SURE: the secure unified research environment

A gateway to better health systems using the power of linked data

Australia has one of the world's most comprehensive collections of population-based health data but its potential is yet to be realised. SURE is a high-powered computing environment developed to help overcome these barriers to making best use of our national knowledge base.

It has been purpose-built as Australia's only remote-access data research laboratory for analysing routinely collected health data. It offers data custodians a secure vehicle for making datasets available to researchers.

HOW DOES SURE WORK?

Each accredited researcher is allocated a virtual computer, which runs entirely on hardware physically located at and controlled by SURE. Researchers see a facsimile of the remote virtual computer screen on their local screen. This eliminates the need for them to use their local computing environments, which may have technical and security limitations. SURE's high-performance computing environment provides enhanced speed, storage and cutting-edge analytic software and tools.

OUR APPROACH TO INFORMATION SECURITY

Our planned, documented and comprehensive approach to managing information security includes:

- Defining requirements for managing information security through exhaustive risk analysis
- Implementing controls in relation to people, technology and processes
- Continuous monitoring and review.

SECURITY FEATURES

Strong access authentication

Users must undertake training in privacy, ethics, statistical disclosure control and information security. Complementary deeds of agreement with individual users, institutions (researchers' employers) and data custodians cover data security and breach management. Third party partners enter into contractual arrangements to ensure compliance with the security standards and procedures required for SURE.

Physical security

SURE is hosted in two physically separate tier-3+ data centres in Sydney (the highest possible level) that also service some of Australia's leading telecommunications, government and financial institutions. The data centres are members of the Australian Government Data Centre Facilities Panel, have strict access controls and continuously staffed surveillance. No data are stored on a researcher's local computer or in their institutional computing environment.

Data security

All files entering or leaving SURE must pass through a purpose-built portal called the Curated Gateway – the control point for all information flow in and out of the facility. Both inbound and outbound files are reviewed to ensure they are consistent with ethics and data custodian approvals and are appropriately anonymised.

The original dataset provided by the custodian is not allowed to leave SURE. Data custodians can request that they prospectively review all or samples of the research output material leaving SURE, to assure compliance with this restriction. Copies of all inbound and outbound files are kept and all file movement activities logged to allow periodic audits to be undertaken.

Within SURE, a user cannot access the internet, email, print or copy data to a USB memory stick or to other removable media.

After a research study is complete, data files are digitally archived in encrypted form and retained in secure storage for the period required by the researchers and data custodians before being destroyed.

Computer and network security

Security is enhanced by rigorous partitioning within SURE of project and study workspaces, ensuring complete separation of each study and its associated data from all others. Three separate firewalls plus VLANS mediate this internal network separation. Intrusion detection and log monitoring systems are in place to detect and prevent potential attacks and maintain data integrity. The entire SURE system runs behind a three-layer firewall with both physical and logical separation of DMZs. Changes to the IT environment are assessed for information security risk before being implemented.

Users are issued with strong, confidential passwords that adhere to SURE guidelines. They are unable to change the passwords themselves. They must also use a physical authentication token for security protection, similar to those used by many banks. Client digital certificates issued by the SURE team must also be installed on each computer used to access SURE.

Incident management

Users must report information security incidents and undertake other actions as directed. SURE staff will investigate information security incidents according to documented protocols and provide timely communication on any security-related service disruptions.

Business continuity

Business continuity and disaster recovery plans are in place and comprehensive backup and restoration processes are in place and regularly tested. All off-site backups and archival data are encrypted before being transferred to secure off-site storage. For users of SURE in academic environments, network access is via the dedicated AARNet research network, rather than the internet.

Breaches and infringements

Breaches or infringements will be investigated as outlined in SURE agreements, which are consistent with the Australian Code for the Responsible Conduct of Research and the Australian Privacy Principles.

WHO IS BEHIND IT?

SURE has been developed by the Sax Institute, a non-profit organisation whose mission is to improve health and wellbeing by driving the use of research in policies, programs and services. The SURE project is part of the Population Health Research Network (PHRN) which is working across the states and territories to develop national health data linkage infrastructure.

FOR MORE INFORMATION

Please contact a member of our team to discuss how SURE can meet your needs as a data custodian.

E sure-admin@saxinstitute.org.au
T 02 9188 9561
W www.sure.org.au

SURE
Secure Unified Research Environment