

SESLHD PROCEDURE COVER SHEET



Health
South Eastern Sydney
Local Health District

NAME OF DOCUMENT	Managing Secure Organisation Access within Cerner EMR
TYPE OF DOCUMENT	Procedure
DOCUMENT NUMBER	SESLHDPR/510
DATE OF PUBLICATION	October 2016
RISK RATING	Medium
LEVEL OF EVIDENCE	National Standard 1
REVIEW DATE	October 2021
FORMER REFERENCE(S)	N/A
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Patricia Bradd SESLHD Health Records Steering Committee
AUTHOR	Lee Speir Clinical Applications Support Manager (SESLHD, ISLHD, SCHN – Randwick)
POSITION RESPONSIBLE FOR THE DOCUMENT <i>including email address</i>	Lee Speir Clinical Applications Support Manager lee.speir@health.nsw.gov.au
KEY TERMS	Cerner eMR, secure organisation, information security, medical record
SUMMARY	This procedure outlines the management of secure organisation access within the Cerner Electronic Medical Record suite of applications.

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY

**This Procedure is intellectual property of South Eastern Sydney Local Health District.
Procedure content cannot be duplicated.**

Feedback about this document can be sent to seslhd-executiveservices@health.nsw.gov.au

SESLHD PROCEDURE

Managing Secure Organisation Access within Cerner eMR

SESLHDPR/510

1. POLICY STATEMENT

To provide a clear procedure outlining the management of secure organisation access (including approval process for secure organisations) within the Cerner Electronic Medical Record (eMR) suite of applications.

2. BACKGROUND

A generic principle of the electronic patient record is to enable access to a record, when access is required for a recognised primary and secondary purpose.

It is acknowledged that some service types require restriction against this principle, and staff within those units will only have access to the service related personal health information. This restricted access is managed through secure organisations within eMR.

3. DEFINITIONS AND ABBREVIATIONS

Confidentiality

The characteristic of data and information being disclosed only to authorised persons, entities and processes with a right to know at authorised times in an authorised manner

eMR

Electronic Medical Record; referring to the Cerner suite of applications.

Primary purpose

The dominant purpose for which personal health information is gathered, usually to provide a health service.

Secondary purpose

Use or disclosure of personal health information outside of the primary purpose for which it was gathered, and as exempted under Health Privacy Principles 10(1) and 11(1).

Service Unit

Service Units are business units within the acute, subacute and community health settings with specific business needs and requirements.

Service Type

Service Types refer to the types of services provided to the clients of the health service. For the purpose of this procedure the relevant service type include:

- Community Health Counselling
- Domestic Violence Counselling
- Sexual Health
- HIV Services
- Sexual Assault
- Child Protection/JIRT/Out of Home Care

SESLHD PROCEDURE

Managing Secure Organisation Access within Cerner eMR

SESLHDPR/510

- Staff Health
- Genetics

Secure Organisation

Secure organisations are facility level locations built within eMR. These locations are secure in the fact that they will not be automatically granted to all eMR users (as occurs within all LHD hospitals), locations will only be granted to the relevant users within the service unit. Information associated with these secure locations is not available to users without access to that organisation.

Based on the service types above, there is a business need to have secure organisations for:

- Illawarra Shoalhaven Child Protection
- South Eastern Sydney Child Protection
- Sydney Children's Hospital Network Child Protection
- South Eastern Sydney Child and Family Counselling
- Illawarra Shoalhaven Child & Family Counselling
- Illawarra Shoalhaven Violence and Neglect
- South Eastern Sydney Violence and Neglect
- South Eastern Sydney LHD HIV & Related Programs (HARP) Services
- Illawarra Shoalhaven Sexual Health
- Albion Street Centre
- Staff health (health screening)
- Southern Sydney Sexual Assault Service
- St George Domestic Violence
- Prince of Wales Hereditary Cancer Care

SWSD

State Wide Service Desk

4. RESPONSIBILITIES

4.1. Service Unit Managers will:

- Ensure staff members have attended eMR training and have account.
- Request access, or removal of access, to applicable secure organisations as required via the State Wide Service Desk (SWSD).

SESLHD PROCEDURE

Managing Secure Organisation Access within Cerner eMR

SESLHDPR/510

4.2. End Users will:

- Abide by the NSW Health Privacy Manual, NSW Health Code of Conduct and relevant SESLHD policies and procedures.
- Attend eMR training.

4.3. Manager Primary and Community Health Information Systems will:

- Ensure access to secure community health related organisations is granted upon authorised request.
- Ensure access to secure community health related organisations is removed in timely manner when notification is received.

4.4. Clinical Application Support Manager will:

- Ensure eMR accounts are created or end-dated in timely manner.
- Ensure audit reports are available for Service Unit Managers.
- Ensure access to secure organisations is granted upon authorised request (non-community health settings).
- Ensure access to secure organisations is removed in timely manner when notification from service unit (non-community health settings) is received.

4.5. SWSD Officers will:

- Receive calls via phone or electronically from Service Unit Managers, triage call and transfer to appropriate eMR support team.

5. PROCEDURE

This procedure is triggered upon:

- Requirement of staff access to secure eMR organisations
- Removal of staff access to secure eMR organisations
- Auditing of staff access against secure eMR organisations
- Request for a new secure organisation.

5.1. Granting or Removing Access to Secure Organisations

- A request to grant/remove access to a secure organisation is made by the Service Unit Manager via the SWSD, SWSD ticket created.
- SWSD staff transfer ticket to appropriate eMR support team.
- The eMR support team email the relevant approvers as per [Approver List](#) to seek:
 - Approval for access to/removal from the secure organisation/team

SESLHD PROCEDURE

Managing Secure Organisation Access within Cerner eMR

SESLHDPR/510

- Approval for access to/removal from the secure organisation/team from the scheduling application.
- The eMR support team provide relevant access via HNA user, including SWSD ticket number, and refer to Scheduling Team to update the relevant scheduling security group.
- SWSD ticket is completed, including written approval attached to ticket, and access granted or removed to appropriate organisation.
- Service Unit Manager is notified.

5.2. Auditing Access to Secure Organisations

- Service Unit Manager runs access audit report for their secure organisation(s).
- Inappropriate access to the organisation (based on report output) is reported to the individual's line manager.
- Access to secure organisation is removed (as per 5.1 above).

5.3. Approval of New Secure Organisations

- Service Unit Manager prepares a brief to request a new secure organisation. The outlines justification (business/clinical requirements) for new secure organisation.
- Brief is forwarded for approval to:
 - LHD Director Primary and Integrated Health (community health organisations)
 - Medical Executive Director (non-community health organisations)
- Following approval as above, the brief is forwarded to the SESLHD Clinical and Quality Council for endorsement.
- If a new secure organisation is approved, the build will be undertaken in eMR; or if not approved, advice is provided back to Service Unit Manager.

6. DOCUMENTATION

- N/A

7. AUDIT

- Bi-monthly audits are completed by Service Unit Managers to ensure appropriate staff access to secure organisations.
- Bi-monthly audit reports are produced and kept by Service Unit Managers, with appropriate action undertaken on any anomalies identified.

8. REFERENCES

- [NSW Health - Privacy Manual for Health Information](#)
- [NSW Health - Code of Conduct PD2015_035](#)
- CHIME – Confidentiality and Information Management PD/119

SESLHD PROCEDURE

Managing Secure Organisation Access within Cerner eMR

SESLHDPR/510

9. REVISION AND APPROVAL HISTORY

Date	Revision No.	Author and Approval
13/06/2015	0.1	Author: Lee Speir, eMR Support Manager (initial draft) Approval: SESLHD Health Records and Medico-Legal Working Group
29/09/2015	0.2	Author: Hayley Ryan (conversion to standard SESLHD template) Approval: SESLHD Health Records and Medico-Legal Working Group
25/11/15	0.3	Reviewed and Approved: SESLHD Health Records and Medicolegal Working Party
05/04/16	0.4	Author: Leonie Patterson and Lee Speir updates to 5.1 and amendments to position titles that have changed since initial draft
	0.5	Reviewed and Approved: SESLHD Health Records Steering Committee
29/09/2016	0.6	Incorporated comments into procedure
October 2016	0.6	Endorsed by DET