

Introduction to SURE

Contents

1.	Introduction.....	3
2.	What is SURE?	4
3.	Aim and objectives of SURE	4
4.	Overview of the facility	4
5.	SURE operations and design.....	5
5.1	Logging on and authentication	5
5.2	SURE virtual computing “desktops”	5
5.3	Transferring files into and out of SURE	5
5.4	Data storage and archiving	5
6.	Staffing and support services.....	6
6.1	Staffing.....	6
6.2	Support services.....	7
7.	Further information.....	7

1. Introduction

This guide has been developed to provide introductory information on the Secure Unified Research Environment (SURE) including:

- Objectives of SURE;
- Design and security features; and
- Staffing and support services.

Information provided in this guide may support researchers to prepare research grant applications and human research ethics applications. It will also be useful for other individuals who are interested in further information on how SURE works.

The Secure Unified Research Environment (SURE) is a secure computing environment that has been purpose-built for analysis using linked health and health-related data. SURE was established with funding from the Australian and New South Wales Governments. It was officially launched in Sydney in July 2012.

The SURE facility is now fully operational and is already hosting a significant number of research projects, including several using linked jurisdictional and Commonwealth data. The SURE team at the Sax Institute is fielding an increasing number of enquiries from researchers around Australia who want to undertake research using data from multiple Australian jurisdictions. Accordingly, we are working with data linkage units in states and territories to distribute information about the SURE facility to stakeholders, including data custodians and human research ethics committees.

Each research study within SURE is discreet and only the researchers listed on the ethics approval and data custodian approvals have access to that studies datasets. The Sax Institute team managing the study spaces do not have access to datasets within the study space where the research teams carryout their analysis. Curation takes place within the curated gateway which is a discreet staging space for all files inbound and outbound to a specific study.

Sax Institute staff do not have access to the datasets within SURE unless they are actually part of a study with full data custodian and ethics approvals. All data is kept at arm's length by the Sax Institute through our policies, procedures and confidentiality agreements signed by all staff.

The system administrators who manage the SURE system can access the study spaces but the only time they would access a SURE study space is for repair and file recovery purposes at the request of an investigator. There are significant checks and balances when this is done through our operational policies and procedures.

Please find enclosed a fact sheet that provides information about the design and features of the SURE facility and some of the benefits it provides in terms of security, performance and fostering research collaboration. Additional information can be found on the SURE website, <http://www.saxinstitute.org.au/our-work/sure/>.

2. What is SURE?

SURE has been developed by the Sax Institute as part of the Population Health Research Network (PHRN). The PHRN was established with funding from the National Collaborative research Infrastructure Strategy to create infrastructure that will facilitate population health and health services research across all jurisdictions in Australia, with an emphasis on the use of linked health data. Further information on the PHRN can be found at <http://www.phrn.org.au>.

SURE is a remote-access computing environment that allows researchers to access and analyse linked health-related data files for approved studies. The remote environment is accessible over encrypted Internet and AARNet connections, replacing a user's local computing environment.

3. Aim and objectives of SURE

Consistent with the goals of the Sax Institute and the PHRN, SURE aims to facilitate research to support health decision making, improve health outcomes and enhance the delivery of health care services in Australia.

The objectives of SURE are to:

- i. Supply a computing environment with enhanced security that substantially increases researchers' ability to protect the confidentiality and privacy of research data;
- ii. Increase the accessibility of research data to researchers undertaking population health, health services and related research and make collaboration between researchers from different institutions in the use of these data easier and more efficient;
- iii. Give researchers access to research data in a stable corporate computing environment with enhanced speed, storage and cutting-edge analytic software and tools.

4. Overview of the facility

A project workspace, which houses virtual computing "desktops" for one or more researchers, is established for each research study hosted by SURE

If a researcher is part of more than one study in SURE, the virtual computing "desktops" are logically separated from each other and cannot interact or share data in any way. Each project workspace has an area of shared file storage that all researchers working on a project can access.

The SURE facility incorporates a range of information security controls relating to the access, storage and transmission of data, including:

- Access to SURE is strongly authenticated and requires a username, password and use of one-time access codes provided by an authentication token issued to SURE users.
- Data is stored centrally on servers housed in a secure data centre. No data is stored on a researcher's local computing environment except where already permitted by the data custodian.
- The only way for a file to enter or leave SURE is via the Curated Gateway. All inbound and outbound files are subject to review as they pass through the Curated Gateway before they can be accessed within the SURE facility or downloaded to a user's local computing environment.

Further information on the operations of SURE and its security measures is provided in subsequent sections of this guide.

5. SURE operations and design

5.1 Logging on and authentication

To access SURE, a user name, password and one-time access code provided by a physical token (Yubikey) are required. Users need access to a reliable broadband internet or AARNet connection. All Australian universities are connected to AARNet.

5.2 SURE virtual computing “desktops”

A user views a facsimile of the screen of their remote virtual computing “desktop” on their local computer screen. SURE virtual computing “desktops” are powerful, highly-specified Microsoft Windows 7 Professional desktops furnished with a range of proprietary and open-source data manipulation and analysis software, including popular tools such as SAS and Stata, which are made available based on a user’s analytical requirements.

Within the SURE facility, users have access to a comprehensive suite of analytical tools but there are strong security controls to protect the privacy and confidentiality of data files. Within SURE, a user cannot access the internet or email, there is no print function and there is no ability to copy data to USB memory sticks or other removable media. Disabling these functions minimises the risk of losing appropriate control over custodian-approved research data. All files move into or out of SURE by passing through the Curated Gateway.

5.3 Transferring files into and out of SURE

The only way for a file to enter or leave SURE is via the Curated Gateway which is a secure application specifically developed for the SURE facility. All inbound data files uploaded to the Curated Gateway for use in SURE are reviewed by a member of the SURE operations team for compliance with ethics committee approval and data custodian requirements. Files other than data files are reviewed by the study’s chief investigator or an alternate senior investigator prior to being accepted for use in SURE. Outbound files uploaded to the Curated Gateway for use outside of SURE are reviewed by the study’s chief investigator or an alternate senior investigator.

The Curated Gateway can support alternative approval workflows and other parties may be involved in the review of inbound and outbound files passing through the Curated Gateway to enter or leave SURE if required for particular studies.

To minimise the risk of unauthorised access and attacks, files are scanned at multiple points with anti-virus software as they pass through the Curated Gateway and prior to storage within the SURE facility. The facility is protected by three layers of perimeter firewalls, as well as firewalls between each project workspace.

All files that pass through the Curated Gateway are logged and may be subject to audit by the SURE team.

5.4 Data storage and archiving

SURE is hosted in a tier-3+ (i.e. most secure available) data centre in Sydney that is also used by some of Australia’s leading telecommunications, government and financial institutions. The data centre is a member of the Australian Government Data Centre Facilities Panel. SURE servers are housed in dedicated, locked cabinets. Premises-wide security measures include 24 hour staffed security surveillance, intruder resistance at all levels and strict physical access controls including access control lists.

Regular backups of data stored in the SURE facility are made using 2 processes. Firstly, disk-to-disk backups are made at the SURE facility. Additionally, data is copied off in encrypted form to tapes that are rotated off-site. Data taken off-site is strongly encrypted using 256-bit Advanced Encryption Standard and stored in a secure facility.

After a research study is completed, files stored for that project workspace will be archived to tape and/or optical disk (depending on the size and quantity of files that need to be archived) and stored at a secure facility in an encrypted format. These will be retained for the period nominated on the project workspace registration form for each study. Restoration of a project workspace from its archived state can be requested and performed at a cost. Research outputs and other artefacts may be able to be retained by researchers as well as archived. Requests for restoration by researchers must be made prior to the end of the SURE retention period.

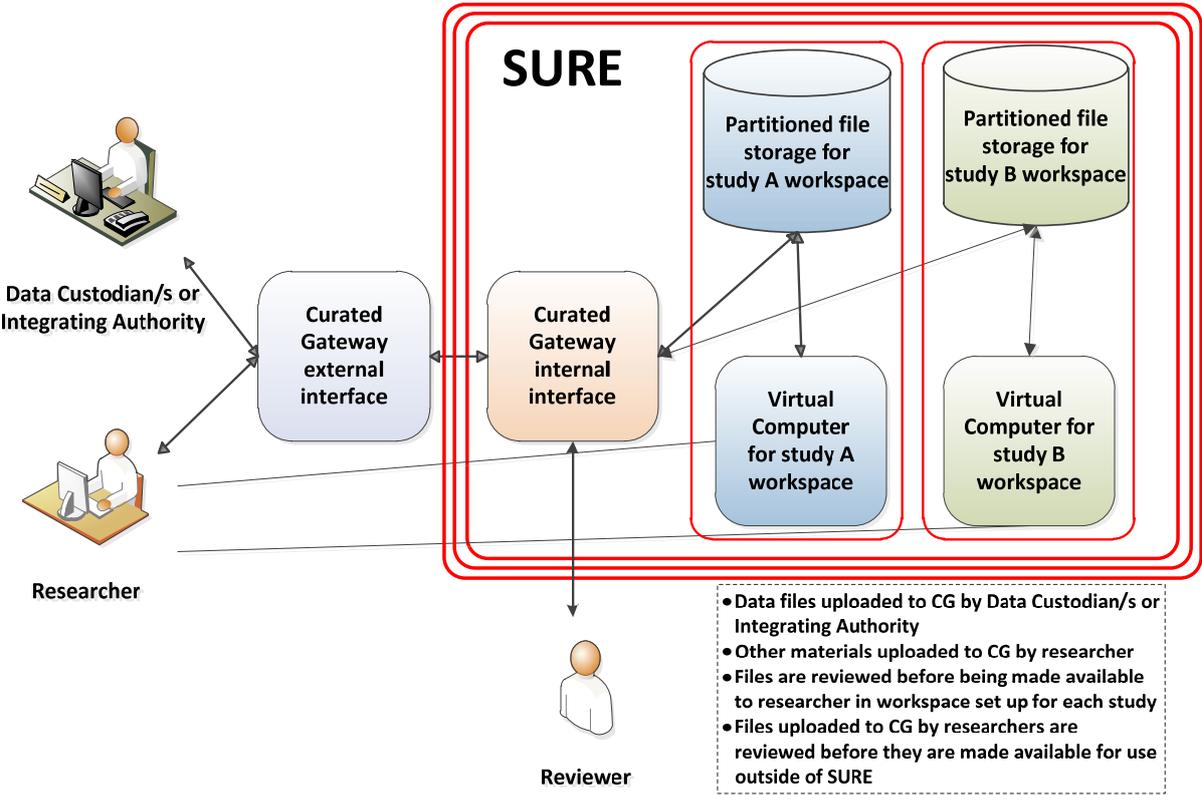


Figure 1. Diagram of operational model for researcher accessing SURE for two studies
 (Note: An Integrating Authority may be involved in the provisioning of data for projects involving Commonwealth data, for more information view the [National Statistical Service website](#).)

6. Staffing and support services

6.1 Staffing

A small staff team is responsible for performing administrative and technical activities necessary for the operation of SURE. Staff are subject to security checks prior to employment and are bound by non-disclosure agreements. While employed, staff members are required to comply with all Sax Institute policies and procedures relating to privacy, security and responsible research conduct and will undertake ongoing training including privacy training. Contractors may be engaged to perform specific tasks and will be subject to checks similar to Sax Institute employees prior to engagement. Duties undertaken by contractors are closely supervised and managed by SURE team members.

In performing system administration tasks on the SURE facility, SURE team members may necessarily have access to research data files but will not have the authority to examine or use the data in any way. An exception to this policy is the team members who may undertake review of research data files passing through the Curated Gateway. As detailed above in section 5.3, file review activities may be undertaken by SURE team members as part of specific study requirements to check compliance with ethics committee approvals and data custodian requirements.

Within the Curated Gateway, the processes for uploading, downloading and reviewing inbound and outbound files are separate so that even though a SURE staff member may be reviewing inbound or outbound files, they have no ability to download files from the Curated Gateway into the SURE facility or out of SURE. The SURE staff member reviewing files for each research project workspace is subject to the same restrictions as a SURE user including not having the ability to transfer any data between project workspaces.

A log of all actions taken on files passing through the Curated Gateway will be kept, including the activities of the SURE staff member who may be undertaking review activities. Copies of files passing through the Curated Gateway are kept to enable later audit for the life of the project workspace.

6.2 Support services

The SURE operations team will respond to queries and provide support for the infrastructure being provided as part of the SURE facility including:

- Using the Curated Gateway to transfer files in or out of SURE and the Citrix Access Gateway for logging into SURE;
- Virtual computing “desktops” established for SURE project workspaces.

Study-specific support will not be routinely provided by the SURE team in areas not related to the operation of the SURE infrastructure including, but not limited to:

- Data analysis, programming and research practices; or
- Use of software programs offered in the SURE environment (e.g. Microsoft Office and statistical analysis packages).

However, within the SURE workstation, the SURE Internal Wiki <http://in2.sure.local> contains configuration resources where information relating to your analysis software may be published.

7. Further information

The SURE team would be happy to answer your specific questions about the SURE facility. Please contact the SURE Administrator on sure-admin@saxinstitute.org.au or 02 9188 9561 if you would like to discuss any aspects of SURE, or arrange an information session.

For more information on any of the issues included in this guide, visit the SURE website at www.saxinstitute.org.au/our-work/sure.