Clinical Informatics and Health Outcomes Research Group  
Department of Clinical and Experimental Medicine  
Faculty Health and Medical Sciences  
System Level Security Policy

**Document Reference**: UoS Clininf SLS Policy  
**Version Number**: 3.1

<table>
<thead>
<tr>
<th>NAME</th>
<th>TITLE</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authors</strong></td>
<td>Dr Tom Chan</td>
<td></td>
<td>16/1/18</td>
</tr>
<tr>
<td><strong>Authorised by</strong></td>
<td>Prof Simon de Lusignan</td>
<td></td>
<td>16/1/18</td>
</tr>
<tr>
<td><strong>Authorised by</strong></td>
<td>John Briggs</td>
<td></td>
<td>22/1/18</td>
</tr>
</tbody>
</table>

**Effective Date**: 01/02/2018  
**Review Date**: 30/01/2020

<table>
<thead>
<tr>
<th>NAME</th>
<th>TITLE</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filipa Ferreira</td>
<td>Project Manager</td>
<td></td>
<td>16/1/18</td>
</tr>
<tr>
<td>Ivelina Yonova</td>
<td>Practice Liaison Officer, RCGP RSC</td>
<td></td>
<td>22/1/18</td>
</tr>
</tbody>
</table>
## CONTENTS

| 1. DOCUMENT HISTORY                       | 3 |
| 2. INTRODUCTION                           | 6 |
| 3. SCOPE                                  | 6 |
| 4. SYSTEM DETAILS                         | 7 |
| 5. SYSTEM SECURITY                        | 7 |
| 6. SYSTEM MANAGEMENT                      | 8 |
| 7. SYSTEM DESIGN                          | 8 |
| 8. OPERATIONAL PROCESSES                  | 9 |
| 9. SYSTEM AUDIT                           | 11 |
| 10. SYSTEM PROTECTION                      | 11 |
| 11. SYSTEM LEVEL SECURITY OWNERSHIP       | 12 |
| 12. DATA PROTECTION REGISTRATION          | 12 |
| 13. ACCESSIBILITIES OF THE POLICY          | 12 |
| 14. POLICY APPROVAL                       | 12 |
| 15. MONITORING, EVALUATION AND REVIEW OF THE POLICY | 12 |
| 16. REFERENCES AND SUPPORTING INFORMATION | 12 |
1. DOCUMENT HISTORY

<table>
<thead>
<tr>
<th>Document no.</th>
<th>Effective Date</th>
<th>Significant Changes</th>
<th>Previous document no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UoS Clininf SLS Policy 1 V1</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| UoS Clininf SLS Policy V2       | 31/03/2015     | • Up-dated references & links to University and Departmental policies  
• Up-dated monitoring methods and procedures in the event of a security or confidentiality breach  
• Reviewed and up-dated the technical details in the sections covering System design, system security, operational processes and system protection. | UoS Clininf SLS Policy 1 |
| UoS Clininf SLS Policy V2.1     | 30/04/2016     | No changes other than extending the review date.                                                                                                                                                                       | UoS Clininf SLS Policy V2 |

We are waiting for the publication of new data security standards as recommended by Dame Fiona Caldicott’s expected report. The publication of the report has been delayed and is likely to be published after the EU referendum on 23rd June. As there have not been any significant changes to the IG infra-structure or procedures within the Department which necessitate an immediate review, Prof de Lusignan, Head of Dept and Mr John Briggs, Faculty IT Services Manager, who has the mandate for approving departmental IG policies on behalf of the Faculty, agreed we would extend the review date until 31/12/2016.
<table>
<thead>
<tr>
<th>Document no.</th>
<th>Effective Date</th>
<th>Significant Changes</th>
<th>Previous document no.</th>
</tr>
</thead>
</table>
| UoS Clininf SLS Policy V2.2 | 01/02/2017 | No changes other than extending the review date and up-dating the name of the Department (and web-addresses), which was renamed 'Department of Clinical and Experimental Medicine', following its transfer to the Faculty of Health and Medical Sciences in 2015 and subsequent managerial changes in 2016.  
At the time of the last review (April 2016), we were waiting for the publication of new data security standards as recommended by the National Data Guardian (NDG), Dame Fiona Caldicott’s expected report. It was anticipated that new data security standards would have been rectified by the DH in September 2016. However, this was not the case: finding of the NDG’s report has undergone a period of consultation and the result of the consultation has not yet been published.  
It was agreed by the Governance Review Group that the review date would be extended by 12 months, unless there are other intervening reasons that necessitate an earlier review (e.g. changes in technology or procedures/policies within the University or the Department). | UoS Clininf SLS Policy V2.1 |
<table>
<thead>
<tr>
<th>Document no.</th>
<th>Effective Date</th>
<th>Significant Changes</th>
<th>Previous document no.</th>
</tr>
</thead>
</table>
| UoS Clininf SLS Policy V3.0 | 31/03/2015     | • Up-dated references & links to University and Departmental policies.  
• Reviewed and up-dated the technical details in the sections covering System design, system security, operational processes, back-ups and system protection.  
• Up-dated the two principal routes for in-bound data flow into the private secure network in Section 8 to include data transfers from NHS Digital using their secure file transfer systems. | UoS Clininf SLS Policy 2.2                                 |
2. INTRODUCTION

The System Level Security Policy (SLSP) has been developed to protect the integrity, confidentiality and security of research data held by the Clinical Informatics and Health Outcomes Research Group, Department of Clinical and Experimental Medicine at the University of Surrey. It describes the system level security arrangements for the Clinical Informatics and Health Outcomes Research Group’s dedicated secure network. The aim of this policy is to ensure business continuity, and to minimise any business damage by preventing and reducing the impact of information systems security incidents.

This document is structured using the SLSP template recommended by the former National Information Governance Board for Health and Social care (http://www.nigb.nhs.uk/s251/howtoapply/slspsview).

3. SCOPE

This policy applies to the private secure network dedicated to support the research activities of the Clinical Informatics and Health Outcomes Research Group. It outlines the security arrangements and procedures in place underpinning this policy.

All staff members, including temporary staff, agency staff and students of the Clinical Informatics Research Group who have access to the private secure network as part of their roles are expected to comply with the terms of this policy.

Other relevant policies/procedures and associated documents

The University has a number of policies and guidelines supporting the Information Governance agenda published in its web pages and handbooks for staff and students. This System Level Security Policy should be read in conjunction with other relevant University and departmental policies and procedures as follows:

University level policies

- University of Surrey Information Security Policy, University of Surrey (2014) (http://www.surrey.ac.uk/about/corporate/policies/information_security_policy.htm)
- Code of Good Research Practice, University of Surrey (2012) (http://www.surrey.ac.uk/about/corporate/policies/code_on_good_research_practice.pdf)
- Research Data Management Policy 2014 (http://www.surrey.ac.uk/about/corporate/policies/research_data_management_policy.htm)

Departmental policies

All up-to-date versions of departmental policies and standard operating procedures of the Research Group can be found in (https://clininf.eu/index.php/information-governance/)

- Departmental Information Governance policy, Clinical Informatics and Health Outcomes Research Group, Department of Clinical and Experimental Medicine at the University of Surrey
• Departmental Mobile computing and teleworking policy, Clinical Informatics and Health Outcomes Research Group, Department of Clinical and Experimental Medicine at the University of Surrey
• Standard Operating Procedure for data extraction, pseudonymisation and transfer of the data to secure SQL (Structured Query Language) server, Clinical Informatics and Health Outcomes Research Group, Department of Clinical and Experimental Medicine at the University of Surrey
• Standard Operating Procedure for data access, Clinical Informatics and Health Outcomes Research Group, Department of Clinical and Experimental Medicine at the University of Surrey
• Risk Assessment of physical security report, Clinical Informatics and Health Outcomes Research Group, Department of Clinical and Experimental Medicine at the University of Surrey
• Departmental Guidance: Security desk, clear screen and printing

4. SYSTEM DETAILS

The System is known as:
Clinical Informatics Research Group Secure Network at University of Surrey – “Surrey Secure Network (SSN)”

The System’s responsible owner is:
Faculty IT Services

The System’s Data Controller is:
Professor Simon de Lusignan

5. SYSTEM SECURITY

Security of the “Surrey Secure Network” is consistent with the framework of University of Surrey’s Information Security Policy, available from:
http://www.surrey.ac.uk/about/corporate/policies/information_security_policy.htm

The System’s responsible security manager:
Mr John Briggs – IT Manager – Faculty Health and Medical Sciences

The security manager duties include

• Managing user access to system (add/remove).
• Managing the physical systems (hardware maintenance) and ensuring network connectivity/security.
• Ensuring that equipment is disposed of according to University regulations and security requirements.
• Ensuring that the firewall is correctly configured to prevent unauthorised access.
• Managing an asset register.

The System incorporates the following security countermeasures

Physical security measures (E.g. secure room, cabinet, etc.)
• Servers are housed in their own physically secure environment with access to the servers restricted to a subset of the University’s IT staff.
• System is contained within its own locked cabinet.
• A risk assessment of physical security of the Research Group was conducted in November 2013 and reviewed in 2016. The assessment shows that the risk of unauthorised access to the premises, equipment, records and other assets is low (https://clininf.eu/index.php/information-governance/).
Logical measures for access control and privilege management

- Workstations on the Surrey Secure Network have login restrictions applied, preventing any unauthorised logins.
- Users are only granted access to the system by permission from the System's responsible security manager, the Faculty's IT Manager.

Network security measures (E.g. firewalls, network segregation, etc.)

- The Surrey Secure Network is protected by a firewall device. No inbound traffic is allowed unless it is in response to an outbound request.
- Patching requests to the Surrey Secure Network are only accepted if they are from the System's responsible security manager, the Faculty's IT Manager.

Other measures (including authentication or certification arrangements, security testing, and audit)

- Users authenticate to the system using their University username/password and are bound by the University's IT policy.
- Users are required to change their password every 90 days.

6. SYSTEM MANAGEMENT

- The System is developed/provided by the Faculty Health and Medical Sciences at the University of Surrey. The System is supported by the Faculty based IT Team.

- The System is implemented by the Faculty IT Team and maintained by the Faculty IT Team. The IT Team is responsible for support and maintenance of the System including replacements for faulty components. Replacement and disposal is handled by the IT team in consultation with the Clinical Informatics and Health Outcomes Research Group and in line with University information security policies. All physical data containing media are securely shredded and destroyed into a non-reusable state by an approved contractor.

- The Secure System is not shared or used by any other person or organisation other than those attached to the Clinical Informatics and Health Outcomes Research Group.

7. SYSTEM DESIGN

- The system consists of a Microsoft SQL Server 2012 application server which is used to host the data. All processing is undertaken on the 'R Analysis Server' which links to the SQL server across the network. Users have to be using a secure desktop connected to the network in order to access the application server. There is a secure file server available to allow storage of project related files and unstructured datasets within the secure network.

- All servers are virtual machines hosted on the Faculty VMWare environment. Disk storage is presented via a fibre channel connection to an SAN array. Secure data is only presented to dedicated virtual machines used with the service. All volumes are RAID6 with redundant hot-spare and backups are taken each evening. All backup data is encrypted from leaving the secure server through to the backup storage.

- Backups of patient level data are stored, using AES-256bit encryption at rest and in transit, in two on-site data centers at the University. No NHS data is stored in 'cloud' hosted systems for off-site backup this is an agreed exception to the general University backup policy.
• The servers are connected to a private IP address network with the workstations connecting on the same network VLAN. Only workstations belonging to the Clinical Informatics Research Group are connected to this network. The connecting workstations have pre-defined static IP addresses and there is no automatic IP address allocation within the secure VLAN.

• A router/firewall provides external access to devices on the private network. Traffic is only permitted to flow out of the network, all inbound connections are dropped.

• Preventing unauthorised access to the system and its data:
  o In order to access the system, members of staff are required to have access to the room where the workstations connected to the secured VLAN are located, and University of Surrey username/password, and have access to the system granted by the head of the Research Group (Prof. Simon de Lusignan).
  o The secure network is located on its own private VLAN, with a link to the rest of the University network provided via a firewalled router.
  o Data can only be accessed and processed using the secure terminals in the Clinical Informatics and Health Outcomes Research Group. The use of personal equipment is not permitted and cannot be connected to the Surrey Secure Network.

8. OPERATIONAL PROCESSES

The specific procedures for the collection and transfer of patient identifiable/sensitive information are described in a Standard Operating Procedure for data extraction (https://clininf.eu/index.php/information-governance/). In essence:

**Collection of patient identifiable/sensitive data**

The Research Group works in partnership with a range of academic & research institutions, NHS organisations and professional bodies such as the Royal College of General Practitioners & Public Health England using routinely collected patient level healthcare data for research and evaluation projects. Currently, there are two principal routes for in-bound data flow:

• On-site collection - data is collected on-site from healthcare providers using encrypted laptops and external hard drives (e.g. use of MIQUEST (Morbidity Information QUery and Export SynTax) in the extraction and collection of clinical data from GP practice information systems)

• Network transfer - transfer or upload of large encrypted and password protected data files through the internet (e.g. file transfers from third party commercial information provider services such as Apollo Medical Software Solutions (http://www.apollomedical.com/), and from NHS Digital using their secure file transfer systems).

The governing operating principles are:

• Patient identifiable/sensitive data are collected only with appropriate consent, formal data sharing agreement, or appropriate approvals as needed (i.e. approval from Research Ethics Committee, or CAG (Confidential Advisory Group) of the National Research Authority).

• All data is sent to us encrypted using industrial standard encryption software during transition and only decrypted once it is within the Surrey Secure Network dedicated to the Research Group.

• On-site data collection from healthcare providers such as GP practices will use only CESG-approved standard encrypted laptops and external hard drives for the secure transfer of data between the data source systems and the Surrey Secure Network.
The data storage

- All of our research data, including sensitive data at patient level, is held electronically, and stored in Group’s secure SQL server within the Surrey Secure Network.
- The SQL data files will be processed into an appropriate format and appropriately labelled by the SQL Developer for analysis by the Research Group.
- No data containing one line per patient is shared outside of the Research Group unless it has been pseudonymised, and then only to ‘bona fide’ researchers and ‘bona fide’ research organisations who give us written confirmation that it is kept according to their Information Governance research policies for holding large pseudonymised data.

The data processing

- Data will be processed using:
  - Desktop computers that are only connected to the secure network
  - Secured encrypted laptops – laptops synchronise data to allow offline work on small sub-set of pseudonymised data which is not patient identifiable. All laptops have their local disk encrypted using CESG approved standards.
- There is no access to the Surrey Secure Network from inside or outside the University and therefore no access to the servers holding the data. Access is only available from a secure workstation connected to the secure network.
- Patient level data is only accessible on the Surrey Secure Network. No other equipment is connected to this network, and access to this network is controlled.

The System’s authorised users

- The System’s authorised users are restricted to the members of the Clinical Informatics and Health Outcomes Research Group approved by the Head of Department, Prof Simon de Lusignan, or his named senior member of the research/teaching team.

Dispose of equipment, back-up media or other stored data

- Research data is retained for 10 years after the completion of the study in accordance with University policy on research data management.

---

1 *bona-fide* research is considered by the Medical Research Council as:

- An intention to generate new knowledge and understanding using rigorous scientific methods. (This includes discovery research, development and validation of methodology and technology, validating and challenging previous findings, and pilot research). And...
- An intention to publish the research findings and share the derived data in the scientific community, without restrictions and with minimal delay, for wider scientific and eventual public benefit. (Recognised constraints include a short prepublication delay to ensure proper management of intellectual property). And...
- The intended activities are not inconsistent with legal and ethical requirements or widely recognised good research practice.

A *bona-fide* research organisation is one that has the capability to lead or participate in high quality, ethical research. It will have a public commitment to adhere to recognised research and information governance good practice.
• The System will be covered by University policy in terms of security, disposal, replacement, licensing, etc.
• When the system or its data has completed its purpose, has become redundant, or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data: In accordance with University policy, all equipment that is no longer required is disposed of via our waste management partner. All media (including hard disks, CDs, memory keys, etc.) are disposed of via confidential waste processes. Hard disks are physically destroyed.

9. SYSTEM AUDIT

• The System shall be risk assessed every 12 months, which includes an annual infrastructure penetration test. The University of Surrey uses the ITIL (Information Technology Infrastructure Library) Risk Management framework for its IT policies and management.
• All in-bound and out-bound data flows of the Research Group are identified and subjected to risk assessments.
• A risk management/security improvement plan shall be established to address all unacceptable risks. This will be incorporated into the system design and review stage.

10. SYSTEM PROTECTION

• Services are backed-up and data replicated between 2 data centres on campus. These are geographically spaced to provide cover for disaster purposes to ensure a copy of the data can be recovered.

• The Clinical Informatics Research Group Secure Network is a single instance system therefore disaster recovery can only help recover the data not the physical hardware. Individual hardware devices have appropriate resilience, and services make use of the VMWare high availability service to move individual servers should there be a hardware failure.

• The system is also protected by a UPS (Uninterruptible Power Supply).

In the event of serious disruption or total system failure:

• In the event of serious disruption or total system failure, business continuity shall be provided by the steps described above. In addition, data is protected against total system failure (within a 1 day window of backup); however, hardware would need to be sourced to allow continuation of service.

In the event of a security or confidentiality breach occurring:

• All systems within the University are bound by the University’s Information Security Policy (http://www.surrey.ac.uk/about/corporate/policies/information_security_policy.pdf). In the event of a security or confidentiality breach occurring, the University of Surrey’s Incident Reporting Procedure shall be followed.
• Within the Clinical Informatics and Health Outcomes Research Group, all staff members have a duty to report potential or actual breach of information security to the Head of Department or to the Programme Manager, so that the Department can co-ordinate an effective management of the information incidents, and onward reporting to the University as appropriate.
11. SYSTEM LEVEL SECURITY POLICY OWNERSHIP

SLSP Responsibility

- This SLSP shall be the responsibility of the University of Surrey’s Faculty of Health and Medical Sciences IT Services Manager.
- This SLSP shall be reviewed at least every two years for its completeness and for any relevant updates.

12. DATA PROTECTION REGISTRATION

Registration number: Z6346945
Expiration date: 17th January 2018

13. ACCESSIBILITY OF THE POLICY

This policy will be placed on the Clinical Informatics and Health Outcomes Research Group’s web page: https://clininf.eu/index.php/information-governance/

All staff members of the Research Group will be alerted to the policy and its implications at the Research Group’s regular team meetings and Technical Group meetings.

14. POLICY APPROVAL

Revisions to this policy are version controlled and logged.

The final agreed version of this policy and its supporting Standard Operating Procedures are endorsed by the Head of Department, and approved by the Faculty’s IT Services Manager on behalf of the Faculty.

15. MONITORING, EVALUATION AND REVIEW OF THE POLICY

Responsibility for monitoring and evaluation of this policy lies with the Faculty’s IT Services Manager and the Head of the Department of Clinical and Experimental Medicine (or a senior academic within the department with delegated responsibility).

Compliance of Information Governance policy will be monitored by:

- Reports of information incidents.
- Notes of meetings of the Research Group’s regular Governance Review meetings.

This policy will be reviewed at least every two years, or when any new legislation or statutory obligations arise, or as required by the University, or to reflect any significant changes in national guidance for best practice in information security.

16. REFERENCES AND SUPPORTING INFORMATION

The development of this policy is informed by key national publications & guidelines, including:

- Information Security Management: NHS Code of Practice
  (http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/securitycode.pdf)
• UCISA Information Security Toolkit Edition 3.0
  (http://www.ucisa.ac.uk/publications/toolkit.aspx)
• NHS IGTK requirements for Hosted Secondary Use Team/Project
  (https://www.igt.hscic.gov.uk/home.aspx)