South London and Maudsley NHS
NHS Foundation Trust

D-CRIS Information Governance Assurance

Date: 05 08 2013

Version: 1.0

Author: Murat Soncul

Contents

1. Introduction 3
2. CRIS Security Model 3
3. SLaM Information Governance Framework 4
4. Roles and Responsibilities 4
5. Information Governance Policies 6
6. Information Governance Assurance 8
7. Proposed Data flow 9
8. Supporting Documentation 10

1. Introduction

South London and Maudsley NHS Foundation Trust (SLaM) will be building and hosting searchable research repositories of clinical data from partner organisations who contribute to the programme of activities under D-CRIS.

The security of the personal identifiable clinical data that will be transferred from D-CRIS partners and hosted in SLaM is of paramount importance. The purpose of this document is to provide an overview of the specific and wider governance framework in SLaM that will maintain the security of personal identifiable information during the transfer of the data between D-CRIS partners and SLaM and throughout its storage once the data enters SLaM.

The information governance framework covers relevant information governance (IG) policies and procedures, responsible officers, oversight and monitoring bodies and assurance processes which support a sound and independently approved security model that will be applied by SLaM to D-CRIS and that will ensure partner organisations' clinical data are protected according to the highest possible governance and security standards throughout the process.

2. CRIS Security Model

SLaM already hosts its own version of CRIS using local clinical data, which has been developed to support anonymised observational research, local clinical audit and identification of potential recruits to trial. A dedicated CRIS Security Model has been developed describing how the ethical and legal rights of patients are protected in the building and use of CRIS (see Appendix A). The model was developed by a patient-led committee, which included representation from local Caldicott and Safeguarding Children Committees.

The CRIS Security Model consists largely of technical components (e.g. deidentification of clinical data to protect confidentiality, access constraints, audit logs etc.) and process components (e.g. the CRIS application process, data handling requirements, operational oversight etc.). The technical and process components of the CRIS Security Model ensure effective pseudonymisation in a safe haven, where all data repositories are kept securely within the Trust firewall, protected using access controls and audit logs. In addition to the CRIS Security Model, the Trust will sign up a data processing agreement based on the data requirements of D-CRIS to provide legal assurance to partner organisations (data controllers) that SLaM will process their data within a safe haven in a responsible, lawful, secure and confidential way in accordance with the CRIS Security Model and SLaM IG policies, in line with the Data Protection Act (1998) for the sole purpose of the D-CRIS Programme.

As a result of the security model, CRIS has received approval from the following internal Trust and external bodies:

- Local research ethics approval as an anonymised data source for secondary analysis,
- SLaM Caldicott Committee approval,
- SLaM Executive approval,

- The Ethics and Confidentiality Committee (ECC) of the National Information Governance Board (NIGB) support for a "consent-for-consent" process that uses CRIS to identify potential recruits to relevant research projects.

It is inevitable that equivalent approvals for D-CRIS will need to be sought by partner organisations internally, including research ethics, Executive and Caldicott sign off. The full application of the CRIS security model should form the key component for these approvals. The technical components of the CRIS security model will be applied by SLAM in the D-CRIS installation. Where necessary, relevant process components of the model will need to be set up locally by partner organisations, e.g. setting up over an operational oversight committee to manage applications and oversee operational use of the system.

However, given that D-CRIS will be built and hosted externally, details of the wider information governance framework used by the host organisation (SLaM) are essential for partner organisations' internal approvals (e.g. Caldicott and Executive) in addition to the elements of the CRIS Security Model. The key objective of the Information Governance Framework in SLaM is to provide an overview of the policies, procedures, responsible officers, oversight and monitoring bodies and assurance processes that underpins the security and confidentiality of person identifiable clinical data in the Trust. With this in mind, following a description of the data flow that will be applied to build D-CRIS this paper details the relevant elements of the SLaM IG framework and where they apply in the processes to build and host D-CRIS, to ensure its protection.

3. SLaM Information Governance Framework

Whilst providing services to treat people with mental illness with effective clinical outcomes, to work in partnership to promote mental wellbeing and to support others by sharing our clinical expertise and knowledge, SLaM is committed to working in accordance with the national statute and NHS information governance standards.

The Information Governance Framework provides a structure that enables the Trust to effectively comply with DH information governance standards, adhere to information governance related legislation, manage information related risks, provide assurance that adequate controls are operating to reduce these risks to acceptable levels and support the Trust to achieve its principal objectives.

4. Roles and Responsibilities

It is the role of the Trust Executive to define the Trust's information governance related policies. The policies and the procedures that support are reviewed by the relevant information governance committee on an annual basis taking into account legal and NHS requirements. The Executive Committee is responsible for ensuring that sufficient resources are provided to support the implementation of the policies.

The Risk Management Committee is responsible for the assessment of potential security risks and must ensure that risk action plans are kept under regular review.

The Caldicott Guardian (Dr Dele Olajide, Consultant Psychiatrist) is the appointed senior clinician, who carries the ultimate responsibility to oversee the use and sharing of personal identifiable clinical information.

The Caldicott Committee supports the Caldicott Guardian and the Head of Information Governance to ensure the Trust meets its legal obligations for data protection and confidentiality implementing the Caldicott principles and the regulations outlined in the Data Protection Act (1998).
The Chief Information Officer (Mike Denis, Director of Information Strategy) sets the vision and the direction for the Trust to ensure information resources are used to their maximum potential for the benefit of our patients and the general public using the technology solutions available.

The Senior Information Risk Officer (SIRO) (Ricky Mackennon, Deputy Director of ICT) is responsible for information risk. The ICT Security Committee and the Risk Management Committee support the SIRO and the Head of Information Governance to ensure the Trust meets national NHS Connecting for Health standards.

The Information Security Committee is responsible for the development and implementation of ICT security policies and procedures, maintaining the integrity of the ICT estate and the infrastructure, ICT contingency planning and undertaking assurance audits and monitoring implementation of action plans.

The FOI Committee ensures Trust compliance with the corporate records management standards and the Freedom of Information Act (2000).

The Head of Information Governance (Dr Murat Soncul) is responsible for the strategic and operational management of the Information Governance Team and is the Trust lead for the annual DH Information Governance Toolkit self-assessment. Head of Information Governance supports the Caldicott Guardian, the CIO and the SIRO to ensure the Trust meets the highest standards for appropriate governance of information in accordance with the NHS standards and Care Quality Commission regulations.

The Head of Information Governance is responsible for overseeing day to day issues regarding confidentiality, information security and records management; developing and maintaining policies, standards, procedures and guidance, and raising awareness where and when necessary. The Information Governance Team provides mandatory staff training at induction and during employment.

An overview of the structure of the roles above is presented in Figure 1 below.

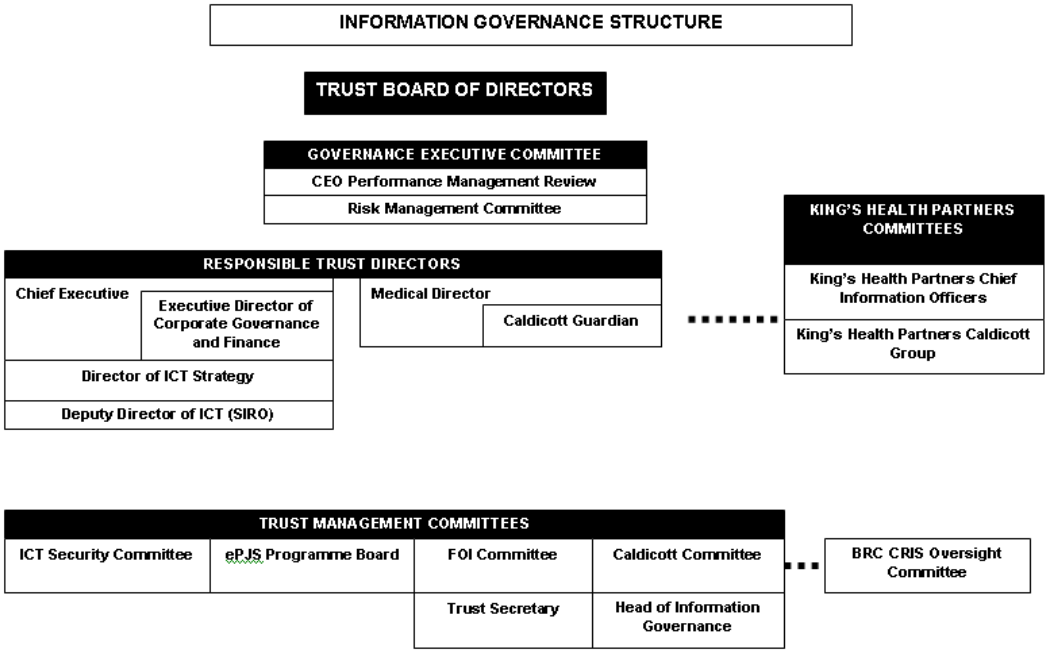


Figure 1- An overview of the structure of the information governance responsible officers and oversight bodies in SLaM

5. Information Governance Policies

The Trust ensures effective and secure management of its information assets and resources as outlined in the ICT Security Policy. The Trust promotes effective security practices to its staff through the ICT Security Policy, relevant procedures and training.

In addition to the SLaM ICT Policy, a system level security policy (SLSP) has been developed to outline the operating and the governance arrangement that support the Safe Haven set up in the Biomedical Research Centre.

The Trust's legal obligations for data protection, information sharing, disclosures, subject access and service user rights to confidentiality are outlined in the Trust Confidentiality Policy. The policy ensures compliance with the Data Protection Act (1998), Access to Health Records Act (1990), Human Rights Act (1998) and common law of confidentiality.

Information Sharing Policy outlines the standards for the sharing of clinical information with other health organisations and agencies in a controlled manner and in consistence with the interests of the service user. This Policy provides the standards for a uniform approach to information sharing with all partner agencies.

The Clinical Records Policy governs the management, handling and retention of clinical records. This policy covers the full clinical information cycle, including the purpose of these records, clinical records keeping standards, retention and preservation schedules with links to the Confidentiality Policy for guidance on access to records.

The full list of information governance related policies is provided below.

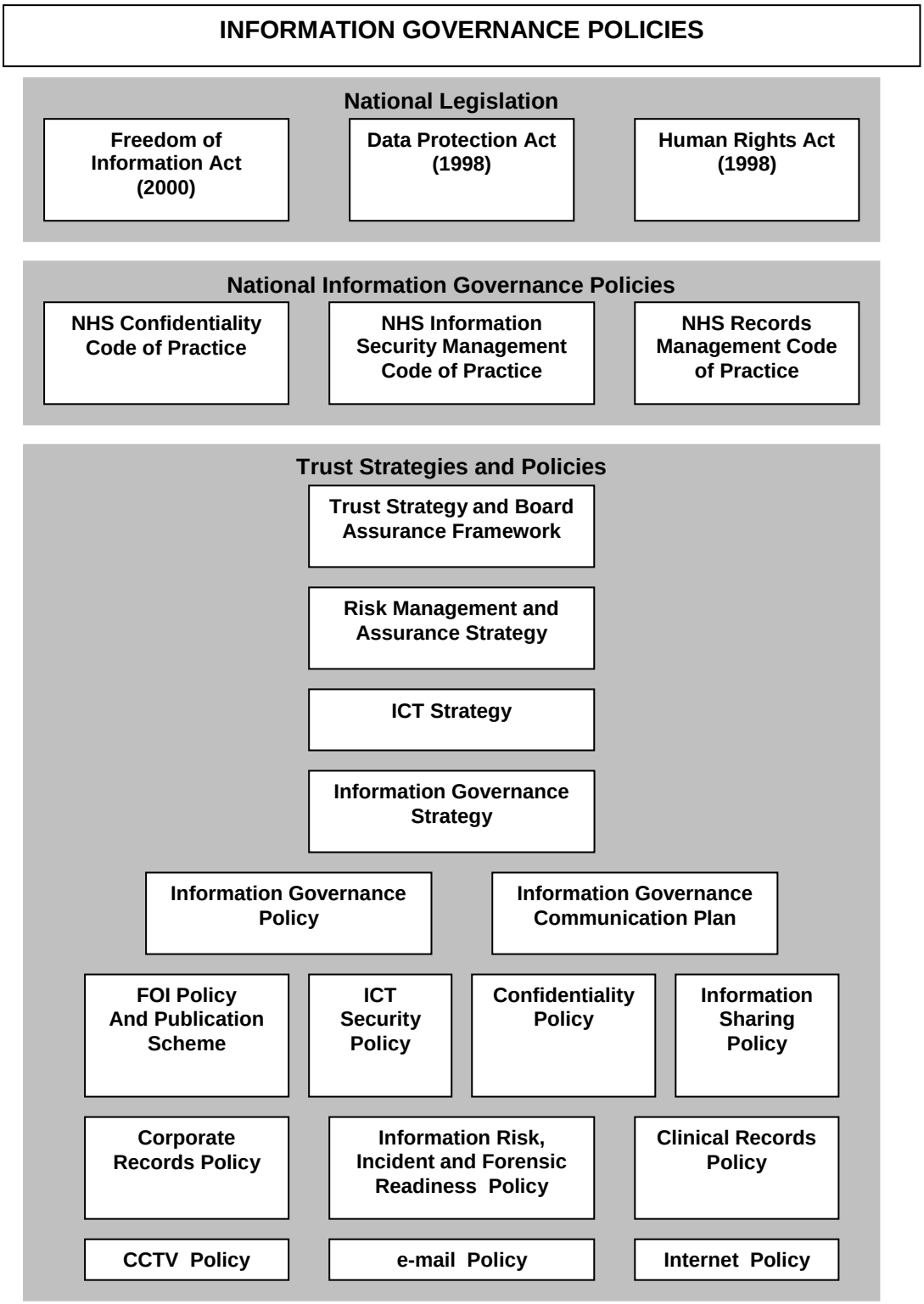


Figure 2- The full list of information governance related policies in SLaM

6. Information Governance Assurance

SLaM undertakes an annual assurance programme to review of its information and ICT security arrangements in compliance with NHS requirements, ISO 27001 security standard and national legislation. The assurance programme comprises the Computer Audit Programme, IG Internal Audits and the Information Governance Toolkit.

An overview of the Trust Information Governance Toolkit submissions for the last 3 financial years (IGT versions 8, 9 and 10), which were independently audited is provided below.

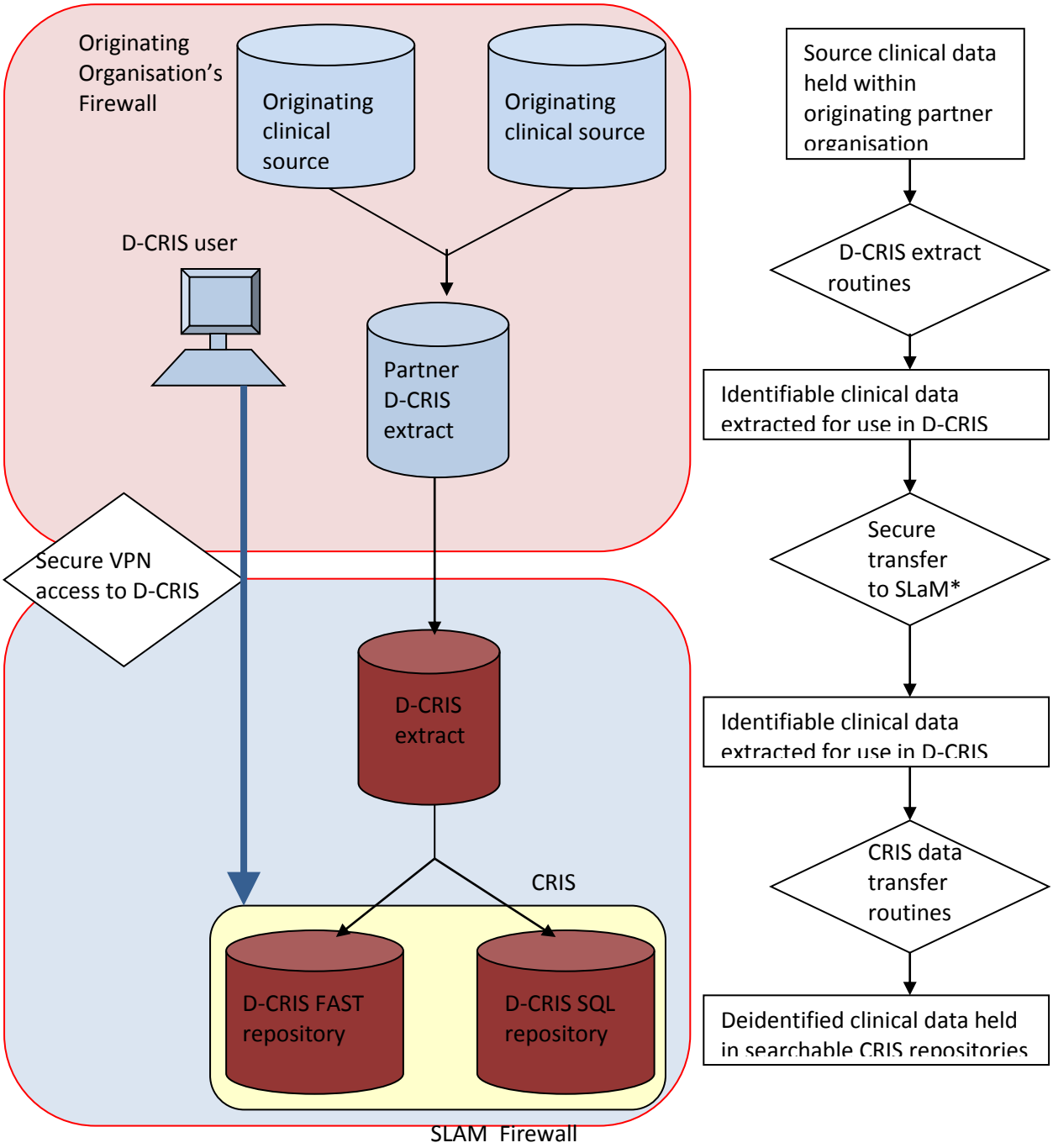
The Trust undertakes the Information Governance Statement of Compliance process by demonstrating a minimum of Level 2 compliance with the key information governance standards in the Information Governance Toolkit and signing the terms and conditions of the Information Governance Assurance Statement during annual submissions of the IG Toolkit assessments.

IG Toolkit scores independently audited and submitted by SLaM

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Not Relevant	Total Req'ts	Overall Score	Grade
Version 10 (2012-2013)	Final	0	0	11	33	1	45	91%	Satisfactory
Version 9 (2011-2012)	Final	0	0	12	32	1	45	90%	Satisfactory
Version 8 (2010-2011)	Final	0	0	14	30	1	45	89%	Satisfactory

7. Proposed Data flow

The proposed secure data flow is detailed below. The data flow process will be reiterated to refresh as required.



* D-CRIS data transfers from partners to SLaM will be undertaken utilising secure routes agreed and approved by D-CRIS partners. A separate document outlines these secure options.

8. Supporting Documentation

The following documents are provided as an appendix:

- CRIS Security Model
- BRC Safe Haven System Level Security Policy (SLSP)
- SLaM ICT Security Policy
- SLaM Confidentiality Policy

Further information on the information governance framework in SLaM can be directed to:

Dr Murat Soncul
Head of Information Governance
South London and Maudsley NHS Foundation Trust
Maudsley Hospital
Denmark Hill
London SE5 8AZ

murat.soncul@slam.nhs.uk