Joint Research Management Office Standard Operating Procedure for:			
External Access to Patient Electronic Health Records			
SOP Number:	**16b**	Version Number:	**2.0**
Effective Date:	**4th September 2023**	Review Date:	**4th September 2026**

Authorship:		**Signature and Date:**
Author:	Marie-Claire Good Senior GCP and Governance Manager	Marie-Claire Good Digitally signed by Marie-Claire Good Date: 2023.08.15 15:27:38 +01'00'

This SOP has been revied by Andrew Vince, Barts Health Head of People Systems and Insight, Sarah Palmer-Edwards, Queen Mary Head of Information Governance, Laura Vosper, CECM QA Manager, Raine Astin-Chamberlain ,Barts Health Senior ED Research Nurse and Nicolene Plaatjies, Barts Health Senior Paediatric Research Nurse.

Authorisation:		**Signature & Date:**
Name/Position:	Mays Jawad Research Governance Operations Manager	Dr Mays Jawad Digitally signed by Dr Mays Jawad Date: 2023.08.16 10:01:41 +01'00'

Background:

Access to Electronic Health Records (eHR) is a requirement of study monitoring, audit, and regulatory inspections.

The Barts Health NHS Trust (Barts Health) Enterprise Patient eHR system is Cerner Millennium, with the eHR component being PowerChart. The Barts Health strategy is to use Millennium as the primary system source of truth for all clinical work, research, audit, and billing. Third parties would require access to Millennium including PowerChart as defined by Good Clinical Practice (GCP) Direct Access.

It is Barts Health policy that all third parties requiring access to Barts Health systems and data will comply with the Barts Health Information Governance (IG) and confidentiality policies and with the Barts Health Confidentiality Agreement for third party contractors.

All third parties that require access to Barts Health information systems must comply with the NHS Confidentiality Code of Practice and the NHS Care Record Guarantee, as well as statutory requirements such as the General Data Protection Regulation.

Any third party found to have violated these codes may be subject to sanctions, up to and including termination of the contract and removal of access rights.

Purpose:

This document is intended to reduce the risk to Barts Health assets and data by ensuring that external study monitors, auditors and regulatory bodies are aware of the correct procedures for accessing Barts Health systems and data. Furthermore, this document clarifies the process for ensuring that access to Cerner Millennium by external monitors is internally reviewed and controlled using organisational security measures.

Scope:

Any external organisation wishing to access any Barts Health eHR including but not limited to Millennium, for the purpose of verifying source data collected as part of a clinical study. This includes monitors, auditors, and regulatory inspectors.

Abbreviations:	
Barts Health	Barts Health NHS Trust
CRO	Clinical Research Organisations
eHR	Electronic Health Record
GCP	Good Clinical Practice
IG	Information Governance
JRMO	Joint Research Management Office
RA	Registration Authority
SOP	Standard Operating Procedure
TAC	Temporary Access Card

SOP Text:		
	Responsibility	**Activity**
1.	Study team/department	**Ensure points 3 to 11 are followed to set up and prepare for external organisations requesting access to Millennium and liaise with other eHR system owners to arrange access.** Ensure suitable facilities and equipment are available for external Monitors /Auditors /Inspector if needed. Departments should consider which other Barts Health wide or bespoke eHR systems they utilise as source data.
2.	Study team with sponsor/ Clinical Research Organisations (CRO)	**During feasibility/set up stage, ensure a clear source data list of agreement is put in place.** This agreement or list (see *SOP 45 Study Specific Essential File Documentation* for templates) should clearly identify which eHR systems will be in use from individual studies. Discuss the need for access with the study team/Sponsor/CRO. The sponsor retains responsibility for the conduct of the study monitors, auditors, or inspectors during the site visits. For monitoring this is as defined in the Clinical Trials Agreement.
External access to Barts Health millennium		
3.	Department Research lead	**Appoint a Temporary Access Card (TAC) guardian**
4.	TAC guardian	**A TAC guardian should be:** • A Barts Health employee. • They must be a full time and substantially employed. • The holder of a smartcard. • A trained CRS user.
5.	TAC Guardian	**Set up Millennium access TAC system and processes.**

		The TAC guardian must read and sign the authorisation form (*Associated Document 1 TAC Authorisation Form*) and send it back to the Registration Authority (RA) department (regauthority.bartshealth@nhs.net) The TAC guardian is responsible for implementation, maintenance of the TAC log (*Associated document 2*) and respond to the monthly audits performed by Barts Health RA. The TAC guardian should provide any support to the monitors/inspectors during their visit.
6.	All	**Any breaches should be reported immediately to Barts Health IG, Joint Research Management Office (JRMO), RA and appropriate Sponsors/CROs.** This report can be by email. Additionally, please submit a Datix incident report as appropriate.
7.	TAC guardian or delegate	**New users must complete basic induction with departmental TAC Guardian during their first visit to the site.** In exceptional circumstances (e.g. illness and short notice leave) this can be delegated to an appropriate member of the study team; any delegation should be made clear on the TAC Log (*Associated document 2*) The induction should: • Provide generic log-in details to user. • Flag Barts Health IG policy: https://weshare.bartshealth.nhs.uk/trust-wide-policies (search IG). *For all users with exception of regulatory inspectors obtain written confirmation this has been read.* • Ensure that users have access to Barts Health millennium e-learning: https://weshare.bartshealth.nhs.uk/millennium-learning. • Ensure the study team or appropriate delegate has provided users with basic navigation of the system. • Highlight the importance of locking computers when not in use.
8.	TAC guardian and / or Study team	**For monitoring and audits** **Before any monitoring activity:** • The study team must book the monitoring visit with the TAC guardian. • The study team must provide a basic introduction to Barts Health and Millenium. • A copy should be provided to the external organisation. The original must remain with the TAC guardian. • TAC guardian must complete the TAC Log sheet (*Associated document 2*) at the start and end of each monitoring visit. • Only external users who have an institution level agreement in place, have signed the 3rd party confidentiality agreement and have signed the TAC log sheet can be given access to the system. Access is given by the TAC guardian or delegate who logs into the Barts Health computer and then the user accesses the system using their TAC. **Before any Inspectorate activity**: • Identify and inform the appropriate TAC guardian of planned visit.

		• TAC guardian must complete TAC Log sheet *(Associated document 2*) at the start and end of each visit. **During visit:** • The TAC guardian is expected to keep a log of TAC usage using the TAC Usage Log form (*Associated Document 3*). • Research team/TAC guardian opens the list of patient records as agreed for the visit. If no list is available, Medical Record Number numbers can be used to search for patient records. This should be clearly demonstrated to avoid accidental viewing of non-study participants. • TAC guardian should be available during monitor visits to assist monitors as required. • Users must always lock computers when not in use. • Users to inform departmental research team member/TAC Guardian when monitoring visit is complete and completes TAC log with time of completion. • All visits must end when the TAC guardian or delegate leaves.
9.	TAC guardian	**Ensure ongoing oversight with Barts Health RA and JRMO.** When contacted by Barts Health RA, confirm in a timely manner that they are still in possession of TACs issued to them. This occurs on a monthly basis. Lack of response is escalated by the RA to the Research Governance Operations Manager in the JRMO.
10.	RA	**The RA will review the audit trail of patient access for the assigned TAC and will liaise with the TAC guardian to confirm only appropriate access to specific patient records were undertaken.** Any discrepancies should be raised with the RA and Research Governance Operations.
11.	Research Governance Operations Manager	**If any access abnormality is raised, working with RA, the TAC guardian and IG must establish full review.** Escalation to the Research Governance Operations Manager is the first instance, then user employee/sponsor as applicable.
12.	Barts Health RA	**At initial set up TACs will not be issued until the TAC Authorisation form is received by the RA department.** Barts Health RA invoice the JRMO for the costs as agreed. A maximum of 2 temporary smartcards will be issued per department or TAC guardian. Each TAC will have a read only position role (R1H View Only). A log of TAC guardians and associated cards will be available on request. A confirmation sheet will be sent to the guardian at the required time. Upon setup of a new TAC guardian, audit trails from smartcard access (establishing which patients where accessed by which card at which time point) should be created a sent to TAC guardian and JRMO representative monthly. If there is a lack of response this is escalated to the Research Governance Operations Manager.

Change control

Section changed	Summary and description of change
Definitions	Removal of definitions section
Relevant SOPs	Removal of section in place of hyperlinks.
Associated Document	Removal of Associated Document 4 in place of direct link to the Barts Health 3rd party confidentiality agreement

List of appendices

There are no appendices associated with this SOP

List of associated documents

Document ref.	Document name
Associated Document 1	TAC Guardian Authorisation Form
Associated Document 2	TAC log form
Associated Document 3	TAC usage log

EDGE Update

There is no EDGE update required