**System Level Security Policy (SLSP) [version2, 08/09/2010]**

**For participant identifiable information obtained in the SABRE Study**

**PI: Professor Nish Chaturvedi**

**International Centre for Circulatory Health,**

**Imperial College London,**

**59-61 North Wharf Road,**

**London W2 1LA**

**System Details**

1. The System shall be known as SABRE Administration Database
2. The System’s responsible owner shall be Therese Tillin ([t.tillin@imperial.ac.uk](mailto:t.tillin@imperial.ac.uk), tel: 020 7594 3396)

The System’s Data Controller shall be Richard Mattin (Data Protection Coordinator for NHLI Division & Information Systems Security Policy advisor) ([r.mattin@imperial.ac.uk](mailto:r.mattin@imperial.ac.uk), tel: 020 7594 3122)

**System Security**

1. Security of the system shall be governed by the corporate security policy of Imperial College London (<http://www3.imperial.ac.uk/secretariat/policiesandpublications/informationsystemssecurity/policy>)

Imperial College’s Information System Security Policy and associated Codes of Practice were developed using ISO 17799 for guidance.

The College has a Data Protection Policy to protect the personal information processed by, or disclosed to, staff or students of the College or other authorised persons. The Policy also has accompanying Codes of Practice and Guidelines. Those of relevance to clinical research include:

Code of Practice (2) Handling of Patient Data <http://www3.imperial.ac.uk/secretariat/policiesandpublications/dataprotection/codesofpractice/cop2handlingofpatientdata>

Guideline (4) Use of Personal Data in Research <http://www3.imperial.ac.uk/secretariat/policiesandpublications/dataprotection/guidance/guide4research>

1. The System’s responsible security manager shall be Daniel Key ([d.key@imperial.ac.uk](mailto:d.key@imperial.ac.uk), (Sabre Study Data Manager, Information Systems Officer) <tel:020> 7594 5946)
2. The security manager duties shall include:
3. Setup and implementation of system.
4. Staff training (use of system, security and confidentiality awareness).
5. Security auditing.
6. Secure data erasure of digital person identifiable information at the end of the study and storage of a minimum identifiable dataset (fullname, sex, ethnicity, date of birth, NHS number, first line of address, postcode) encrypted using AES 256 encryption in order to enable future follow-up of the cohort.
7. The System shall incorporate the following security countermeasures:
8. The system is housed on the third floor of a secure building (59-61 North Wharf Road, London W2 1LA) where two swipe-card locks must be passed to gain access. Access to the building is limited to those employees of Imperial College London and Imperial College Healthcare NHS Trust who are staff members of the |nternational Centre for Circulatory Health, all of whom are contractually bound to confidentiality (which extends after employment ends)

The building is open plan on each floor level. The stand-alone PC system is located in an area of the third floor which is dedicated to the SABRE study research team. Only those members of the study team named in section 18 are able to access the password protected SABRE Admin stand-alone PC system.

Standard Windows XP access control is used to prevent use of the machine by anyone other than members of the SABRE team. The system’s two machines are networked only to each other and have no interface with either the University’s network or the internet.

Each SABRE team member has a user account with passwords conforming to the Windows XP Complexity requirements (<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/504.mspx?mfr=true)m>) and a security policy will be set requiring it to be changed every 60 days.

1. All Patient Identifiable Information will be held inside TrueCrypt (AES 256) containers with a password known only to the study team, both on the computer hard drive and when removed for backup on a USB thumb drive.
2. Paper records are held in locked cabinets in the same building area as the stand-alone PCs. Keys to these cabinets are locked within a desk unit to which only the Sabre study team have access.
3. All authorised users are fully trained in Good Clinical Practice.
4. All authorised users are contractually bound to confidentiality (which extends after employment ends)
5. Authorised users who are engaged in data collection from primary care medical records have signed honorary confidentiality agreements with the relevant primary care trusts and GP practices.
6. Imperial College's Information System's Security Policy statement is given to all new members of staff. Failure to comply with the policy may lead to instigation of disciplinary procedures.
7. Only the chief investigator, one co-investigator (Therese Tillin) and the study data manager (Daniel Key) are able to export identifiable data from the Admin PC (encrypted, for backup purposes only).

**System Management**

1. The System is provided by Daniel Key, SABRE Team IS Officer.
2. The System shall be implemented and maintained by Daniel Key and the Imperial College ICT department, who will provide equipment repair and replacement where appropriate.
3. The System shall not be shared or used by any other organisation.

**System Design**

1. The System shall comprise two PCs networked only to each other and to a printer.
2. The ‘Admin PC’ hard drive contains an Access ‘Admin’ database which contains all patient identifiable information and a ‘Results’ database which contains pseudonymised study results.
3. The ‘Results PC’ is connected directly to the ‘Admin PC’ via Ethernet cable and given access to the Admin database via Windows (SMB) file sharing.
4. Paper records**.** Each participant who attends the SABRE study clinic or who completes a follow-up questionnaire has a paper folder containing these records. Identifiers included in the folder are study ID number, the consent form(s) which include(s) the participant's name, blood test results and ECGs, which also include the participant's name and study ID number. HES data or cancer registrations will not be included in these paper folders. These folders are held in locked cabinets in the same area of the same building as the stand-alone PCs. Keys to these cabinets are locked within a desk unit to which only the Sabre study team have access.

**Operational Processes**

1. Encrypted data received from HES and the Cancer Registry will be received in electronic format and will be electronically merged with existing study data on the basis of NHS numbers, dates of birth, sex and dates of death within the Admin database housed within the Admin stand-alone PC as described above. Records will be individually checked against the study baseline data, using NHS number as the primary merge field, to ensure that names, ethnicity and postcode (where available) provide confirmation of a true match for each participant. Pseudonymised study data collated from other sources (e.g clinical measurements) are subject to rigorous data checking procedures including independent checking of 10% of case report forms, plus random checks of data entry accuracy and data range checks.
2. Participant identifiable data is derived from the baseline dataset (provided to the study team by participants at the time of the baseline studies 1988-19). These data include names, dates of birth, sex, ethnicity, NHS numbers. The NHS tracing service was used in 2008, and a further tracing using the NHS batch tracing process was conducted in 2010, to identify current participant addresses and GP details. These tracing processes were conducted by The Information Systems Department at Imperial College NHS Trust, with both ethical and Caldicott approvals. Data from NHS tracing processes were transferred to the stand-alone Admin database PC by Therese Tillin using an encrypted USB thumb drive, which was immediately erased following transfer. AFD Address Management Software is used to attempt to identify current addresses of those for whom the NHS tracing processes have not returned a current address. This tracing is conducted on a password protected standalone PC, situated adjacent to the Admin database PC; any retrieved addresses are manually entered onto the Admin database. Address searches using AFD Address Management Software are conducted by the members of the study team named in section 18; these searches are not recorded or stored on the PC.

The data will be stored in a Microsoft Access 2007 database on a physically and logically secure local network (described above). AES-256 encrypted copies are taken for remote backup and ‘Results Database’ data (no identifiable information) is copied off the system for analysis. Identifiable data will be transferred only from secure systems to the ‘Admin PC’ via thumb-drive which is afterwards erased. All portable media used for data transfer are encrypted.

1. At the end of the current 20 year follow-up study, paper records will be archived in secure Imperial College managed archives. Only archive staff or the study PI or designated representative will be permitted to access these stored data and in any case, admission to Imperial College Archives is by appointment only to bona fide scholars; prior proof of status, proof of identity and a description of the research project is required.
2. Identifiable data will be processed only on the study stand-alone Admin PCs. A backup utility exists which creates an AES-256 encrypted container (using Truecrypt) and copies it to an erased USB thumb-drive for remote storage using a key-phrase known only to the SABRE Team. Study results are anonymised by the copying of only the ‘Results’ database onto a thumb-drive for analysis, which contain*s* (as above) no identifiable information. No remote access system exists, or is possible as the system is connected to no external network. Patient identifiable information is printed for sending of patient and GP letters, only members of the SABRE team have the PC access to do so.
3. The System’s authorised users shall be: Therese Tillin, Nishi Chaturvedi, Emma Coady, Daniel Key, John Heasman, April McGowan, Chloe M Park, Lucy C Smeaton, Robert Spiller, Claire S Tuson, Laura M Villis, Joseph Willis, Mark Baker, Helen Walkey.
4. When the system or its data has completed its purpose the following methods will be adopted to dispose of equipment, back-up media or other stored data: Block erase software loaded on a boot disc will be used to wipe PC hard drives and all paper records will be securely incinerated. Daniel Key is responsible for digital disposal and Therese Tillin is responsible for disposal of paper records. Future follow-up of the cohort is anticipated, subject to funding and regulatory approvals, hence storage of a minimum identifiable dataset will be required (fullname, sex, ethnicity, date of birth, NHS number, first line of address, postcode) encrypted using AES 256 encryption.

**System Audit**

1. The System shall benefit from the following internal audit arrangements.

Lucy Smeaton, Information Systems manager will monitor adherence to the above mentioned procedures on a 6 monthly basis and will deliver any additional staff training that may be required to maintain these processes. If modifications to the SLSP are required these will be notified to the NIGB/ECC.

1. Risk assessment : This small stand-alone system will be risk assessed annually, and in response to any incident or weakness reports, by the data controller and will comply with Imperial College’s policy: <http://www3.imperial.ac.uk/secretariat/policiesandpublications/informationsystemssecurity/guidelines/guide9>

**System Protection**

1. The System shall benefit from the following resilience / contingency / disaster recovery arrangements: remote (encrypted) backups on an Imperial college network share, subject to Imperial backup arrangements.
2. In the event of serious disruption or total system failure, business continuity shall be provided by the following means: replacement hardware as necessary and restoration from aforementioned backups.
3. In the event of a security or confidentiality breach occurring the following procedure shall be followed ; Immediate notification of the Data Custodian, Imperial College Clinical Research Governance Office and Director of Information and Communications Technology who will advise the appropriate course of action as noted below:.

* *Anyone suspecting that there has been, or is likely to be, a breach or weakness of IS Security should inform the director of ICT immediately who will advise the College on what action should be taken.*
* *In the event of a suspected or actual breach of security, the Director of ICT may, after consultation with the relevant Custodian or College Authorised Officer, make inaccessible/remove any unsafe user/login names, data and/or programs on the system from the network and report this to the IS Security Co-ordinator.*
* *Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of the Data Protection Act 1998 and could lead to civil or criminal proceedings. It is vital, therefore, that users of the College’s Information Systems comply, not only with this policy, but also with the College’s Data Protection Policy and associated Codes of Practice, details of which may be found on the College website.*
* *The Rector or his Deputy has the authority to take whatever action is deemed necessary to protect the College against breaches of security.*

**System Level Security Policy Ownership**

1. This SLSP is the responsibility of: Daniel Key and will be reviewed Lucy Smeaton on an annual basis for its completeness and for relevant update.
2. The SLSP shall be distributed to the SABRE Study Team in hard copy and will be available through the secure means of the NIHR Portal.

**Data Protection Registration**

1. Imperial College has Data Protection Registration to cover the purposes of research and for the classes of data requested and is registered with the registration number Z5940050.

.