NHS
South London and Maudsley
NHS Foundation Trust

Biomedical Research Centre

Clinical Record Interactive Search (CRIS)

Operational Security model

Development and change log:

Date	Version	Presented to	Outcome/changes made
15/9/08	Draft	CRIS Project board	Approved
8/10/08	Draft	Trust Executive	Approved
14/11/08	Approved	Oversight and Advisory Committee	1.1 – exemptions to the model noted Table 3.3.1 – reference to data sticks added.
6/11/09	Approved	CRIS Oversight Committee	Modifications made to reflect technical changes associated with PJS SQL move; Update of proposed recruitment model following application to NIGGB
1/07/10	Approved	CRIS Oversight Committee	Modifications following technical upgrades and enhancements
1/02/11	Approved	CRIS Oversight Committee	Addition of C4C model – appendix G
25/11/13	Approved	CRIS Oversight Committee	Redrafted. Iaptus and Email for recruitment functionality added
30/05/18	Approved	CRIS Oversight Committee	Include technology refresh phase I & GDPR
27/05/21	Approved	CRIS Oversight Committee	National opt out added – table 1.vi. IG training requirement - table 2,iia Approval to use for quality improvement purposes – 2.2 and table 2.i Clinical text management - table 2, ix, appendix E Oversight Committee ToR – appendix D
05/05/23	Approved	CRIS Oversight Committee	Appendix C section 1.2 – reference to anonymised data removed Appendix D

			section 2, project approvals – minimum requirements (quorum) for approval decisions section 2, project approvals – recusal conditions section 2, CRIS Security Model – frequency of routine reviews of ToRs and the CSM section 4.1, committee membership – membership of the committee need not be limited to the given list section 4.1, committee membership – removal of requirement for IAPT representative section 4.2 – quorum for decision making

1. Introduction

1.1 The SLaM Biomedical Research Centre (BRC) electronic Case Register (CRIS) represents a ground-breaking opportunity to further translational research in mental health. This document details the technical and procedural elements in place to safeguard the legal and ethical rights of SLaM service users during the development and use of CRIS.

1.2 Technical elements of the CRIS Security Model (CSM) were initially devised by the BRC Working Group and signed off by the Trust Caldicott Committee (Nov. 2007). The procedural elements were initially devised by the Case Register Security Procedures Working Group as part of the CRIS Development Project. All elements of the CSM will be subject to regular review by the operational CRIS Oversight Committee.

1.3 The SLaM CSM applies to CRIS installations derived from SLaM clinical data only, i.e. data from ePJS, JAC and SLaM IAPTus.

1.4 A record of updates and changes to the CSM will be recorded in the development and change log on the front cover of this document.

2. CRIS – what it's for and what it does

2.1 Sir William Castell, chair of the Wellcome Trust Fund, described accessing information from health records as one of the top three priorities for health research (Biomedical Forum, Guy's Hospital, February 2008). In a nut-shell this is what CRIS is designed to enable. Rather than being largely restricted to laboratory or trial based evidence only, access to CRIS will allow researchers to investigate the social and biological factors that both influence and predict actual outcomes in day-to-day clinical practice, thereby informing improvements in routine outcomes for all across clinical services. CRIS will also hugely increase the opportunity for service users to participate directly in specific research projects themselves by enabling researchers to identify potential recruits to projects from the whole service user population.

2.2 CRIS contains de-identified clinical data from SLaM NHS Foundation Trust. As well as research, CRIS may be used for Trust audit, quality improvement and service evaluation. CRIS may not be used for service management.

2.3 Using primarily MSSQL Server technology, CRIS allows researchers to define relevant service user groups by searching against any combination of structured fields (date, numerical etc.) or unstructured fields (user-defined text strings) from clinical data source. CRIS consists of a both de-identified SQL Server database that can be queried directly, and a front-end query builder – the CRIS Application – that enables users to 'hit' relevant records based on search terms, e.g. a particular diagnosis and/or a particular word or phrase in a clinical assessment or event. Users then specify the output fields they are interested in, also any combination of structured and unstructured fields from the clinical data source, which are returned in spreadsheet format and can be exported to other applications for analysis. Researchers can run searches against the whole data repository or set them up to run against entries made in the last 7 days only.

3. CRIS Security.

3.1 For CRIS to fulfil its potential to improve outcomes and opportunities for services users it is essential that the legal and ethical rights of service users are safeguarded throughout. With this in mind the development of the CSM was a core element of the overall CRIS development project. The CSM is broken down into two component parts – technical specifications built in to the application itself and procedural standards that govern the day-to-day use of CRIS.

3.2 **CRIS Security – Technical Elements**: these were initially developed by the BRC Working Group alongside functional requirements during the specification phase of the development project, from September to November 2007. The following table summarises the main security elements including in the CRIS design. For detailed specifications see Appendix A.

Table 1: Headline technical elements of the CSM	
i.	**Excluding personal identifiable information (PII) in CRIS:** All PII should be removed from CRIS data repositories entirely, including references in text and dedicated PII fields, or sufficiently truncated/modified to protect confidentiality, e.g.: • Date of birth: truncated to month and year of birth only • Post code: modified to Lower Super Output Area • Ethnic category: collapsed into the NHS standard 16+1 categories.
ii.	**Pseudonymising service user IDs:** A unique local ID number, the BRC ID, is created for all records for each CRIS instance. The BRC ID is linked to local source system ID, e.g. the ePJS ID. The linkage table is then separated from the searchable CRIS data repositories and so unavailable to CRIS users. A second pseudonym derived from NHS number – the 'shared_id' – is added and could be used to join data from independent CRIS instances. The link between the shared_id and the NHS number cannot be revealed by CRIS users.
iii.	**De-anonymising** It will not be technically possible for CRIS users to reveal the link between the BRCID and the source system ID / shared_id and NHS number or vice versa under any circumstances. Only the CRIS System Administrator or members of the CRIS technical team will be able access these links. The CRIS Administrator will be able to trigger emails from CRIS to service users' care co-ordinator or consultant that include the name and source system ID in the body of the email, e.g. to prompt possible consent to participate in research trials. The body of the email including the PII will not be accessible to the CRIS Administrator or CRIS users. The recipient will not be able to respond directly to the email, thereby inadvertently sending back the PII in an email reply.
iv.	**Access control**

	Access to CRIS repositories is password protected. Access is managed by the CRIS Administrator and technical team and granted for approved users (approved projects and suitable SLAM contract) only.
v.	**Audit trail** All activity is logged in an audit trail accessible to the CRIS Administrator only.
vi.	**Opt out** Local opt-out: Patients have the right to opt out from having their record in CRIS. CRIS includes an 'opt out' function that automatically excludes records specified in a configurable exclude list. National opt-out From 01-apr-2021 the national opt-out was deployed in CRIS. In accordance with guidance national opt-out must be applied where "Disclosures using S.251 support – Health Service (Control of Patient Information) Regulations 2002 Regulations 2 and 5" are deemed necessary (from *NDOPNationalDataOptOutPolicy_v4.0, section 5 When Does National Optout Apply, p.21*). This choice is submitted by local GPs and logged centrally by NHS Digital. Following deployment in April 2021 the NHS numbers of patients that have opted out at national level are logged in the CRIS source data. Researchers may not apply to scrutinise or in any way derive (e.g. from source data) the characteristics of individuals that have chosen to opt out.

For further details of CRIS technical security see Appendix A.

The full technical security model was signed off by the Trust Caldicott Committee, 9th November 2007.

3.3 **CRIS Security – Procedural Elements**: were initially developed by the CRIS Security and Confidentiality Procedures Development Group, a time-limited project team chaired by Dr. Felicity Callard, BRC Stakeholder Participation Theme. Membership included the Trust's Caldicott Guardian and child protection lead.

Table 2: Processes and actions required for CRIS to be fully implemented	
i.	The CRIS Oversight Committee (see appendix D for ToR) should be patient led and is responsible for overseeing and monitoring the use of CRIS, including: – **Managing the CRIS application process**. All projects proposing to use CRIS are required to submit a written application to the committee. Applications are judged according to • underlying value and potential benefits of the project, e.g. to inform patient care; • appropriate supervision / governance, e.g. research governance for research projects; formal clinical governance approval for audits; SLAM director sign-off for service evaluation; SLAM Quality Centre approval for quality improvement projects

	• inadvertent risk of deanonymisation, e.g. the likelihood of particularly small cohort / cell sizes (< 10 cases); appearance of high profile publicly known / published information, etc. In these cases additional measures may be put in place to safeguard confidentiality. Note: CRIS has not been developed to support service management. Applications to use CRIS to evaluate or monitor staff-level performance will not be granted. Applications to use staff names for legitimate research / audit purposes may be granted but additional supervision may be put in place, e.g. encryption of names in CRIS extractions. **Monitoring use**, e.g. comparing intended and actual use of CRIS through routine monitoring of the audit trail; **Managing the CRIS Security Model** – ensuring the model is fully implemented at all times and updated as required to meet appropriate standards. **Managing the CRIS Communications Plan** – ensuring relevant stake-holders, including SLAM service users and staff, are able to access relevant information about CRIS, including the right to opt-out **The CRIS Administrator** acts on behalf of the Oversight Committee, including managing CRIS applications, users' accounts and access to audit logs, committee meetings. The CRIS Oversight Committee is accountable to the Trust Caldicott Committee and includes SLAM Information Governance representation.
ii.	Individual users named in approved projects require a SLAM contract (honorary or substantive), KHP passport or research passport, which ensures users are contractually obliged to adhere to relevant Trust policies regarding confidentiality and data protection. Note – additional contractual obligations may be demanded by third-party data controllers through contracts and approvals with SLaM BRC Clinical Data Linkage Service.
iia.	All CRIS users are required to show up-to-date IG training at the point of project approval, e.g. from SLAM, KCL or other appropriate provider.
iii.	CRIS may be used to identify potential recruits to trial in accordance with the SLAM consent-for-consent (opt-in) process approved by the National Information Governance Board only (see appendix C). Applications to use CRIS for recruitment require CRIS Oversight Committee approval. In these cases reverse searches are carried out in batch by the CRIS Administrator. The link between the BRCID and the patient identifier is not revealed to users.
iv.	Patient identities from Trust Audit and Service Evaluation projects carried out on CRIS may not be revealed without explicit Trust Caldicott approval, in addition to CRIS Oversight approval. In these cases reverse searches are carried out in batch by the CRIS Administrator. The link between the BRCID and the patient identifier is not revealed to users.

v	CRIS may be used to extract clinical data for existing research cohorts recruited from SLAM. In these cases the BRCIDs of participants will need to be linked to known identifiers, i.e. source system ID or first name/last name/DoB combination. Permission to link known identifiers to the BRCID will only be given if explicit consent to access records has already been given as part of an existing, ethically approved project. In these cases reverse searches are carried out in batch by the CRIS Administrator. The link between the BRCID and the patient identifier is not revealed to users.
vi.	By default, patient level data must remain at all time within the SLAM firewall, including the data build phase (from PJS into datalake and throughout the de-identification process into SQLCRIS); searchable CRIS data repositories; the SQL table linking BRC ID with source-system and other identifiers, front-end applications to access these data, and all patient-level data exported from CRIS*. This ensures these data are subject to the same rigorous security standards (technical and policy) applied to other patient level data by the Trust. In addition, CRIS data should not be loaded onto Trust data sticks including encrypted sticks. All CRIS users are made aware of this decision when access is first granted. *project-specific output from CRIS should be saved to a dedicated SLAM network drive – BRC_CRIS. Access to this drive is granted to current CRIS users only.
vii.	The technical security elements are fully functional including the de-identification algorithms.
viii	CRIS has appropriate, up-to-date formal approvals, including Trust (Caldicott and Trust Executive) and ethics approval as an anonymised data source for secondary analysis (see 4. below). Note: as a deidentified data source, R&D approval is not required for CRIS
ix.	CRIS applications that require access to clinical text to manually derive quantitative outcomes are subject to additional review and recommendations to minimise risks of inadvertent deanonymisation. Outcomes of this review are shared with researchers and stored, as per the example template in appendix E, with the CRIS application.

3.4 CRIS operational support services: Specific and dedicated services to support day-to-day use of CRIS have been set up:

- CRIS Extraction – develops detailed extract specifications in collaboration with users for approved projects and writes extraction code out of SQLCRIS / CDLS / NLP repositories.
- Clinical Data Linkage Service (CDLS) - manages secure data linkages between CRIS and other third-party patient level data sets, including governance and approvals, data linkage, hosting and access.
- Natural Language Processing (NLP) - development and deployment of entity specific NLP applications to extract structured data out of clinical text.
- CRIS Admin - all elements of CRIS administration including project application process and CRIS communications

- CRIS Technical Support - development, maintenance and administration of CRIS technical infrastructure and data processing pipelines.

Note:
In carrying out their day-to-day duties the CRIS Clinical Informatics teams (above), SLAM Digital Services technical support and appropriately contracted third party suppliers are exempt from CRIS access and reverse search rules. In all cases there will be a contractual responsibility to protect identifiable patient data.

Specific projects may request patient level data to be taken out of the firewall, e.g. linking CRIS data with other health data outside SLAM through a trusted third party. In these cases applications detailing project-specific procedures to protect data must be made and require prior and explicit approval from the SLAM Caldicott and CRIS Oversight Committees. Subject to SLAM Caldicott recommendation, Section 251 approval or equivalent may also be required.

4. CRIS approvals

Table 3: CRIS approvals

Approving body	Approval for:	Date approved
SLAM Caldicott	CRIS security model	09.11.2007
	Consent for Consent model	14.01.2011
NRES Committee South Central - Oxford C	CRIS as an anonymised data source for secondary analysis ref: 18/SC/0372, previously: 08/H0606/71+5	16.09.2008 Renewed: 04.07.2013 Renewed: 2018
Trust Executive	CRIS security model	08.10.2008
	Consent for consent model	19.01.2011
South East London REC 4	Consent for consent model ref: 10/H0807/88	29.10.2010
National Information Governance Board	Consent for consent model	27.07.2010

Note: additional approvals obtained for data linkages between CRIS and other data sources (Hospital Episode Statistics, Thames Cancer Registry, ONS mortality, Lambeth Data Net), including s251, Trust Caldicott and Ethics amendments, are not listed here.

Appendix A: CRIS Technical Security Model.

The CRIS technical transformation process creates two complete, fully de-identified SQL repositories .

1. Hosting

The CRIS repositories are hosted on SLAM Azure infrastructure and only available from inside the SLAM firewall. CRIS is administered by the Clinical Informatics Technical Team and may be further supported by SLAM Digital Services infrastructure services. CRIS instances are protected by relevant SLAM IG and IT Security Policy and practice. SLAM has formal Data Security and Protection Toolkit (formally the IG Toolkit) approval.

2. Data de-identification

Data in both CRIS repositories are fully de-identified.

2.1 Pseudonymisation:

The BRCID: is a pseudonym created for every record as it is passed in to CRIS. The BRC ID is locally generated against the source system patient ID. The BRCID is not fully anonymised (i.e. the link between the BRCID and the PJS ID is not permanently destroyed):

- so that the BRCID allocated to each record remains consistent over time whilst allowing nightly updates from the source and periodic full data rebuilds;
- to enable reverse searching under agreed circumstances, e.g. to identify potential recruits that have consented to be contacted.

However, the link between the BRCID and the PJSID is not retained within searchable CRIS repositories and so is not accessible by CRIS users, rendering the BRCID as an effective anonym for CRIS users.

The shared_id: is a second, entirely independent pseudonym, created against the NHS number. Given appropriate permissions, the shared_id will enable records from independent CRIS repositories, e.g. ePJS and SLAM IAPT, to be joined, if and when the NHS Number is entered into both sources.

To enable possible linkages with CRIS repositories generated and hosted outside SLAM, the shared_id is generated through an NHS-approved encryption method that is unknown outside the CRIS technical team(s). It is therefore not possible for CRIS users to de-encrypt (reverse) the shared_id to reveal the NHS Number.

2.2 Removal of Personal Identifiers

All personal identifiers (PIs) are removed from CRIS repositories to protect the identity of services users.

Structured and small-text data: dedicated fields from PJS where PIs are recorded, e.g. first name, last name, address details, date of birth etc. are either excluded entirely from the searchable CRIS repositories or are truncated within CRIS.

Truncation/modifications: particular PIs are truncated so they are available for research purposes, without compromising confidentiality, e.g.

- date of birth – from dd/mm/yyyy to 01/mm/yyyy
- post code –Lower Super Output Area is derived from full postcode and replaces postcode in both FAST and SQL repositories. Output Area is also derived from full postcode but is not included in the FAST repository. Output Area is only available in CRIS SQL and is used by the CRIS administrator to extract deprivation scores and other area-based census data on behalf of CRIS users.
- ethnic category collapsed to NHS standard 16+1

N.B. Date of death is not truncated or modified in CRIS. Full date of death is available in both CRIS repositories.

Unstructured open text: service-user forename, surname, full date of birth (any known format), full address (any of lines 1-3 + postcode), phone numbers, alias(es) are all masked in unstructured field returns, e.g. Mr John Smith will be shown as Mr ZZZZZ ZZZZZ. Equivalent information relating to contact(s) – forename, surname, full address (any of lines 1-3 + postcode) and phone numbers will be masked by 'QQQQQ'. Where PIs are shared by patient and contact, e.g. last name, ZZZZZ will be used.

Field-level details of which fields are excluded, masked in, masked from are recorded in relevant SLAM CRIS data dictionary.

Detailed evaluation has demonstrated the effectiveness of the CRIS masking algorithms (Fernandes *et* al. [2013] *Development and evaluation of a de-identification procedure for a case register sourced from mental health electronic records*, BMC Medical Informatics and Decision Making.2013, 13:71).

NB Following the CRIS technology refresh (see Appendix B below) evaluation of the CRIS masking algorithms was formally repeated. As intended, results showed the new pipeline performed as well as the previous version. This evaluation was presented to and signed-off by the CRIS Oversight Committee (05/2018).

3. The CRIS Application

The CRIS application is front end query builder designed to facilitate direct query access to CRIS. The following technical security components are built in to the application.

3.1 Role-Based Access Control.

Two different roles are available:

Role 1 Observer – can:

- Observers can carry out full search and export from de-identified CRIS index
- Observers cannot conduct reverse searches (access the link between the pseudonyms and related patient identifiers) or access email for recruitment.

Role 2: **System Administrator** - can:

- create and modify user profiles, including allocating authorisation to use CRIS and modification of user details,
- view and truncate the Audit Trail,
- manage the list of ethically approved projects in CRIS
- Carry out reverse search (see below)
- Access to email for recruitment functionality (see below)

- Full search

3.2 Reverse search

The CRIS administrator is able to:

- reveal the source system ID and NHS number from the BRCID;
- reveal the BRCID from any of NHS Number; source system ID; first name, last name and full date of birth combined.

Reverse searches carried out by the administrator are directly linked to a specific project, from a database of ethically approved projects stored within CRIS. This link is recorded in the CRIS audit trail (see below).

N.B. the CRIS administrator can only carry out reverse searches in accordance with procedural guidelines (see Table 2, items iii, iv, v above)

3.3 Email for Recruitment

CRIS can be used to trigger emails to the care co-ordinators or consultants for selected patients. The selected patients' full names and source system IDs are automatically inserted into the body of the email along with additional user-defined text. The body of the email including the patient identifiers cannot be seen by the CRIS user or CRIS administrator. Only the email recipient (the care co-ordinator or consultant) can see the full email text including the patient identifiers. The email recipient will not be able to 'reply' to the email, i.e. inadvertently send an email containing the patient identifiers back to CRIS.

CRIS users are not able to access the Email for Recruitment functionality. The CRIS administrator only can access this functionality. For approved projects only the CRIS administrator will trigger Emails for Recruitment on behalf of CRIS users.

3.4 Audit Trail

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

3.5 Access controls

Access through the CRIS Application is password protected using authenticated SLAM network user name and password. It is not possible for data exported from CRIS to be

saved directly outside the firewall. Email alerts from alert searches will not contain any personally identifiable information and will be sent to internal SLAM email addresses only.

3.6 Sign-off

All functionality in the CRIS Application relating to security was tested and signed off by the Project Security Group following the initial CRIS development (September 2008).

4. SQLCRIS

SQLCRIS database is accessed through a standard MS SQL Server Management Studio client.

4.1 Audit

An audit log of all queries run by users is retained and can be queried by the CRIS Administrator.

4.2 Access control

Access is managed by the technical team. An assigned CRIS DBA grants access with the instruction of and only of the CRIS administrator.

5. SLAM CRIS – data sources

SLAM CRIS consists of two independent CRIS instances.

5.1 PJS CRIS

PJS CRIS is fed from the SLAM electronic record system, the Patient Journey System (PJS). In addition, patient level data from the Trust's pharmacy dispensing system, JAC, is integrated into PJS CRIS.

5.2 IAPT CRIS

IAPT CRIS is fed from the four borough-based adult IAPT services, from clinical data recorded in the IAPTus system.

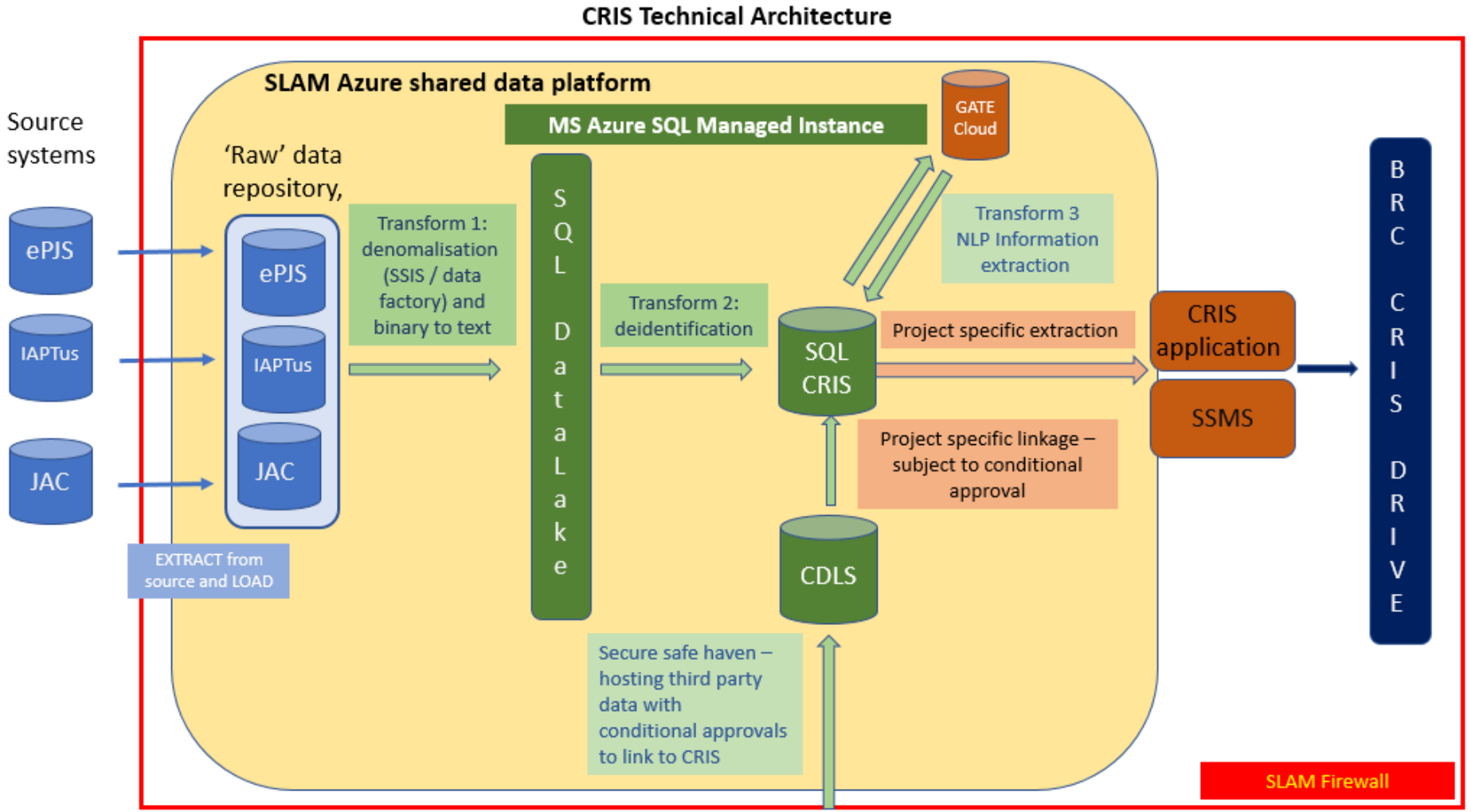
5.3 Linking PJS CRIS and IAPT CRIS

The two SLAM CRIS instances are built and maintained independently. However, given appropriate permissions data from two independent SLAM CRIS instances can be linked outside CRIS, e.g. including query joins between SQLCRIS dbs) using the shared_ID (see 2.1 above).

6. Opt out

During the CRIS build and for all data updates, records are automatically excluded from the CRIS repositories if they appear on an exclusion list of source system IDs derived from local opt out processes (see table 1,vi. above)

Appendix B – CRIS technical architecture



Appendix C:

Research participant recruitment through electronic medical records in the South London and Maudsley NHS Foundation Trust (SLaM)

BRC Recruitment Model

1. Introduction

1.1 The potential for using electronic medical records for research is considerable and widely recognised. The NIHR Specialist Biomedical Research Centre (BRC) for Mental Health at the South London and Maudsley NHS Foundation Trust (SLaM) and King's College London (KCL) has generated a secure and independent search engine for research, based on the electronic medical records of SLaM (Patient Journey System – PJS). This engine, the Clinical Record Interactive Search, (CRIS) has been approved for anonymised research by the relevant ethics review and Trust's Caldicott Committee and Executive.

1.2 CRIS is a pseudonymised case record system and therefore has the potential for reverse search, enabling identification of SLAM service users who meet given characteristics. One such characteristic might be previous agreement for such use of medical records and to be contacted for future research participation. This potential raises the possibility of using CRIS to enable service user participation in ethically approved clinical research studies.

1.3 This annex describes the proposed model for recruiting suitable participants for BRC research projects from the SLaM clinical population using CRIS. The model was developed by a dedicated project team, whose explicit aim was to ensure that the ethical and legal rights of SLaM service users were protected.

1.4 The team was led by the BRC's Stakeholder Participation Theme, which has been set up to help ensure that service users' views and interests are central to BRC initiatives, and which includes service user researchers. Membership of the team included the Trust's Caldicott Guardian and Child Protection Officer.

1.5 This model has been formally approved by the Trust's Caldicott Committee and Executive.

2. Model for ascertaining assent to be contacted about future research projects

2.1 The assent process for participation in this process will be conducted entirely by the service user's own clinical team.

2.2 A member of the service user's clinical team will discuss with the service user the BRC's research programme and the potential opportunities and implications of their participation in this 'assent for use of medical records for contact' process. Staff will be trained in research governance focussing on assent/consent issues and capacity to provide assent/consent. The process will emphasise to service users that they are not being asked for consent to participate in any particular study – simply to being contacted in the future about potential participation in specified research projects based on information in their medical records. The following points will be emphasised:

1. Participation in any subsequent study following contact will be entirely optional;
2. Independent consent for participation will be made for each subsequent study;
3. Future contact will only be made by researchers conducting projects fully approved by ethical committee;
4. Service users will have the option to withdraw from the 'assent for future contact' process at any point without having to provide a reason for this;
5. Service users' agreement or lack of agreement (or withdrawal of agreement) to be approached will not in any way affect their clinical care.

2.3 Staff training will include the assessment of mental capacity to provide informed assent. For service users lacking capacity in this respect, proxy assent will be sought from a close friend or relative. This person is most likely to be the principal caregiver identified in the clinical record.

2.4 A Research Participation Form will be created as an additional window in the SLaM electronic medical records system. This will record the following information:

1. Whether a discussion has taken place with the service user about being approached in the future for research and for information on their clinical records to be used for this purpose;
2. If so, a confirmation that this was carried out in accordance with Trust training, for which a supporting document/web link will be available);
3. Whether the service user agreed or not;
4. The name of the staff member discussing the matter with them and the date discussed;
5. A free text box to record any further information (e.g. the service user's particular preferences regarding research opportunities, if any).

2.5 An alternative Research Participation Form will be created for situations where the person has insufficient capacity to provide agreement. This will contain the same information in addition to details of the proxy with which this was discussed.

2.6 For service users that have given assent to be contacted, the Research Participation Form in the electronic medical record will also be used to record all subsequent contacts made by researchers, all projects the service user is participating or has participated in, all projects that the service user has declined to participate in, and any further relevant comments, e.g. types of projects the service user is particularly keen to participate in or not. If a service user withdraws consent to be contacted then the ability to link to their NHS number will be prevented (see 3.6).

3. Model for identification and contact of potential research participants

3.1. In order to access the medical records search engine (CRIS) for approaching potential research participants, a 'BRC recruiter' will be nominated by the project team. This person must have a substantive or honorary contract with SLaM and be an employee of one of the organisations forming King's Health Partners (KHP;

the Academic Health Sciences Centre comprising SLaM, KCH and GSTT NHS Trusts and KCL). Use of CRIS for all forms of research is logged and audited and misuse would be considered a serious matter by all members of King's Health Partners potentially resulting in disciplinary action. Employees of KHP organisations with substantive or honorary contracts with SLaM must receive training in CRIS before accessing the medical records database for research. Project teams will be asked to specify the line management of nominated BRC recruiters. In practice (described below), the BRC recruiter will also have to have access to the source electronic medical records, which will be applied for in the usual way (i.e. as for any other member of SLaM staff requiring records access).

3.2. BRC recruiters will use the electronic medical records search engine CRIS to identify potential recruits. As noted above, the CRIS application is a pseudonymised copy of the SLaM electronic records – the Patient Journey System (PJS). It enables researchers to search through records without revealing the identities of service users. Within CRIS, records are identified by a locally generated BRC ID. The BRC ID is linked to the source system ID number in the building of the CRIS data repository. All other identifiers from the clinical records are stripped out of CRIS. Research users of CRIS are unable to access the link between BRC ID and system ID, which sits in a separate SQL database, outside the CRIS data repository. For this level of access CRIS has received ethics approval as an anonymised research data source for secondary analysis.

3.3. To access CRIS a written application will be submitted to the BRC CRIS Oversight Committee. This committee manages access and monitors use of CRIS, is led by the BRC's Stakeholder Participation Theme and includes Trust Caldicott representation. Applications to use CRIS as a tool to identify potential recruits will only be considered for:

1. projects that already have specific ethics and R&D approval,
2. applicants nominated as BRC recruiters who have a contract with the Trust (substantive or honorary*) and are employed by one of the organisations forming King's Health Partners (SLaM, KCH, GSTT, KCL),
3. documentary evidence of an enhanced CRB check for the BRC recruiter,
4. existing permission to access PJS.

3.4 For approved projects, BRC recruiters will first search the anonymised CRIS data repository to identify potentially suitable recruits for their project. From these searches, potential recruits will be identified by their BRC ID only.

3.5 To contact potential recruits it will be necessary to link these BRC IDs with corresponding NHS numbers. However, CRIS has role-based access control, so researchers are not able to access the separate SQL database that links BRC ID to NHS number. Instead, the BRC recruiter will submit the BRC IDs of potential recruits they wish to contact to a trusted third party appointed and monitored by the Oversight Committee. In most cases this trusted third party (TTP) will be the CRIS project manager.

3.6 Through the CRIS application the TTP will have project-specific access to the SQL data base linking IDs. Access is only permitted by CRIS when a request

for de-anonymisation is linked to the specific Research Ethics Committee reference of the relevant project. As well as containing BRC ID and NHS number, this database includes the data indicating if service users have given assent to be contacted about research participation. Following a request for de-anonymisation, CRIS will only reveal the corresponding NHS numbers of those that have given assent to be contacted in PJS. The technical specifications built into the system mean that CRIS cannot bring back the NHS number of any service user that has not given assent to be contacted in PJS under any circumstances. The TTP will then pass the NHS numbers brought back to the BRC recruiter: i.e. of the potential research participants identified by the researcher that have given prior assent to be contacted. The link between BRC ID and NHS Number for this cohort will not be revealed and will be destroyed by the TTP.

3.7 The BRC recruiter who, as stated above, will have permission to access PJS, will use NHS numbers to access the full records of potential recruits. The researcher will then inform the care co-ordinator that he/she intends to contact the service user to discuss participation in the project and ask if there are any objections to this.

3.8 With the agreement of the service user's clinical team, the BRC recruiter will then contact the service user directly to discuss participation in the project. Details of the contact and its outcome will be entered by the BRC recruiter into the Research Participation Form in the service user's record.

3.9 The Oversight Committee will monitor the Patient Participation Forms. Participation in more than three studies will automatically trigger a flag for attention by the Oversight Committee. Options for action will include contacting the service user or their clinical team about whether they continue to be willing to be approached about research projects during the course of the current projects in which they are participating. The ability to identify by NHS ID through CRIS, the records of service users withdrawing consent to be contacted would be prevented (see 2.6 and 3.6) but service users would also have the option to temporarily withdraw consent to be contacted in which case this would be recorded on the Patient Participation Form

*N.B. It has been agreed that applicants holding honorary contracts with SLaM, otherwise employed by Kings College London, will face the same sanctions to those with substantive Trust contracts for breaching relevant Trust policy, e.g. a duty of confidentiality, including potential disciplinary action.

Appendix D

South London and Maudsley NHS
NHS Foundation Trust

CRIS Oversight Committee

TERMS OF REFERENCE

1. Background and purpose

1.1 The CRIS Security Model describes the terms and conditions under which SLAM clinical data can be accessed for research purposes in a way that protects the legal and ethical rights of patients. This model was given Trust Caldicott and Executive approval in September 2008 as well as Ethics approval.

1.2 The CRIS Oversight Committee is the owner of this model and is responsible for its content and overseeing its deployment by the BRC CRIS Services.

1.3 This document describes the specific Terms of Reference for the CRIS Oversight Committee.

2. Key responsibilities

- Project approval:

  Following scrutiny of all CRIS project applications against the principles and specific terms and conditions described in the CRIS Security Model, the committee is responsible for making the decision to approve each individual project application.

  The decision to approve will be quorate if:

CRIS project category	Minimum approvals required
All	• Patient representative • Trust IG Lead
Including data linkage	• CDLS lead
Including consent for contact	• R&D governance representative

  Committee members will recluse themselves from the approval process for projects in which they have a direct research interest.

  The committee is responsible for ensuring any additional constraints and conditions for accessing linked data held in the CDLS and agreed with third party data controllers are also observed.

- CRIS Communications:

Effective CRIS communications are essential for informing relevant stakeholders (patients; carers; public; professionals) about the access to clinical data through CRIS and benefits this access provides. The committee is responsible for maintaining and delivering the operational CRIS Communications Plan.

- Operational security:

  The committee is responsible for ensuring all other procedural elements of the CRIS Security Model are being followed and deployed through the BRC CRIS Services, including routine query audits, user contract and IG training requirements, other data security requirements.

- Complaints / queries

  The committee is responsible for responding to queries or complaints related to CRIS, e.g. from patients, excluding issues relevant to research governance for ethically approved projects or Trust audit

- CRIS Security Model

  As the owner of the CRIS Security Model, the committee is responsible for regularly reviewing the content of the model and ensuring the security model is updated as required to meet the latest legal and best-practice standards.

  The committee Terms or Reference will be reviewed at least annually.

  The Security Model will be reviewed at least biannually.

3 Deliverables

- The written CRIS Security Model
- The CRIS leaflet
- The CRIS Communications Plan
- The on-line CRIS Application Form
- Other documents, websites and reports developed and maintained by the CRIS operational services to support delivery of operational CRIS security including the Welcome To CRIS Guide; the Maudsley BRC CRIS website; the operational Balanced Business Scorecards; CDLS Annual Audit reports.

4 Membership and organisation

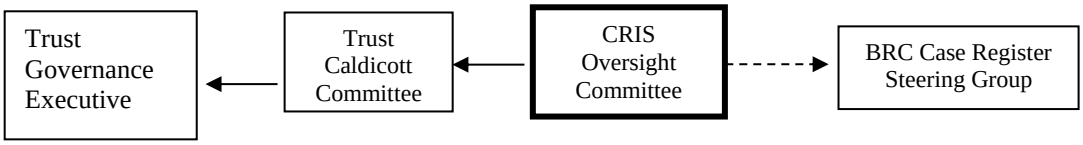
4.1 The committee will include, but is not limited to, relevant experts and representatives as follows:

- Patient and carer representation – including as Committee chair
- Trust Caldicott representation and IG Lead
- CAMHS clinical representative
- R&D governance representation
- CRIS Academic Lead
- CRIS operational service representation

- CRIS administration representation
- CDLS Lead

4.2 The committee will meet quarterly. Attendance of 50% of committee members + 1 are required to constitute a quorum for decision making. In addition, the committee will work electronically and remotely between meetings as required and agreed, e.g. the receipt and management of project applications

4.3 The committee will inform/report to relevant BRC and Trust groups as required and be directly accountable to the Trust Executive



Appendix E – Managing Access to Clinical Text

Based on experience to date, the following scenarios are the primary ones where text field reviewing is required:

1. To develop natural language processing (NLP) algorithms
2. As part of a qualitative research study with clinical text as the main data
3. As a pilot procedure to investigate the feasibility of a more substantive study (primarily using the CRIS front end)
4. To derive new quantitative data manually for a substantive study – i.e. one with a defined question to be answered

The fourth of these scenarios is the focus here. The rationale is most likely to be that at least some information required for a project is not available in existing structured fields and is not available (or not adequately available) through current NLP algorithms; therefore, manual text reviewing is required in order to derive this information.

The primary concern arising is the risk of inadvertent de-anonymisation as a result of text reviewing. A secondary concern is that over-ambitious projects are proposed that are dependent on text screening without sufficient resource, consequently failing to produce output and placing unnecessary workload on the CRIS extraction team. The following steps are recommended to accommodate text reviewing and reduce these risks:

1. There should be a clear rationale justifying the reviewing of text for the proposed project. Where reviewed text is one of several sources of variables for the project, these variables should be sufficiently justified as necessary for the validity of the project. This will be adjudicated by the Oversight Committee who will request specific written justification if this is not clear enough in the initial application.
2. There should be sufficient person-time resource for the text-reviewing by the study team. This will be adjudicated by the Extraction Team following discussion with the applicant(s) and clarification of data requests.
3. The sample for text reviewing should be clearly defined for/by the Extraction Team with no element of exploration involved. If the definition of the sample raises further concerns about inadvertent de-anonymisation (e.g., as a total sample of a particular clinical population/service), this should be raised again with the Oversight Committee.
4. The measurements to be derived from text reviewing should be pre-defined and a coding protocol/spreadsheet should be agreed in advance.
5. Where there are doubts about 2, 3 or 4, a pilot extraction is recommended, with a limited random selection of the proposed sample (e.g. 20-30 documents) and a review point with the Extraction Team (and, if indicated, with further Oversight Committee review) to establish final requirements in advance of any further extraction.
6. The final-stage text reviewing and coding should occur as a separate step from any analysis, so that text-derived information is assembled as a first step. This first-stage primary extraction for text reviewing should be limited only to the fields requiring review and to fields that will allow derived information to be linked with additional data at a second step. Ideally identifiers will be document

IDs, although patient-level IDs may be used if there is a need to derive information from several documents per patient. There should be a review point agreed when text-derived information has been fully assembled and where this is joined to the other variables required to complete the proposed analysis.

7. Consideration should be given to the individuals involved in the text reviewing – either to reduce the risk of them inadvertently guessing a patient's identity from the content of the text reviewed, or to reduce the risk of this de-anonymisation being inappropriate (e.g. because the individual is a clinician who would normally have permitted access to source records from a given service).
8. Outcomes and recommendations should be documented, shared with the researcher and be subject to oversight committee review annually. The following documentation structure is recommended:

Project number:

Researcher(s):

Describe text requirements:

- Search strategy
- Coding / trawling strategy
- Export / save requirements
- Publishing / distribution requirements

Made aware of risks and responsibilities, e.g. management of patient level exports; contractual and professional commitment to protect confidentiality:

Additional measures agreed: