Restricting Access to Electronic Clinical Records

Lead executive	Medical Director
Authors details	Trust Records & Information Governance Manager 01244 397384

Type of document	Standard Operating Procedure
Target audience	All CWP staff
Document purpose	To set out the procedure for restricting access to electronic clinical records e.g. in the event of investigation of a death, safeguarding, protect evidence for crime investigation, patient is member of staff or a celebrity.

Approving meeting	Information Governance & Data Protection Sub-Committee	Date 16-Mar-20
Implementation date	16-Mar-20	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
IM7	Confidentiality policy
CP3	Health Records Policy

Document change history	
What is different?	Policy recoded in line with policy library reshape
Appendices / electronic forms	N/A
What is the impact of change?	N/A

Training requirements	Yes - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of the Information Governance & Data Protection Sub-Committee
Corporate services	Corporate representatives of the Information Governance & Data Protection Sub-Committee
External agencies	N/A

Financial resource implications	None

External references

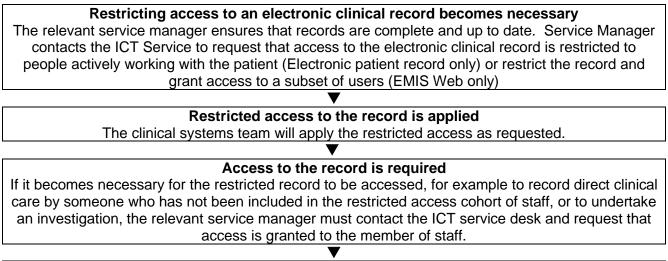| **Equality Impact Assessment (EIA) - Initial assessment**	**Yes/No**	**Comments**

Equality Impact Assessment (EIA) - Initial assessment	Yes/No	Comments
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable? N/A		
Is the impact of the document likely to be negative?	No	
- If so can the impact be avoided?	N/A	
- What alternatives are there to achieving the document without the impact?	N/A	
- Can we reduce the impact by taking different action?	N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	N/A	
What is the level of impact?	N/A	

Content

Quick reference flowchart for restricting access to electronic clinical records

For quick reference the guide below is a summary of actions required.

Restricting access to an electronic clinical record becomes necessary
The relevant service manager ensures that records are complete and up to date. Service Manager contacts the ICT Service to request that access to the electronic clinical record is restricted to people actively working with the patient (Electronic patient record only) or restrict the record and grant access to a subset of users (EMIS Web only)

▼

Restricted access to the record is applied
The clinical systems team will apply the restricted access as requested.

▼

Access to the record is required
If it becomes necessary for the restricted record to be accessed, for example to record direct clinical care by someone who has not been included in the restricted access cohort of staff, or to undertake an investigation, the relevant service manager must contact the ICT service desk and request that access is granted to the member of staff.

▼

Restriction no longer necessary
If the restriction no longer needs to be applied to a record for example, an investigation is complete or the circumstances have changed, the relevant service manager contacts the ICT service desk and request that the restriction is terminated.

1.   Introduction

All patients' details are stored in the Trust's secure electronic patient records systems, the two primary clinical systems are Carenotes and EMISWeb. All staff accessing patient records in Clinical Systems are bound by the Trusts policies on confidentiality, security and information governance. Exceptionally, there may be patient records which need additional safeguards. Examples of reasons why this may be required include:

- Victims of crime where the alleged perpetrator works within the organisation.
- A family member works within the organisation.
- The patient is a current or previous member of staff or student.
- The patient is under a witness protection scheme.
- The patient is a celebrity.
- To protect evidence when a patient is being investigated by the police or another law enforcement agency.
- Following a request from a Safeguarding Board.

Whilst there are benefits for restricting access to records there are also risks associated with restricting access to records as information may not be accessible when needed. Consideration should be given as to how the record can be restricted, who should authorise the restricting of the record, the duration of the restriction and who should be allowed access to the record whilst it is restricted.

2.   Possible restrictions

Additional auditing and monitoring
No restrictions put in place but Care –coordinator or Team manager takes responsibility for checking who has accessed the record on a monthly /weekly basis. This can be done by any Electronic patient record user or by the Clinical Systems team for EMIS Web.

Restrict access to people actively working with this patient. CARENOTES ONLY
The clinical systems team can restrict access to the record, to allow only members of staff who are recorded as a Team member (Care Coordinator, Primary Worker, Secondary Worker, Consultant etc) access. Other Electronic patient record users will be able to see the patients name, date of birth, postcode and NHS Number from the search screen but will not be able to proceed into the record.

Restrict record and grant access to a subset of users.   EMIS WEB ONLY
The clinical systems team can restrict access to the record, to allow only members of staff with enhanced access levels to access the patient record. Any staff that has a legitimate reason for accessing the record would need their access level increasing. *Please note: In EMISWeb it is not possible to give access to only one restricted record, members of staff with access to restricted records could access all restricted records.* Other users will not be able to find the patients record.

3.   Procedure

3.1   Restricting access to an electronic clinical record becomes necessary

The relevant service manager must ensure that records are complete and up to date. The relevant service manager will contact the ICT Service and request that access to the electronic clinical record is restricted to people actively working with the patient (CareNotes only) or restrict the record and grant access to a subset of users (EMIS Web only)

3.2   Restricted access to the record is applied

The clinical systems team will apply the restricted access as requested.

3.3   Access to the record is required

If it becomes necessary for the restricted record to be accessed, for example to record direct clinical care by someone who has not been included in the restricted access cohort of staff, or to undertake an investigation, the relevant service manager must contact the ICT service desk and request that access is granted to the member of staff.

3.4   Restriction no longer necessary

If the restriction no longer needs to be applied to a record for example, an investigation is complete or the circumstances have changed, the relevant service manager must contact the ICT service desk and request that the restriction is terminated.

4.   Training
- Raising awareness to fully implement the procedure.
- To publish on the Intranet and communicate via the e-bulletin.

5.   Monitoring

For this procedure:
- All staff are aware of relevant procedural documents e.g. Confidentiality Policy, health records policy etc..
- Untoward incidents resulting from the restricted access to electronic clinical records will be logged on DATIX and reported to the Information Governance Team (including the Caldicott Guardian) who will support further investigation in accordance with the Confidentiality Policy (IM7)

6.   Duties and Responsibilities

6.1   Chief Executive

The Chief Executive will assume overall accountability for ensuring that records issues are effectively addressed within the Trust.

6.2 Trust Board

The responsibility for the provision of a procedure for restricting access to electronic health records rests initially with the Trust Board and is delegated to the Information Governance Team. Additionally, the Trust Board will ensure through the line management structures that this policy is applied and that staff are aware of the restricting access to electronic records procedure.

6.3 Clinical Systems Team/ICT Service Support

The ICT service desk will log all requests for restricting access to electronic clinical records and the clinical systems team will action the request.

6.4 Information Governance/Health Records Team

Information Governance and Health Records Teams will provide guidance to support managers in deciding which type of restriction to electronic clinical records will be appropriate.

6.5 Service Manager's Responsibilities

Service managers must ensure that all information which needs to be added to the record is complete prior to requesting that the record is restricted. The manager must then contact the service desk to request the appropriate restricted access. The manager must also contact the ICT service desk to request access is granted to an employee e.g. to record direct clinical care or to undertake an investigation.

6.6 Employee's Responsibilities

Employees should ensure that they undertake annual mandatory information governance training and only access electronic clinical records on a need to know basis. If a record which is accessed has been restricted, the service manager must contact the ICT service desk to request that access is granted and the reason for the access e.g. to record direct clinical care or to undertake an investigation.