STANDARD OPERATING PROCEDURE (SOP)

SOP Number: NCP/R&D_011

SOP Title: Clinical Record Interactive Search Procedure

Role	Name	Signature	Date
SOP Author	Tanya Smart – CRIS Project Manager		21/10/16
SOP Reviewer	Dr. Peter Phiri – R&D Manager		21/10/16
SOP Authoriser	Dr. Shanaya Rathod – R&D Director		21/10/16
SOP Review Date			

Review History

Version	Effective Date	Review Undertaken/Significant Changes	Date Approved
1	13-Oct-2016	Initial Version	

STANDARD OPERATING PROCEDURE (SOP)

SOP Number: R&D 011

SOP Title: ***Clinical Record Interactive Search Procedure***

1. Purpose and Context

1.1. The purpose of this document is to describe the procedures and methods that will be used by Southern Health NHS Foundation Trust (SHFT) Clinical Record Interactive Search (CRIS) team to ensure that CRIS searches are conducted in accordance with the UK-CRIS Standard Operating Procedures and Security Model.

1.2. Clinical Record Interactive Search (CRIS) system allows authorised staff with regulated access to compare and search an extensive amount of pseudonymised clinical data, linked to the OpenRiO patient record for audit, service evaluation and research purposes. It is a tool that identifies relevant records based on search terms (e.g., a particular diagnosis and/or a particular word or phrase in a clinical assessment or event). The researcher/clinician defines relevant patient groups by searching against any combination of structured fields (date, numerical, etc.) and unstructured fields (user-defined text strings) from clinical data sources.

1.3. In accordance with the approved UK-CRIS Standard Operating Procedures and Security Model and Terms of Reference, the CRIS Monitoring Group is responsible for overseeing and monitoring the use of CRIS within SHFT and will include representation from patients. The CRIS Monitoring Group is comprised of key Trust roles (e.g. Caldicott Guardian Representative, Information Governance, Director of Research, etc.). The Monitoring Group will ensure relevant stakeholders, including Trust patients and staff, are able to access relevant information about CRIS, including the right to opt-out.

1.4. The CRIS Administrator acts on behalf of the Monitoring Group on a day-to-day basis, including managing CRIS applications, users' accounts and access to audit logs, and Monitoring Group meetings.

1.5. This document is to ensure that:

- Access to the CRIS application is by SHFT approved/regulated staff.
- The CRIS search is conducted in accordance with the approved CRIS application and will compare intended use specified in initial applications with actual use recorded in audit log
- Reverse searches are being conducted in accordance with the UK-CRIS Standard Operating Procedures and Security Model.

2. Definitions

2.1. SOP Author - Any person who is familiar with the activity covered by the SOP and who is competent to carry it out.

2.2. SOP Reviewer – A person who is appropriately qualified or experienced to review the procedure covered by the SOP

2.3. CRIS – Clinical Record Interactive Search

2.4. NIHR- National Institute of Health Research

3. Infrastructure

3.1. Security of data on the hosted environment is of paramount importance and a supplier of an infrastructure service was selected by the Sponsor, Oxford University, on this basis following an extensive procurement exercise. The physical datacentre which the Trust instance of CRIS is hosted on is provided by Equinix.

3.2. The reader is directed to the UK-CRIS Standard Operating Procedures and Security Model for further information about the security credentials of the hosted service and the process by which data is transferred.

3.3. The providers of the service and support escalation processes are also outlined in the UK-CRIS Standard Operating Procedures and Security Model.

3.4. The Information Asset Owner for CRIS is the Director of Research and Development (R&D) and the Information Asset Administrator is the R&D Manager.

3.5. The Grant fund for CRIS implementation was provided by Dementia Platform UK Programme and coordinated by Oxford University in partnership with SHFT.

3.6. Post implementation, the Trust will remain responsible for CRIS with the R&D department managing the daily CRIS project.

3.7. The R&D Business Impact Analysis outlines the business continuity procedures for the department and the impact on the continuation of the department if CRIS was unavailable.

3.8. Detailed Data/Service Backup and Disaster Recover Procedures for CRIS are provided in the UK-CRIS Standard Operating Procedure and Security Model.

3.9. All actual or suspected breaches of security regarding CRIS are to be reported to the CRIS Administrator, who reports all incidents to the Information Governance Manager and Caldicott Guardian (see section 6 and Appendix 1 – Flow Chart for Potential PI breach) In addition, all CRIS incidents involving Trust data will have an Ulysses incident raised.

4. Monitoring Group

4.1. The CRIS Monitoring Group is responsible for overseeing and monitoring the use of CRIS and will include representation from patients and key Trust roles (e.g., Caldicott Guardian Representative, Information Governance, Director of Research, etc.).

4.2. The Group's responsibilities will include:

4.3. **Managing the CRIS application process:** All projects proposing to use CRIS

are required to submit a written application to the SHFT CRIS Monitoring Group using the standardised questionnaires (see Section 5). Applications are judged according to:

- Underlying value and potential benefits of the project (e.g., to inform patient care).
- Appropriate supervision/governance. For example: research governance for research projects; formal clinical governance approval for audits; Trust director sign-off for service evaluation.
- Inadvertent risk of patient identification. For example, the likelihood of particularly small cohort/cell sizes (< 10 cases); appearance of high profile publically known/published information, etc. In these cases additional measures may be put in place to safeguard confidentiality.
- The need to support service evaluation. Note: applications to use CRIS to evaluate or monitor staff-level performance will usually not be granted. Applications to use staff names for legitimate research/audit purposes may be granted, but additional supervision may be put in place.

4.4. **Monitoring the use of CRIS:** For example, comparing intended and actual use of CRIS through routine monitoring of the audit trail.

4.5. **Managing the UK-CRIS Standard Operating Procedures and Security Model:** Ensuring the model is fully implemented at all times and updated as required to meet new standards or changes.

4.6. **Managing the CRIS Communications Plan:** Ensuring relevant stakeholders, including Trust patients and staff, are able to access relevant information about CRIS, including the right to opt-out.

4.7. **Appointing and supporting the SHFT CRIS System Administrator(s):** This role will act on behalf of the Monitoring Group on a day-to-day basis, including managing CRIS applications, users' accounts and access to audit logs, Group meetings, etc.

5. Application Process

5.1. Access to the CRIS data repositories requires formal authentication methods (currently username and password). Only individuals authorised by SHFT will have permitted access. This will include staff authorised to undertake maintenance and data processing activities, as well as staff undertaking approved searches of the data.

5.2. All searches are to be in agreement with the approved CRIS application.

5.3. All application enquiries are directed to the CRIS Administrator. Following initial discussions, the relevant CRIS application form is sent to the CRIS researcher. These are located in *S:\ResearchandDevelopment\CRIS Confidential* under *CRIS Application Form.*

5.4. All CRIS searches require application approval:

- Feasibility for clinical trial
- Research study
- Service Evaluation

- Trust Clinical Audit question

5.5. If the CRIS researcher is not already a Trust member of staff, the type of contract the researcher holds needs to be established in accordance with the NIHR guidelines to confirm that the researcher is authorised to conduct a CRIS search under Trust Approval. A CRIS specific letter of access is then issued if required. http://www.nihr.ac.uk/policy-and-standards/research-passports.htm

5.6. The CRIS researcher and project details are added to the **CRIS Studies and Users** file located in *S:\ResearchandDevelopment\CRIS Confidential*

5.7. All completed CRIS applications forms are sent to the Monitoring Group for approval. The researcher/clinician is informed of the approval outcome.

5.8. A '**CRIS Project Decision Document'** located in *S:\ResearchandDevelopment\CRIS Confidential* is completed and sent to the researcher/clinician.

5.9. CRIS Account Creation

- A CRIS User is created on the Active Directory within the CRIS Shared Drive. The instructions for this are located in file named '**CRIS_UserManagement_Southern**' on the *S:\ResearchandDevelopment\CRIS Confidential.*
- All user accounts are the same however the CRIS Administrator holds extra permissions which includes the ability to conduct reverse searches (Type 2 use of CRIS) and create users etc.
- The CRIS Adminstrator authorises all user creations and can determine and determine the timescale of a users log-in as specificed in the CRIS application process to the Monitoring Group.

5.10. The CRIS Administrator is responsible in ensuring that CRIS user accounts are disabled/deleted following the completion of a researchers CRIS activity or at the end of the predetermined timescale of a user application to use CRIS.

6. Location of Potential Personal Identifiable Data

6.1. All personal identifiable information is removed from CRIS data repositories entirely, including references in text and dedicated personal identifiable information fields, or sufficiently truncated/modified to protect confidentiality. For example: Date of birth: truncated to month and year of birth only.

6.2. A unique CRIS local ID number, known as the BRC ID, is created for all records for each CRIS installation. The BRC ID is linked to the local source system ID. The linkage table is then separated from the searchable CRIS data repositories and so unavailable to CRIS users.

6.3. However a researcher may locate what they consider to be potential identifiable data when conducting a CRIS search. Potential identifiable (PI) data may be subsequently considered a breach and the following process should be followed.

6.4. **What constitutes a potential breach?**

Potential breaches are where data is missing from a set Patient Identifiable (PI) field in the original data source or there is a typographical error. Therefore information contained within a free text field could potentially be considered identifiable. 'Potential' here implies that the source PI might be guessed or inferred.

6.5. **What constitutes a full breach?**

Breach of the algorithm - PI data that is displaying in CRIS is also located within a masked field within the original data source and therefore should have been masked.

6.6. Upon a researcher highlighting potential PI in a CRIS record, the *'Yellow Flag'* from should be raised with the CRIS Coordinator who will investigate this.

6.7. Reverse searches and 'Yellow Flag' queries are logged in *S:\ResearchandDevelopment\CRIS Confidential*

6.8. The CRIS Coordinator will do a reverse search on the BRCID to identify the patient ID and then search the original data sources for the relevant field which appears to be displaying PI against the patient ID.

6.9. The outcome of the reverse search will determine the level of the breach and in accordance with Appendix 1 – Flow Chart for Potential PI breach should be followed.

7. Auditing of CRIS

7.1. The CRIS Administrator is responsible for the auditing of CRIS searches. This ensures that CRIS searches are conducted in accordance with the approved CRIS application.

7.2. All CRIS searches (research, audit or service evaluations) approved by the SHFT CRIS Monitoring Group will be audited.

7.3. The CRIS Monitoring Group is responsible for the overseeing and monitoring the use of CRIS. The Group will compare the intended and actual use of CRIS through routine monitoring of the audit trail.

7.4. The audit report will be completed for each Monitoring Group by the CRIS Administrator, estimated to meet monthly, on all CRIS usage. This will be reviewed and amended accordingly as the use of CRIS expands within the Trust.

7.5. Users may be asked to report to the Monitoring Group at any point during or at the end of their project's lifespan. Permission to use CRIS for a particular project may be withdrawn, with justification, by the Group at any point.

7.6. Any significant security breaches identified, e.g. breaches of policy or unauthorised searching, will be dealt with according to disciplinary procedures in line with Trust policy and will follow accepted research governance practices.

7.7. The audit data will be available in line with Trust Record Keeping Procedures.

7.8. CRIS will log details of all searches carried out, including:

- login, logout date/ timestamp
- search instance details:
- user name, date timestamp
- chosen search parameters and search parameter values
- chosen result dataset outcome variables
- export instance details:
- user name, date timestamp
- name and folder location of results dataset file exported
- truncation of the Audit Trail by the Systems Administrator, date timestamp.
- results from alert search sent to user.
- alert details
- recruitment email sent

7.9. Audits of CRIS are located in the 'Search Audit Trail' of the CRIS front end. Searches can be performed on:

- Username: (CRIS user)
- Event Type: (User Created, Basic Search, Reverse Search BRCIDs, Search Results Exported and Basic Search Total Hits)
- Return audits before: (date)

7.10. Searches will be verified through the CRIS application and the '**Criteria and objective fields**' file which summarises the search criteria and output fields.

7.11. All audit searches details will be added to the '**CRIS audit log**' file located in *S:\ResearchandDevelopment\CRIS Confidential\Audit of CRIS*

8. Training

8.1. The CRIS Administrator must read and sign off this SOP as part of staff induction. All training must be documented as per Trust policy.

9. Supporting Materials and Attachments

9.1. Appendix 1 – Flow Chart for Potential PI breach