SDHS Security Policy v5.3, revised March 2015

The SDHS Security Policy is reviewed annually by the Council of the School - the policy presented here was approved in March 2015. Interim revisions may be made by CSCS and the IGO in response to the individual requirements after a risk assessment.

1. Overview

The purpose of this security policy is to outline the Clinical School's Secure Data Hosting service (SDHS) and general working practices in handling sensitive data. The SDHS is designed to ensure that highly sensitive information, required by research groups at the Clinical School, is secure from unauthorised modification or disclosure, either accidental or deliberate and that the storage of this data complies with all required regulations.

It has been developed, implemented and managed by the University of Cambridge.

It is for use by Clinical School research groups.

Authorisation to use the service is provided by the Information Governance Officer (IGO).

Queries on School Policy for existing studies must be addressed to the Information Governance Office (currently Caroline Edmonds, Carolyn Read)

The IT infrastructure is provided by the Clinical School Computing Service (CSCS).

The policy structure has been agreed by the Cambridge University Data Protection Officer and the Addenbrooke's (Cambridge University Hospitals NHS Trust) Data Protection Officer.

All data is managed in accordance with the Data Protection Act 1998. The University of Cambridge is registered under the Act, registration number Z6641083.

The standard CSCS Acceptable Use Policy is applicable to the SDHS

The Security Managers (SMs) within CSCS are the Head of Department and his nominated deputies in the CSCS Management Team. They are responsible for ensuring that all operations undertaken by CSCS staff on the SDHS are in accordance with this Policy.

The identities of the SMs will be recorded in the service documentation.

Each research group using the SDHS will require an authorised Chief Investigator (CI), who:

- Must be an employee of the School of Clinical Medicine.
- Approves a Data Manager (DM) for a study.

- Acts on behalf of, or appoints a replacement DM, if the original DM is not available.

Each research group using the SDHS will require an authorised Data Manager (DM), who:

- Is the recognised point of contact between the Research Group and the IGO in the area of confidential data.
- Is the recognised point of contact between the Research Group and CSCS in the area of confidential data.
- Is responsible for ensuring the working practice of the study conforms to this Policy.
- Is responsible for requesting any desired exceptions to this Policy.

2. Applications for existing studies

Applications for existing studies must be reviewed and approved by the IGO before being passed to CSCS for consultation.

CSCS will consult with the study team to ensure that the study team's working practices can be migrated to the SDHS.

CSCS will report to the IGO if there are concerns arising from the consultation.

CSCS will give written confirmation upon successful implementation of the SDHS.

3. Applications for new studies

Applications for new studies must be approved by the IGO before being passed to CSCS for implementation.

CSCS will report to the IGO if there are concerns arising from the implementation.

CSCS will give written confirmation upon successful implementation of the SDHS.

4. Clarifications and exceptions to Policy

If the DM or CI believes a study's working practice is inadvertently or unjustly impacted by the technical implementation of this Policy, they may make a written request clarification from the SM.

It will be decided by the SM whether the implementation is appropriate to the Policy.

If judged inappropriate, CSCS will review the implementation with the IGO

Any alterations to the implementation will be recorded in the Exceptions Log (EL).

If decided appropriate, the SM / CI may decide to request an exception to the Policy.

Exceptions to the policy will be decided upon by a member of the SM and a member of the Information Governance Office.

Any exceptions to policy will be recorded by the SMs in the EL.

The Exceptions Log will be reviewed as part of the next SDHS review to determine if this Policy requires amendment.

SDHS System Design

5. Authentication to the SDHS

Authentication and access to the SDHS is provided via unique, individual University user accounts. These accounts are managed by CSCS.

A research group requiring access to the SDHS must be first authorised by the IGO, who will provide written authorisation. The CI / DM will then contact CSCS. CSCS staff are not permitted to add new groups to the SDHS without this authorisation.

Changes in access to the SDHS, e.g. a new member of staff requires access for an existing research group, must be authorised by the DM or CI. CSCS will only accept instructions to carry out the changes from the DM or CI.

Access into the SDHS must only be done by CSCS approved methods (see technical design for details). Circumvention of these methods using other services is forbidden.

6. Data Storage within the SDHS

All personally identifiable research data should be stored within the SDHS.

The decision to designate research data as appropriate for the SDHS is done by the CI / DM in conjunction with the IGO. CSCS will not provide advice in these decisions.

Anonymised data should be located on the normal data storage but it is expected that for practical reasons, some anonymised data will be stored in the SDHS.

CSCS is responsible for the provision of data storage within the SDHS. Storage is logically allocated to research groups as requested.

CSCS are responsible for setting security permissions so that research staff may have access into group-level storage areas.

Within a group-level storage area individual file permissions are managed by the DM.

CSCS will assist the DM where required.

The permissions of CSCS must not be altered or removed.

Patient identifiable information should be separated from research data and a link only made where clinically important information needs to be passed to a participant or their doctor.

In limited circumstances sensitive data may be temporarily stored on a computational server also attached to the SDHS network. This is done only as part of an agreed working procedure specific to the research study.

7. The SDHS network

The SDHS is a logical vlan, not a separate physical network.

The extent of the SDHS vlan will be minimised wherever possible to reduce the security risk.

Devices added to the SDHS vlan must be authorised by CSCS.

The SDHS vlan is protected by a firewall which restricts access into and out of the SDHS. The firewall is managed by CSCS.

Firewall rules are approved by the CSCS in consultation with the Information Governance Office.

Web filtering is applied to the SDHS network such that websites that represent a security risk are not accessible.

8. Computer Access

Only approved access methods can be used with the SDHS.

CSCS provides a browser-based remote virtual computer to access the SDH Network. This is the default method of access for all users.

It is not necessary for the local computer to be managed by CSCS, however;

- The user should ensure they have a private workspace when viewing PID.
- The user should be sure that the computer has up-to-date security (OS patches, anti-malware, etc) as any malware infection increases the chance of data loss, e.g. by screen capture, keystroke capture.
- Data cannot be transferred from the virtual computer to the local computer.

If limitations inherent in remote working are deemed to hinder or prevent a user from performing their work then a consultation with CSCS to determine possible workarounds will occur.

If a computer needs to be connected directly to the SDH network to perform data analysis, then this will be considered a workaround and entered into the risk / exceptions log.

For all workarounds, a, CSCS, the IGO and the CI / DM will determine a new working practice that is achievable using remote access and agree a timescale for adoption.

9. Data Flows in and out of the SDHS Network

Data must flow in and out of the SDH Network by approved methods only. These include NHS email, encrypted media and the SDHS Transfer server and printing via the CSCS print server.

Data that has been anonymised by study co-ordinators can be published onto the standard Clinical School IT infrastructure for access by researchers for normal analysis.

There will be no direct access between the SDH network and the standard network.

Publishing to the standard network must be via a gateway server (SDH Transfer server or the Cerberus SFTP server) to reduce the risk of accidental publishing of PID.

There will be no internet access from the SDH Network, except for approved data sources.

Approved data sources currently include:

- *NHS.net*
- https://www.surveymonkey.com/
- https://sdhstransfer.medschl.cam.ac.uk

From SDH Workstations, sensitive data will only be copied onto removable media once it or the media is encrypted as per this Policy. Removable media that does not meet the encryption requirements will be blocked.

CSCS will manage secure mechanisms for initial data imports into the SDHS.

10. Restrictions on the use of Remote Access Virtual Computers

By default there is no internet access from the virtual computers.

Printing from the virtual computers to locally connected printers is not possible.

Printing is possible via CSCS-managed print servers to on-site network printers only.

You must nominate required printers during the application process, or subsequently in writing.

Printers used to print PID must be suitably private and have appropriate policies governing their use.

Data cannot be moved or copied between virtual computers and local computers; this includes files, clipboard data, screen captures or video / audio recordings.

A limited number of applications are available in the Citrix environment. Applications must be approved and published to the Citrix environment; not all applications are suitable. If you would like an application included, you should submit a request to the CSCS helpdesk.

Applications must be suitable for the Citrix environment, as judged by a member of the Server Team.

Applications must be judged suitable for use with PID, as judged by the SMs.

Access to Virtual Computers requires two factor authentication; CSCS provide a network security fob for this purpose.

Virtual Computers will lock after 10 minutes of inactivity, and will require re-authentication to unlock.

Local computers that are left unattended should be physically secured, e.g. by Kensington lock.

11. Restrictions on workstations directly attached to the SDHS (SDH Workstations)

Computers directly connected to the SDH network will have the following internet restrictions:

Internet access is restricted, with the following services, as defined by the firewall, restricted:

- *Botnet*
- *File Sharing*
- *Proxy*
- *Game*
- *Remote Access*
- *Peer to Peer*

Website access to the following categories is filtered to prevent access to websites that present a security risk:

- *Child Abuse*
- *Proxy Avoidance*
- *Malicious Websites*
- *Phishing*
- *Spam URL*

- *Pornography*
- *P2P File Sharing*
- *Dynamic Content (URL shortening sites)*
- *Website access to the following categories will display a warning highlighting the above average risk:*
- *Explicit Violence*
- *Social Networking*
- *Online Storage*

CSCS approved anti-virus must be present and active on each directly attached workstation.

Appropriate O\S and application patching must be applied. CSCS manages patches for Windows, OSX, Ubuntu and applications. For a specialist O\S, such as Sun Solaris, it may be managed by the research group as part of an agreed working procedure specific to the research study.

Workstations attached directly to the secure network may be refused connection if the O\S and application patches have not been successfully applied.

Workstations attached directly to the secure network will be subject to restrictions that prevent them from installing or running software that presents a security risk.

The following application categories, as defined by CSCS anti-virus solution Sophos, will be prevented from running:

- Browser plug-in
- Distributed computing
- Download managers
- File sharing application
- Game
- Jailbreak Software
- Mobile Synchronization
- Online storage
- Password / license recovery tool
- Pranking Software
- Privacy tool
- Proxy / VPN tool
- Remote management tool
- Screen capture tool
- Software updater
- Telnet client
- Toolbar
- USB Program launcher

Individual exceptions may be requested by the CI or DM, and will be decided by the SMs, and recorded in the EL.

Workstations will lock after 10 minutes of inactivity, and will require re-authentication to unlock.

Workstations that are left unattended should be physically secured, e.g. by Kensington lock.

12. Administrator Rights and Software Installation

Users will not have administrative rights over any computer attached to the SDH network.

If users wish to install software on their SDH workstation, they must request that the CSCS Service Desk perform the installation.

CSCS Service Desk will not install any software they believe to be inappropriate for an SDH workstation.

The Helpdesk will use the existing blocked categories as the basis for their decisions.

Either the Service Desk of the DM may request clarification on suitability from the SMs

Final decision on which applications are appropriate rest with the SMs.

13. Drive Security

Computers that will be used as SDH workstations require the boot drive to be encrypted, using Bitlocker for Windows, and a suitable alternative for other platforms.

Computers will be reinstalled with a version of Windows that supports Bitlocker (Ultimate or Enterprise), with any costs payable by the user.

CSCS will retain a copy of the decryption key for data recovery purposes.

14. SDH Workstation Security Requirements

Workstations intended for the SDH network will be subjected to full security audit by CSCS prior to migration.

Only computers installed running approved Operating systems will be allowed on the SDH network. Currently the approved list is:

- Windows 7, Enterprise or Ultimate
- Ubuntu 12.04

Previous versions of the listed operating systems are not permitted. Other operating systems considered upon request.

Workstations will lock after 10 minutes of inactivity, and will require re-authentication to unlock.

15. Remote Workstation Security

A limited number of applications are available in the Citrix environment. Applications must be approved and published to the Citrix environment; not all applications are suitable. If you would like an application included, you should submit a request to the CSCS Service Desk.

Applications must be suitable for the Citrix environment, as judged by a member of the Server Team.

Applications must be judged suitable for use with PID, as judged by the SMs.

Remote workstations require two factor authentication; CSCS provide a network security fob for this purpose

Workstations will lock after 10 minutes of inactivity, and will require re-authentication to unlock.

Workstations that are left unattended should be physically secured, e.g. by Kensington lock.

16. Emails

University email systems should not be used to send PID. The SDHS Transfer Server is provided to fulfil this function.

The NHS.net email system is designed to handle sensitive data and should be used wherever possible if staff have access to an NHS.net email account. It can be used to receive and send sensitive data to any appropriate source or destination under the terms of the research project. It is accessible from within the SDHS.

Consenting volunteers may email their own information to a Clinical School email address providing prior agreement has been arranged under the terms of the research project.

Sensitive data stored as plain text in emails should be recorded appropriately by the researcher, before being deleted and expunged.

Emails containing patient identifiable data must not be copied, or saved, from the University email systems onto personal data storage (e.g. laptop, USB stick or a mobile phone).

Received email attachments containing patient identifiable data must be removed – either deleted or saved to the Secure Data Storage.

17. Sharing data files with collaborators outside of the Clinical School

The distribution of data files, containing sensitive information, to external collaborators can only be performed using the provided secure website.

An individual area of the website will be supplied for each specific study. It will include a simple level of customisation (e.g. description, contact details). It is a functional website, rather than an information website.

Data files may be sent to, or received from, collaborators using the secure website.

Data files sent to a collaborator must be individually encrypted. The password\key for decryption must be supplied to the recipient via a separate email, letter or telephone conversation. They must not be left on the website.

Accounts for external collaborators are set up by CSCS on request of the DM. They can be granted permission to download files from the Clinical School, upload files to the Clinical School, or both.

Data files left for downloading by collaborators should be removed from the website as soon as possible after being downloaded. Data files older than a set age will be automatically removed from the web site whether they have been downloaded or not.

Data files uploaded to the website will be automatically checked for viruses. The files can then be moved to an appropriate data store.

A default storage size will be set for each study. This can be increased on request. The website should not be used as a permanent data store, data files on the website will not be backed up.

There will be a default maximum size for individual files. This can be adjusted on request.

Collaborators should only decrypt PID to an NHS IGT certified 'Safe Haven'.

18. **Password Policy**

A separate password policy shall apply to all users of the SDH service, either via SDH workstation or Citrix remote access

The policy will differ from standard CSCS policy as follows:

Minimum password length is increased from 8 to 14 characters.

Password history is enabled, with a setting of 1 (users cannot reuse the same password consecutively, but can reinstate a password following IT reset).

The lockout threshold is reduced from 5 to 3.

The lockout timer is set to 20 minutes.

All users of the SDH Service are required to change their password upon joining the service.

19. **Methods of Encryption**

Sensitive data may be protected by encryption at the file or drive level.

256bit AES is the minimum standard of encryption to be used in all cases.

CSCS will manage Bitlocker implementations for all PCs used as SDH workstations.

CSCS will store recovery keys for its managed Bitlocker installations.

It is the user's responsibility to use appropriately complex encryption keys.

It is the user's responsibility to memorise the encryption keys as loss would render the data unrecoverable.

If Keys do need to be recorded they should be stored within a utility that protects them with a master password, such as KeePass.

20. System Protection

All electronic data is regularly backed up to an off-site mirror (see technical details).

Physical access to the SDHS file-storage and servers is protected by the use of swipe cards or code lock, with only approved staff having unsupervised access.

21. System Audits

The CI / DM must inform the IGO and CSCS of employees that should be removed from the SDHS service.

CSCS reserves the right to remove user's access if the CHRIS system indicates they have left the University.

CSCS will audit the group storage areas to ensure that access is limited to the correct individuals.

22. SDHS Risk Assessment

The SDHS design shall be risk assessed every 12 months.

The Exceptions Log will be reviewed as part of the risk assessment.

CSCS will arrange penetration testing of the SDHS by a third party to verify its effectiveness

A retest will be arranged following any significant change to the service.