Procedure

Document ID: C-PRO 538 V1.0

Access to Patient Integrated Electronic Medical Records (ieMR)

Mackay Hospital and Health Service

1. Purpose

This Procedure describes what is deemed as appropriate access of a patient's electronic medical record (ieMR).

This Procedure also describes the process to follow when there is suspicion that a patient's ieMR has been inappropriately accessed.

Examples of inappropriate access to ieMR include access to a staff member's personal information and/or that of their family, friends/acquaintances, other staff members and any other individual for which the staff member has no legitimate and lawful reason to access the information, and where inadvertent access has occurred.

2. Scope

This Procedure applies to all MHHS employees (permanent, temporary and casual) and all organisations and individuals acting as its agents (including agency nurses, Visiting Medical Officers and other partners, contractors, consultants and volunteers).

3. Procedure including roles and responsibilities

3.1 Appropriate access

We trust that our employees only access information that is within the scope of their official duties.

In order to access a patient's ieMR, training must be completed in the use and navigation of the ieMR. This training may be in person or web based. Once training has been completed the relevant access can be requested using the Online IT Support. This request must be authorised by the staff member's line manager.

Appropriate access of a patient's ieMR is:

- Clinical documentation and access to ensure continuity of care
- Health Information Management
- Scheduling of patient activities
- Auditing purposes including investigations, audits, Riskman incidents, complaints management and approved teaching and research activities.

Under no circumstances are any staff to use any of Queensland Health's clinical information systems to view their own medical records or the medical records of friends, family or any other patients to which they are not responsible for providing care and treatment. Staff can only access patient records relating to their current workload and that they have a genuine work related need to access.

3.2 Training

All staff are advised of the governance surrounding confidentiality during staff orientation. Clinical staff also receive training about patient confidentiality through their professional education and induction. The privacy of patient information is also discussed during other training sessions, such as ieMR training. All staff are required to complete training in the use of the ieMR before access is granted.

Additional training can be provided by contacting the line manager.

3.3 Conflict of Interest

Access to a staff member's own record or that of family members is not permitted. If a staff member requires access to their own or a family member's confidential health record then an application can be made through the Information Access Unit. This application can be applied for in person with proof of ID at the reception desk located Level 0, A Block, Mackay Base Hospital or by applying online or by post.

Where it could be deemed that there is a conflict of interest for a staff member to access a particular patient's ieMR to perform their duties, the staff member should make alternative arrangements and/or request another staff member to undertake the task.

Potential conflicts of interest would include the staff member's own record, a family member, a friend's record or that of a fellow staff member.

If staff members are concerned about any potential or actual conflicts of interest they should discuss the matter with their line manager.

3.4 Routine Reporting of Suspected Inappropriate Access to ieMR

As part of our assurance processes, audits of access to medical records are scheduled to run each month and are also undertaken on an ad hoc basis. These reports are used to identify potential access to information breaches within the ieMR system.

Where matches are identified by the Health Information Manager (HIM), they will review and report potential breaches to Human Resources.

The delegate will determine the appropriate course of action depending on the number of breaches and the type of record viewed.

3.5 Procedure for Reporting Suspected Inappropriate Access to ieMR

3.5.1 Reporting by a Staff Member

Where a staff member suspects that another staff member may have inappropriately accessed the ieMR of a patient, their own or a family member's record or that of another staff member, they must immediately report this suspicion to their Line Manager. The Line Manager should liaise with Human Resources regarding appropriate methods of dealing with potential breaches of information privacy.

3.5.2 Inadvertent Access

Where a staff member accidently accesses a record for a family member, staff member or other they should advise their line manager of the patient and date of access who will then record details in the accidental access register maintained by Health Information Manager. Any inadvertent access must be reported immediately to the HIM via the Line Manager.

3.5.3 Reporting by a Patient/Client of the HHS

Where a patient/client expresses concern to a staff member regarding inappropriate access to their medical record, the staff member should immediately notify their Line Manager of the unit in which the issue was considered to occur.

In both circumstances, the Line Manager should liaise with the HIM and the Consumer Liaison Officer. The HIM will then liaise with Human Resources regarding appropriate methods of dealing with potential breaches of information privacy.

3.6 Information Required When Reporting a Suspected Breach

- Unit Record Number (URN), Name and Date of Birth (DOB) of the ieMR record that is suspected of being accessed inappropriately.
- Name of the staff member suspected to have inappropriately accessed a record.
- Reason for suspicion of potential breach.
- Approximate date of potential breach.
- Name of person reporting the suspected breach.

3.7 Contact Details for Reporting Suspected Inappropriate Access

- Human Resources Mackay
  Email: Mackay_HR_Services@health.qld.gov.au
  Phone: 07 4885 6809
- Line Manager
- Manager Health Information Services – 07 4885 7373
- Consumer Liaison Officer – 07 4885 7690

3.8 Procedure for Health Information Manager

Where a breach is reported, the Health Information Manager will provide a report to Human Resources on the specific patient record, identifying all staff members that have accessed the patient's ieMR.

The staff member will be provided the opportunity to respond to the potential breach and will be provided with the URN of the patient, date, time and access evidence.

The Human Resources Department will establish with the HIM whether a breach of this policy has occurred.

3.9 Potential Disciplinary Actions

If after investigation a staff member has been determined to have inappropriately accessed an ieMR causing a privacy breach, disciplinary action may be taken. This will be determined on a case-by-case basis but may include the following actions:

- Line Manager and Human Resources to report breach to staff member's Executive Director.
- Formal written warning to staff member.
- Performance Management Processes.
- Suspension.
- Organisational and/or personal (monetary) fine.

- Termination.
- Referral on to the Crime and Corruption Commission or the Office of the Health Ombudsman.

4. Supporting documents

4.1 Authorising policy and standard/s

- Crime and Corruption Act 2001
- Code of Conduct for Queensland Public Service
- Information Privacy Act 2009 (Qld)
- Right to Information Act 2009 (Qld)
- Hospital and Health Boards Act 2011

4.2 Procedures, guidelines and protocols

- QH Information Security Policy (QH-POL-066:2014)
- QH Data Management Policy (QH-POL-279:204)
- Queensland Department of Health Use of Information Communication and Technology (ICT) Services Policy (QH-POL-032:2015)
- Requirements for Reporting Corrupt Conduct HR Policy E9 (QH-POL- 218:2018)
- Workplace Conduct and Ethics Policy E1 (QH-POL-113:2018)
- Confidentiality General Principles, Hospital & Health Boards Act 2011, September 2017

5. References and suggested reading

- CHHHS Privacy and Confidentiality of Patient Integrated Electronic Medical Records (ieMR) Procedure 2017

6. Definition of terms

Term	Definition	Source
Integrated electronic medical record (ieMR)	Cerner Powerchart is an integrated electronic Medical Record system that changes the way clinicians' access patient information, replacing the paper based system with a secure electronic record. Patient information at Mackay Hospital is stored electronically in Powerchart.	ieMR Program Webpage on QHEPS
Corrupt Conduct	Corrupt Conduct is any conduct connected with the performance of an employee's duties that is dishonest or lacks impartiality, involves a breach of trust or is a misuse of officially obtained information or material, provides a benefit	Requirements for Reporting Corrupt Conduct Policy -on QHEPS

	to a person or a detriment to another person and which if proven is a criminal offence or conduct serious enough to justify dismissal.	
Crime and Corruption Commission (CCC)	The CCC is a statutory body set up to combat and reduce the incidence of crime and corruption in the public sector	Website: www.ccc.qld.gov.au
Office of the Health Ombudsman (OHO)	The OHO is Queensland's independent health complaints agency. It was established as a statutory authority under the Health Ombudsman Act 2013 and is required by law to act independently, impartially and in the public interest.	Website: www.oho.qld.gov.au

7. Consultation

Key stakeholders (*position and business area*) who developed/reviewed this version are:

- Manager, Health Information Services
- Senior Health Information Manager
- Executive Directors
- Manager Human Resources

8. Procedure revision and approval history

Date	Created/Modified	Authorised by
09/2018	Manager Human Resources	Executive Director, HR & Engagement
10/2018	Manager, Health Information Services	Executive Director, HR & Engagement
11/2018	Executive Leadership Team	Chief Executive

9. Audit Strategy

Level of risk	Medium (9)
Audit strategy	Monthly P2Sentinel reports
Audit tool attached	N/A
Audit date	Monthly
Audit responsibility	Manager Human Resources
Key elements/ indicators/outcomes	Number of incidents reported

10. Approval and implementation

Custodian/review officer	Executive Director, HR & Engagement
Version no.	V1.0
Applicable to	All MHHS Staff
Approval date	13/11/2018
Effective from	14/11/2018
Next review date	13/11/2021
Supersedes	New Document
Marketing strategy	Direct briefings, E-Connect, Screensaver, CE Email, Health Chat, Posters displayed in key areas.
Keywords	Access, ieMR
Accreditation references *NSQHS, EQuIP and other criteria and standards*	

11. Approved by

Signatory	Position	Signature	Date
Rebecca Wells	A/Executive Director HR & Engagement	The signed version is held and retained by MBH File Clerk	13/11/2018