient* to check all persons who have accessed their electronic record within a specified time range

Audit by staff member: An audit run against an individual *staff member* to check all patient records that have been accessed within a specified time range

Chart: also known as “health record”

Client/patient: any person to whom a health care provider owes a duty of care in respect of provision of health care services

Clinical Portal: Part of HealtheNet that provides NSW Health clinicians access to specific types of patient information imported from hospital electronic medical records.

Confidentiality*:* the restriction of access to information, and the control of the use of release of personal information, in order to protect patient privacy

Electronic Health Record: Includes all electronic health record systems such as eMR Cerner, eMaternity, eRIC, MOSAIQ, ARIA or any other electronic medical record application/system.

eMR Access Audit: Audit of access to the Cerner electronic medical record. May be conducted via the Explorer "eMR Chart Access Audit" Report or P2 Sentinel access auditing tool.

HealtheNet: An eHealth NSW program that connects NSW Health systems.

Health Information:

(a) personal information that is information or an opinion about:

(i) the physical or mental health or a disability (at any time) of an individual, or

(ii) an individual's express wishes about the future provision of health services to him or her, or

(iii) a health service provided, or to be provided, to an individual, or

(b) other personal information collected to provide, or in providing, a health service, or

(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or

(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual, or

(e) healthcare identifiers, but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the HRIP Act generally or for the purposes of specified provisions of the HRIP Act

Health Record: a documented account, whether in hard copy or electronic form, of a client/patient's health, illness, and treatment during each visit or stay at a public health organisation
Note: holds the same meaning as "health care record", "medical record", "clinical record", "clinical notes", "patient record", "patient notes", "patient file", etc.

Health Service Staff – Anyone who carries out work for NSW health service, including employees, visiting health practitioners, contractors and sub-contractors, agency staff, volunteers, apprentices, trainees, and students.

HIM: Health Information Manager

HRIP Act (HRIPA): Health Records and Information Privacy Act 2002 (NSW)

misuse of information: a staff member has knowingly and intentionally accessed, used and/ or disclosed information held by the health service for a purpose outside of, and unrelated to, their work duties. Such breaches of privacy may possibly constitute corrupt conduct.

MRM: Medical Record Manager

My Health Record: Australia wide secure online system with personal health information accessible to healthcare providers/organisations
Note: My Health Record is an "opt-out" system

PCO: Privacy Contact Officer

Person of interest: A person or group of persons targeted for auditing because of the presence of increased privacy-related risk factors. May include, but not be limited to, the following:

- Celebrity / Famous person
- Politician
- News worthy person / person in the news
- Novelty injuries / "Interesting" conditions 'deceased under concerning circumstances (for example: sentinel events)
- Staff members
- Staff members' family / partners
- Other patients/clients who have voiced concerns during their stay

In some of the above cases it may be up to staff to use their discretion as to who should be notified as a person of interest.

Proactive audit – random: An random audit of access by staff members or access to a patient record performed by Health Information Managers, Mental Health and Community Clinical Information Coordinators, Drug and Alcohol Health Information Managers, ward/unit or emergency Nurse Unit Managers, and Medical Workforce Managers

Proactive audit – persons of interest: An audit that is initiated based on notification of person of interest presentation to a health service. The audit will be run to check all eMR account holders who have accessed the patient chart

Reactive audit: An audit that is initiated following a complaint/potential breach of confidentiality from a patient, authorised representative or staff member.

Settings: Health care or business settings which should be in scope of this audit procedure:

- Inpatient units/wards
- Emergency departments

- Mental health community
- Community health services
- Outpatient Clinics.

4. RESPONSIBILITIES

4.1. All Health Information Managers/Medical Record Managers will:

- Perform:
  - reactive audits based on a complaint or notification
  - proactive audits based on presentation notification of a person of interest
  - proactive random audits
- Submit the results of all audits to the SESLHD Health Records and Medicolegal Committee.
- Retain a copy of the audits and provide as requested for Accreditation purposes.
- Secure the paper health record if necessary
- Liaise with data managers of non-Cerner EHRs for system reports
- Escalate suspected breaches to the Employee Relations and/or the Privacy Contact Officer as per this policy
- Provide feedback to relevant parties post audit and/or investigation if appropriate
- Assist community health or other affiliated facilities/departments with auditing where required.

4.2. Data Managers for electronic health record (non-Cerner) systems will:

- Liaise with site HIMs/MRMs regarding person of interest or complaint audits. This includes:
- Providing HIMs/MRMs reports/audits when required/requested
- Escalating any complaints, persons of interest, or issues to site HIMs/MRMs for investigation
- Perform proactive random audits
- Retain a copy of the audits and provide as requested for Accreditation purposes.

4.3. Drug and Alcohol Health Information Manager will:

- Submit results to Drug and Alcohol Governance Group and Community Health Outpatient Care (CHOC) Working Groups and the SESLHD Health Records and Medicolegal Committee.

4.4. Mental Health Information/eHealth Support Manager will:

- Liaise with local site executive where suspected breaches are identified
- Submit results to the eHealth Committee and Clinical Governance Committee
- Escalate confirmed breaches, via the Mental Health Service General Manager, to Employee Relations.

4.5. Community Health Service Team Leaders will:

- Perform proactive random audits

- Feed results to Community Health Managers and Community Health Outpatient Care (CHOC) Working Groups and the SESLHD Health Records and Medicolegal Committee
- Where community health sits in a 3rd scheduled hospital refer results to the medical records department.
- Retain a copy of the audits and provide as requested for Accreditation purposes.
- Securing the paper health record if necessary
- Notification of attendances by Persons of Interest or complaints/notifications to site HIMs/MRMs for audit initiation.

4.6. Nurse, Midwifery, Medical Workforce, Outpatient Clinic, and Allied Health Managers:

- It is recommended that proactive random audits are completed on monthly basis, the suggested volume is five (5) patient charts and/or five (5) staff member audits. Note – a higher number or a percentage may be a more appropriate depending on the sample size/activity. If audits are completed, they should be retained for accreditation purposes.
- Should notify site/facility HIMS/MRMs of attendances by Persons of Interest or complaints/notifications for audit initiation.

4.7. Health ICT

- Provide first level support and escalation to vendor for systems issues.
- Refer any requests for privacy breaches / investigations to the SESLHD PCO or relevant site-based HIM/MRM.

4.8. Privacy Contact Officer

- Advise on, refer, or investigate matters as required
- Notification of attendances by Persons of Interest or complaints/notifications to site HIMs/MRMs for audit initiation
- NSW Health, IPC, and OAIC notifications/reports of breaches where required
- Review as to whether open disclosure is appropriate, and if so, action
- Liaise with HIMs/MRMs regarding risk mitigation – such as follow-up audits or access removal
- Notify affiliated/external organisations of suspected breaches as identified by a HIM/MRM.

4.9. Internal Audit

- Notification to ICAC where required.

4.10. Hospital/Facility Business Partners

- Provide site HIMs/MRMs basic employment information (such as position title, work location, and reporting lines) when required/requested.

4.11. SESLHD Employee Relations

- Investigate and manage misconduct processes for alleged breaches by SESLHD staff escalated by HIMs/MRMs in accordance with Managing Misconduct PD2018_031
- Report confirmed breaches to PCO and Internal Audit
- Provide HIMs/MRMs feedback on unsubstantiated breaches
- Responsible for notification of breaches to registration boards and law enforcement agencies where applicable
- Provide reports to the SESLHD Health Records and Medico-Legal Committee once a year outlining general investigation outcomes (i.e. number of investigations, general outcomes, disciplinary action stats).

5. PROCEDURE

This procedure is initiated:

- Upon patient complaint or identified potential breach of confidentiality
- For random patient chart audits or staff member audits
- When a breach of confidentiality has been identified
- Upon notification of attendance of a person of interest to a facility/service.

5.1 Types of Audits

5.1.1 Reactive Audits

- Notification of potential breach of privacy (e.g. complaint or concern) is received
- Health Information Manager (HIM) or Medical Record Manager (MRM) for relevant site is contacted
- HIM/MRM records details of the notification in their site's Chart Access Audits Log (Example in Appendix B)
- HIM/MRM informs notifier of investigation and review process and possible timelines
- HIM/MRM runs the an access report for the relevant staff member/s or particular patient record (dependent upon nature of complaint)

  Note: If a patient has been identified as presenting to departments/facilities/wards that utilize a non-Cerner electronic health record system, the relevant data manager/s should be contacted to run the equivalent access reports and provide the results to the HIM/MRM.

- Access report/s are analysed against particulars of complaint (see Appendix A for more information on analysing reports).
  Note: If staff member is part of the SESLHD Mental Health Service then their executive or General Manager should be consulted for input where queries exist.

- Results of analysis:
  - If analysis identifies irregularities or potential breaches in access to health information the HIM/MRM:
    - updates details within the site's Chart Access Audits Log
    - Escalates the matter as per Section 5.3 of this procedure
    - Notifier is informed of escalation if appropriate.

  - If analysis does not identify any irregularities or potential breaches; results should be entered in the site's Chart Access Audit Log and feedback given to notifier if appropriate.

5.1.2 Proactive Audits (random patients or staff members)

Managers, HIMs, Data Managers, team leaders, and other disciplines outlined above should run random eMR Access Audits on monthly basis for their relevant business unit on at least five (5) random patients and/or staff members.

- If analysis identifies irregularities or potential breaches in access to health information the staff member should escalate to the site HIM/MRM for further investigation

- HIM/MRM records details of the notification in their site's Chart Access Audits Log (Example in Appendix B)

- HIM/MRM informs notifier of investigation and review process and possible timelines

- Site HIM/MRM re-runs any access reports for further information if required.

  Note: If a patient has been identified as presenting to departments/facilities/wards that utilize a non-Cerner electronic health record system, the relevant data manager/s should be contacted to run the same reactive audit report and provide the results to the HIM/MRM.

- Audit report/s are analysed against particulars of complaint (see Appendix A for more information on analysing reports).
  Note: If staff member is part of the SESLHD Mental Health Service then their executive or General Manager should be consulted for input where queries exist

- Results of analysis:
  - If analysis identifies irregularities or potential breaches in access to health information the HIM/MRM:
    - updates details within the site's Chart Access Audits Log
    - Escalates the matter as per Section 5.3 of this procedure
    - Notifier is informed of escalation if appropriate

  - If analysis does not identify any irregularities or potential breaches; results should be entered in the site's Chart Access Audit Log and feedback given to notifier if appropriate

5.1.3 Proactive Audits (Persons of Interest)

- Notification of person of interest presentation may be made to site HIM/MRD by any member of staff. Notifications must include:
  - Identifying information (Name/DOB or MRN)
  - Reason for notification
  - Time frame for audit if outside of current/most recent attendance

- HIM/MRM records details of the notification in their site's Chart Access Audits Log (Example in Appendix B)

- HIM/MRM informs notifier of investigation and review process and possible timelines

- HIM/MRM runs an eMR Access Audit against the staff member/s or particular patient record (dependent upon nature of complaint)

  Note: If a patient has been identified as presenting to departments/facilities/wards that utilize a non-Cerner electronic health record system, the relevant data manager/s should be contacted to run the same reactive audit report and provide the results to the HIM/MRM.

- Audit report/s are analysed against particulars of complaint (see Appendix A for more information on analysing reports).
  Note: If staff member is part of the SESLHD Mental Health Service then their executive or General Manager should be consulted for input where queries exist.

- Results of analysis:
  - If analysis identifies irregularities or potential breaches in access to health information the HIM/MRM:
    - updates details within the site's Chart Access Audits Log
    - Escalates the matter as per Section 5.3 of this procedure
    - Notifier is informed of escalation if appropriate

  - If analysis does not identify any irregularities or potential breaches; results should be entered in the site's Chart Access Audit Log and feedback given to notifier if appropriate

5.1.4 Proactive miscellaneous audits

Each electronic health record system may allow for varying levels of audit functionality. Further audits may include, but not be limited to audits of:

- Access by staff member to patient records with the same name/s as themselves
- Access to by staff member to an excessive number of patient records
- Access to particular patient's information by an unusually large number of staff members

The general process for these audits should follow the most relevant of the above processes as closely as appropriate.

5.2 HealtheNet and My Health Record access auditing

In NSW Health, access to the NSW Clinical Portal and My Health Record is via the state-wide HealtheNet system, which is accessed through the Cerner eMR.

The Clinical Portal and My Health Record can only be accessed via the eMR, and access should be identifiable within the access reports. A request for further information from HealtheNet should only be carried out if a breach has been identified at the site level

The HealtheNet team within eHealth manages the auditing functionality which tracks clinicians' access to the Clinical Portal and My Health Record. If an audit of access to the Clinical Portal or My Health Record is required, a request should be logged to the HealtheNet team via SARA.

Analysis and management of Clinical Portal and My Health Record access reports should be carried in the same manner as the eMR access reports.

5.3 Escalation of potential breaches to Employee Relations for further investigation

5.3.1 SESLHD Employees

If a potential breach is identified through the access reports, the HIM/MRM will submit a summary of findings as well as the access reports to the Employee Relations for further investigation. Employee Relations will conduct a formal investigation under the NSW Health Policy Directive PD2018_031 - Managing Misconduct.

Note: Serious alleged breaches should be reported to Internal Audit (ICAC notification) and the SESLHD PCO (risk/legal review) as soon as possible (even before an investigation proceeds).

As per the NSW Health Policy Directive PD2018_031 - Managing Misconduct, the normal timeline for investigations is up to 12 weeks, however, this is dependent upon scope, access to staff members, and other factors.

If Employee Relations does not find any evidence of a breach, they will inform the site HIM/MRM.

If a breach has been confirmed by the investigation, the Employee Relations will inform the following of the result:

- Privacy Contact Officer (PCO)
- Internal Audit
- Registration boards (where a breach constitutes unprofessional conduct and notification is required as per the policy)
- NSW Police (where breach consists a breach of law, and depending on circumstances, requires reporting to the Police for investigation/charge)

5.3.2 Affiliated/External employees

If the employee/s are from an affiliated/external facility, the HIM/MRM submit a summary of findings as well as the access reports to the SESLHD PCO. The PCO (on behalf of SESLHD) will notify the affiliated/external facility's Human Resources Department and Chief Executive to request a formal investigation.

Note: Affiliated/external facilities do not need to inform SESLHD of details of investigation or actions taken.

5.4 Confirmed Breach Notifications, Reporting, Feedback, and Open Disclosure

5.4.1 Notifications and reporting

Notifications or reports to government entities may be required where a privacy breach has been confirmed. Responsibility for review of the audit results and the appropriateness of notification is as follows:

- Ministry of Health - PCO
- Information Privacy Commission NSW (IPC) – PCO
- Independent Commission Against Corruption (ICAC) – Internal Audit
- Office of Australian Information Commissioner (OAIC) – PCO
- My Health System Operator (The Australian Digital Health Agency) – PCO (for breach involving My Health Record only as per Section 75 of the *My Health Records Act (2012)*

Note: Serious alleged breaches should be reported to Internal Audit (ICAC notification) and the SESLHD PCO (risk/legal review) as soon as possible (even before an investigation proceeds).

5.3.2 Reactive Audits – Feedback to notifier

Where an audit has been conducted in response to a complaint or query and no breach has been identified, the HIM/MRM should provide feedback of the results of the investigation to the notifier.

Where a breach has been identified, the PCO will review and feedback to the notifier.

When providing feedback to the requestor/notifier, details of the investigation and outcome should not be discussed. Only an outline of the process and general result may be provided. The HIM/MRM should assure the requestor/notifier that the complaint has been taken seriously and that the appropriate action has been taken as per appropriate policies.

The HIM/MRM should also ensure that the notifier/requestor is notified of their right to apply for a privacy internal review by the PCO.

5.3.3 Other audits – Open Disclosure/Notification of affected individuals

Where an audit and investigation have been undertaken and the patient/s has not been privy to the process, the PCO should weigh up whether the affected individual/s should be

notified. This may require the investigator to seek further advice from their management, executive team. *Note that in NSW notification of the affected individuals is not mandatory by law and a decision should be made based on individual circumstances.*

If the decision is made to notify the affected individual/s this should include:
- An outline of the process
- Assurance that the breach has been taken seriously and appropriate action has been taken
- Their right to apply for a privacy internal review by the PCO.

When providing feedback to the requestor/notifier, details of the investigation and outcome should not be discussed.

5.5 Follow-up auditing

For persons of interest and reactive audits, the HIM/MRM should re-run the audit process 3 months and 6 months after initial notification.

For confirmed breaches, the PCO will notify the HIM/MRM of the need for re-auditing.

6 DOCUMENTATION

Audit documentation and Chart Access Audit Log should be kept at a site/unit level.

Separate investigation records relating to potential misconduct will be held by Employee Relations. Only the investigation outcome letter will be held against the health service staff member's personnel record.

7 AUDIT

Site HIMs/MRMs report to the SESLHD Health Records and Medico-Legal Committee on proactive (persons of interest) and reactive audits.

Further auditing not required as the procedure outlines auditing processes.

8 REFERENCES

- Health Records and Information Privacy Act 2002
- The Independent Commission Against Corruption Act 1988 (NSW)
- My Health Records Act (2012)
- NSW Health Privacy Manual for Health Information
- eMR Chart Access Audit Quick Reference Guide (QRG)
- MoH Information Sheet – Reporting Misuse of Information as Suspected Corrupt Conduct H17/50926-2
- NSW Health Code of Conduct PD2015_049
- NSW Health Policy Directive PD2016_029 - Corrupt Conduct – Reporting to the Independent Commission Against Corruption (ICAC)
- NSW Health Policy Directive PD2018_031 - Managing Misconduct

9 VERSION AND APPROVAL HISTORY

Date	Version No.	Version and approval notes
17/06/2015	0.1	Author: Lee Speir (initial draft)
07/10/2015	0.2	Author: Hayley Ryan (conversion to standard SESLHD procedure format).
25/11/15	0.3	Reviewed and Approved: SESLHD Health Records and Medicolegal Working Group
September 2016	0.4	Draft for Comment
October 2016	0.5	Changes following Draft for Comment
November 2016	0.6	Tony Sara: Draft for Comment circulated to Directors of Clinical Services and Directors of Nursing
February 2017	0.7	Changes following Draft for Comment in November 2016 Reviewed and Approved: SESLHD Health Records and Medicolegal Working Group
July- August 2017	0.8	Changes following Draft for Comment in April and May 2017 Reviewed and Approved: SESLHD Health Records and Medicolegal Working Group
November 2017	0.9	Changes following initial DET review and further input by Internal Audit, PCO and Human Resources Advisory Services Reviewed and Accepted: SESLHD Health Records and Medicolegal Working Group
June 2020		Margaret Suda: Review as per recommendation from Executive.
Sept 2020	DRAFT	Reviewed and endorsed by the Health Records & Medico Legal Committee
Dec 2020	1.0	Draft for comment period – changes incorporated and endorsed by Health Records & Medico-Legal Committee.
Aug 2021	2.0	Update of investigation and misconduct management sections to reflect new working practices and practice of open disclosure.
14 September 2023	2.1	Minor review. Minor changes/amendments to reflect approval to use additional auditing functionality by Ministry of Health.

Appendix A: Tips for reviewing an access report

1) Manipulate the report in Excel so that every column can clearly be seen.
2) Add a column for “Auditor Comments”
3) Review the report to confirm staff members’ involvement in care. This can be done by:
   a. Checking the “eMR Comment” column on the report (this displays the comments put in by staff members when accessing the eMR)
   b. Using XR Charting to produce a PDF for each relevant episode of care. Then using the “Find” tool, search for each staff members name
   c. Checking other electronic health record systems for documentation
   d. Checking staff members area of employment
   e. Review JMO rosters
   f. Staff duty rosters
4) Highlight all staff members/patients that have been unable to be identified as being accessed as part of employment related duties

Appendix B:

Example of Received Audit Log for local sites.

Audit Number	Patient/Staff Member LAST NAME	Patient/Staff Member FIRST NAME	Facility	MRN	Source of Notification / Request	Date of Notification	Date of Audit	Audited dates	Audit Comments	Audit Submission Date	Submission/ Feedback Comments	Manager Completing Request	3 Month Follow up Audit	6 Month Follow up Audit
1														
2														
3														
4														
5														
6														