## STANDARD OPERATING PROCEDURE FOR DATA ACCESS AND DATA SHARING

**SOP Reference**: UoS Clininf SOP 2  
**Version Number**: 2.2

<table>
<thead>
<tr>
<th>NAME</th>
<th>TITLE</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author</strong></td>
<td>Dr Tom Chan</td>
<td></td>
<td>16/01/2017</td>
</tr>
<tr>
<td><strong>Authorised by</strong></td>
<td>Prof Simon de Lusignan</td>
<td></td>
<td>30/06/17</td>
</tr>
<tr>
<td><strong>Authorised by</strong></td>
<td>John Briggs</td>
<td></td>
<td>24/01/17</td>
</tr>
</tbody>
</table>

**Effective Date**: 01/02/2017  
**Review Date**: 31/01/2018

### READ BY

<table>
<thead>
<tr>
<th>NAME</th>
<th>TITLE</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. PURPOSE

The Standard Operating Procedure (SOP) for data access and data sharing provides a set of instructions on data access, including remote access, and data sharing with bona-fide researchers of external academic, professional or research organisations. The purpose of this is to ensure that the procedures for data access and sharing in the Clinical Informatics Research Group are:

- transparent and consistent with best practice
- performed consistently with minimal variability
- compliant with legal obligations and national and University guidance

2. INTRODUCTION

The Clinical Informatics Research Group of the Department of Health Care Management & Policy works collaboratively with academic, commercial, statutory and voluntary services partners in a range of funded research and evaluation projects using healthcare data. Formal data sharing statements, if needed, are incorporated in the funding agreements. From time to time, members of the Research Group need to access research datasets from home; our research partners also need to access pseudonymised data remotely from other research/academic institutions to contribute to the analysis and reporting in collaborative studies.

Data collection in health research is expensive and time-consuming. The Clinical Informatics Research Group supports the Medical Research Council (MRC) and the Organisation for Economic Co-operation and Development’s (OECD) call for a culture of openness and sharing to increase the return on public investments in scientific research and exchange of good practice. Making research datasets available to bona-fide investigators beyond the original research team in a timely and responsible manner, subject to appropriate safeguards, will generate key benefits:

- Faster progress in improving health
- Better value for money
- Higher quality science

3. SCOPE

The Standard Operating Procedure for data access and data sharing covers the specific procedures for accessing pseudonymised patient level data by the following groups of eligible users:

- Employed and associated staff members of the Clinical Informatics Research Group
- External researchers in collaborative studies
- External researchers of bona-fide organisations who wish to access pseudonymised data for secondary analysis in domains congruent with the research aims of the Clinical Informatics Research Group
- Students of the taught courses conducted by the Clinical Informatics Research Group (e.g. the Surrey Information Summer School)

The Standard Operating Procedure for data access and data sharing does not cover formal data sharing agreement as part of the funding agreement, which is addressed on a project-by-project basis with the support and guidance of the University’s Research and Enterprise Support (RES) service.
4. **ABBREVIATIONS & DEFINITIONS**

CAG – Confidential Advisory Group of the Health Research Authority

R&D – Research and Development

REC – Research Ethics Committee

RES - Research and Enterprise Support

5. **DUTIES & RESPONSIBILITIES**

**Information Compliance Officer**

- Acts as the University’s equivalent of the Caldicott Guardian and Data Protection Officer
- Advises on the protection and security of confidential information

**Head of Department and/or designated senior academics**

- Ensure that systems are in place to review information technologies, research methods, and information governance processes as an on-going developmental process, in order to improve the efficiency and security in accessing data for research and evaluation purposes.
- Receives and scrutinises all requests for access to patient level data held by the Research Group
- Approves and signs off applications for access to patient level data by eligible users

**Central IT Services**

- Maintains an asset register of IT equipment for the Department of Health Care Management and Policy.

**Faculty IT Services Manager**

- Manages access rights, and ensure that business continuity and recovery plans are in place.
- Conducts risk assessments of system level security and implement plans for the reduction of such risks, as needed.

**Principal/Chief Investigators**

- Ensure that data sharing and intellectual property issues are addressed with the support of RES in all external funded projects
- If appropriate, ensure that a data sharing statement is included in the grant applications and applications to the appropriate authorities for approval (e.g. REC, local audit committee, local R&D Office, and CAG)

**SQL Developer**

- Uploads collected data into the SQL server within the secure network of the Research Group and maintain documents for the processes.
- Maintains an asset register of databases for the Department of Health Care Management and Policy.
- Makes available in the external facing analytical server a subset of the data from the database meeting the approved requirements of the approved request, ensuring that no patient identifiable information is released.
- Monitors and reviews requests for access to patient level data periodically
All employed and associated staff members of the Research Group

- Ensure personal information is processed in accordance with the eight Data Protection Principles and other requirements of the Data Protection Act.
- Adhere to the confidentiality clause in their employment contract.
- Comply with the University’s Data Protection and Information Security policies.
- Comply with the Standard Operating Procedure for data access and data sharing when accessing or sharing data remotely, taking account of the Departmental Mobile Computing Policy and University Teleworking Policy.
- Complete basic IG training, the University e-learning modules on Data Protection, and refresher trainings as required.
- Report any breaches of confidentiality.

IG Lead in the Research Group

- Ensures that IG policies are complied with, and that incidents are reported and addressed in accordance with the University’s Information Compliance Unit guidance.
- Reviews the Standard Operating Procedure annually to reflect developments in technologies and governance frameworks, within the University and in line with national guidance.

6. SPECIFIC PROCEDURE

Patient level databases are held in the SQL server (DBServer1) within the Research Group’s secure network in accordance with University’s guidance on retention of research data and the terms of the approval for the project concerned.
The Research Group’s secure network is diagrammatically represented in Diagram 1. The secure network is sited behind a firewall within the University’s network, all in-bounded connections are block, but out-bounded connections are allowed. All staff members of the research group working within the team base work from secure workstations or secure laptops with encrypted drive.

Currently ‘R Studio’ is the analytical tool of choice within the Clinical Informatics Research Group. Subsets of the patient level databases are made available in the ‘Private R Studio Server’ (AnalysisServer1), or the ‘Public R Studio Server’ within the University network as appropriate by the SQL Developer to approved researchers. Access to the SQL server and to the Public or Private R Studio Servers is managed by the SQL Developer. Access to the SQL server and to the R studio servers are permitted only with explicit authorisation from the designated senior academic.

Staff members of the Research Group working within the Group’s Team base

- Access to the SQL server is restricted to the SQL Developer or approved staff members who have the expertise and authorisation to work with SQL databases.

- Employed and associated staff members of the Research Group working within the Research Group’s team base will access and analyse sub-sets of patient level data within the ‘Private R Studio Server’ (R Analysis Server) working from secure workstations or secure laptops with encrypted drive.

- Analysis of data in other formats or statistical packages, if required, will need to be discussed and approved by the Head of Department and/or designated senior academics.

All external researchers or staff of the Research Group working outside the Group’s Team base

Members of the Research Group sometimes need to work from home and our external research partners also need to access data from other research/academic institutions. The principles for remote access are documented in the Department’s Mobile Computing Policy. The procedures for data access and sharing are as follow: -

- Data, a subset of the database held in the secure server, is accessed remotely from the external facing analytical server, the ‘Public R Studio Server’ within the University network.

- Only pseudonymised data will be accessible remotely for members of Research Group or for external research partners. No patient identifiable information will be shared through remote access.

- Requests for accessing data by ‘bona-fide’ external research are managed by a three-layered process:
  - All requests for remote access to data must first apply for a University account IT using the ‘University IT Form 1b: Miscellaneous Account Registration Form’. Legitimate applications (including study protocol and analysis plan) are scrutinised and approved by the designated senior academic of the Department and authorised by the Faculty’s IT Services Manager.
  - All requests for remote access to data must apply for an account on the External Facing using the ‘Clininf-ServicesAccessForm v1.2’, which identifies the purpose and requirements for the access. Legitimate applications are signed-off by the senior academic and forwarded to the Faculty’s IT Services Manager for authorisation.
The Research Group’s SQL Developer will make available in the Public R Studio Server a subset of the data from the secure server meeting the approved requirements of the request, ensuring that no patient identifiable information is released.

The Faculty’s IT Services Manager maintains a record of requests and the Research Group’s SQL Developer reviews the requests periodically.

Students of the taught courses conducted by the Clinical Informatics Research Group

- All accepted students will be registered for a University IT account using the ‘University IT Form 1b: Miscellaneous Account Registration Form’.
- A subset of the data is extracted from a dataset appropriate for the teaching purposes of the course, ensuring that all patient, care provider, or study site identifiers are removed. Where appropriate, a further 10% of the cases in the subset are randomly removed to ensure that no GP practices or Clinical Commissioning Groups could be identified through matching of practice or locality population size.
- The anonymised data is made available in the ‘virtual desktop’ in a shared drive within the University’s network for the teaching sessions.

7. FORMS/TEMPLATES TO BE USED

- University of Surrey, University IT Form 1b: Miscellaneous Account Registration Form
- Clinical Informatics Research Group, University of Surrey, Request for accessing the Clinical Informatics services

These forms are available from the Designated Senior Academic on request.

8. INTERNAL AND EXTERNAL REFERENCES

Standard Operating Procedure for data access and data sharing aims to meet with the requirements of both the University’s internal standards and national standards in Information and Research Governance frameworks.

Internal References

- University of Surrey Information Security Policy, University of Surrey (2014) ([http://www.surrey.ac.uk/about/corporate/policies/information_security_policy.htm](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](http://www.surrey.ac.uk/about/corporate/policies/code_on_good_research_practice.pdf))
- Teleworking policy, University of Surrey ([http://portal.surrey.ac.uk/pls/portal/docs/PAGE/HUMANRESOURCES/EMPLOYMENT_INFO/COLLEGES/TELEWORKING_POLICY_0.PDF](http://portal.surrey.ac.uk/pls/portal/docs/PAGE/HUMANRESOURCES/EMPLOYMENT_INFO/COLLEGES/TELEWORKING_POLICY_0.PDF))
- Department Information Governance Policy, Clinical Informatics and Health Outcomes Research Group, Department of Clinical and Experimental Medicine at the University of Surrey
- Departmental System level security 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
9. CHANGE HISTORY

<table>
<thead>
<tr>
<th>SOP no.</th>
<th>Effective Date</th>
<th>Significant Changes</th>
<th>Previous SOP no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UoS Clininf SOP 2 V1</td>
<td>11/11/2013</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>UoS Clininf SOP 2 V2</td>
<td>31/03/2015</td>
<td>• Up-dated references &amp; links to University and Departmental policies</td>
<td>UoS Clininf SOP 2 V1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Up-dated procedures for analysis of data in other formats or statistical packages</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Up-dated the diagram for the Surrey Secure Network</td>
<td></td>
</tr>
<tr>
<td>UoS Clininf SOP 2 V2.1</td>
<td>30/04/2016</td>
<td>No changes other than extending the review date.</td>
<td>UoS Clininf SOP 2 V2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
**SOP no.** | **Effective Date** | **Significant Changes** | **Previous SOP no.**
---|---|---|---
UoS Clininf SOP 2 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 SOP 2 V2.1

---

**‘bona-fide’ research** is considered by the MRC 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 prepublishation 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.
A ‘bona fide’ researcher is a person with the professional expertise and experience to conduct bona fide research and a formal relationship with a bona fide research organisation that requires compliance with appropriate research governance and management systems.