Medicine

UNIVERSITY OF Southampton

BRAIN UK

UK Brain Archive Information Network

INFORMATION TECHNOLOGY SECURITY POLICY

SOP Reference	BUK SOP 3
Version number	1.31
Date created	15 April 2015
Date of last review	15 April 2015
Date of next review	15 April 2017

Author:

Name	Dr Clare Mitchell
Signature	

Authorised by:

Name	Prof. James A R Nicoll
Signature	

THIS PAGE IS BLANK

Table of Contents

THIS PAGE IS BLANK

1. Purpose

BRAIN UK processes and maintains a large amount of valuable data. This policy aims to protect such data against loss, unauthorised access and modification, inadvertent destruction and to ensure that the integrity and quality of stored data is maintained.

The data processed by *BRAIN UK* falls into one of two distinct categories:

1. Data derived from the medical records of the deceased that is used to construct the central database to which the UK research community will have ultimate access in an anonymised format. This will facilitate high quality research in neuromedicine and allied fields by identifying those Participating Centres that hold pertinent tissue within their diagnostic archives.

2. Data derived from the living (both donors who have undergone a surgical or diagnostic procedure and those researchers applying for access to tissue held within the diagnostic archives of Participating Centres). This is processed and maintained :

   i. to facilitate high quality research in neuromedicine and allied fields by identifying those Participating Centres that hold pertinent tissue within their diagnostic archives;

   ii. to enable efficient communication between applicants, *BRAIN UK* and Participating Centres; and

   iii. as a consequence of the requirements of ethical approval, to enable an audit trail to be created should it be required in the future.

In order to process this data effectively it is important that all staff are aware of all relevant legislation and policies regarding data security and confidentiality issues.

The most important piece of legislation regulating the acquisition, holding and processing of personal information is the Data Protection Act 1998 (the 'Act'). *BRAIN UK* is committed to abide by the not only the letter but also the spirit of the Act and to promote the highest possible standards of conduct mandated by the Act. **It is important to note that the a component of the *BRAIN UK* database will be using data solely derived from the deceased (i.e. *BRAIN UK 1* and *BRAIN UK 2*) and that, in law, the Act does not apply in this instance. However, *BRAIN UK* will still adopt principles that abide by the spirit of the Act in this instance to ensure the implementation and maintenance of best practice**. In relation to personal data collected as a consequence of the application procedure the Act will be adhered to as it applies in this situation.

2. Policy Declaration

2.1 Data Storage

The *BRAIN UK* database will not store any patient identifiable information either electronically or in a written or printed format. *BRAIN UK* data will be stored electronically, by the provision of a folder, on networked SAN storage dedicated to University research data in secure University data centre; By storing the data on networked storage, risk of theft or loss of data on the client PCs is minimised. Further encryption and securing of the client PCs minimises further risk of loss of data via data remnants, swapfile contamination and orphaned temporary files.

2.2 Backup and Recovery Plan

The *BRAIN UK* database and the database relating to the application process contain valuable sensitive data. It is considered best practice to ensure that these files are maintained on a networked SAN storage dedicated to University research data in a secure University data centre. Backups of the data will be automated via functionality inherent in the networked storage, providing a minimum of 90 days snapshots of the data for recovery purposes, and mirrored to an offsite secure University data centre for business continuity purposes.

(Current configuration provides snapshots every 2 hours, retained for one month, and offsite replication every 6 hours, retained for 3 months).

2.3 System Access and Passwords

The System shall be accessible from any staff University PC with permitted access control with access permissions set and verified to permit only those with authorised user access. Network logins ensure access by authorised staff: project staff, project supervisor and authorised iSolutions staff under supervision (ISO27002:2013 9.2.3) with access restricted by Active Directory permissions to authorised staff and minimal set of senior trusted administrators. (ISO27002:2013 9.4.1). The system will only be accessed *BRAIN UK* Data Co-Ordinators on a routine basis and will be made available to the *BRAIN UK* Director (Professor James A. R. Nicoll), his deputy (Dr David Hilton) upon request**.**

There will be enforced regular robust password changes (ISO27002:2013 9.4.3), review of user access rights at regular intervals (ISO27002:2012 9.2.5) and review of access permissions on a regular basis and following exceptional events such as termination of employment (ISO27002:2013 9.2.5).

Paper records that are generated as a consequence of this study will be filed in a locked cupboard in the Data Co-ordinator's office. The key to this facility will be kept on the person of the Data Co-ordinator. For use in unforeseen circumstances, a duplicate key will be kept in a secure location in the offices of the Chief Investigators.

2.4 Encryption

Current encryption guidance for NHS organisations can be found in "Guidelines on use of encryption to protect person identifiable and sensitive information"[1], and we would expect any electronic solution for the handling of patient identifiable / sensitive data to comply with this guidance as a minimum.

User access will be via Windows based PCs provided by iSolutions. By storing the data on networked storage, risk of theft or loss of data on the client PCs is minimised. Further encryption and securing of the client PCs minimises further risk of loss of data via data remnants, swapfile contamination and orphaned temporary files. *BRAIN UK* employs full disk encryption of all PCs accessing *BRAIN UK* data using MS Bitlocker as per iSolutions policy (ISO27002:2013 10.1.1) with central recovery keys for MS Bitlocker having restricted administrator access (ISO27002:2013 10.1.1)

Data will only be transferred using an encrypted Zip file (AES-256 encryption; many Zip programs offer this functionality) with the password for the zip file shall be communicated via another medium. Data required to be physically transported will us an encrypted USB drive that conforms to NHS-approved standards (FIPS-140-2; 3-DES or AES, to 256-bit strength. Kingston Technology DataTraveler Locker 4GB 256-SHA is a typical approved device).

2.5 Data Transfer

Given historic and high profile security lapses in a range of UK governmental and organisational settings concerning the loss of sensitive data, measures maintaining the security of data during its transport or transfer from the originating site to the core database are considered to be of the utmost importance. Therefore protocols for the safe and secure transportation or transfer of data will be developed in line with the recommendations of best practice contained within the NHS Information Security Management Code of Practice The bulk extraction and transfer of data will also only occur once the specific management authorisations of the Participating Centres have been received in line with the NHS Information Governance Framework.

In the best interests of security the following methods will be employed to transfer data from Participating Centres to the centralised database:

Physically, using secure and accredited courier services, or collected in person by the Data Co-ordinator. In each case, data will be maintained in a suitably encrypted form on electronic storage media (*e.g.* encrypted USB drive or PC's employing full disk encryption) to maintain security should incidents of loss or theft occur.

- Electronically, by using an encrypted Zip file and the use of the University's 'DropOff' service (https://dropoff.soton.ac.uk) for secure transmission of the file. With the password for the zip file being communicated via another medium; telephone, post or email to an alternative email account used for the 'DropOff' process.

The application process will generate data of a different quality from that of the main *BRAIN UK* database. Data will be collected electronically via e-mail and through standard postal services. As the individuals concerned are living applicants, this undertaking is made **at their own risk** and a disclaimer will make this apparent in the declaration associated with the tissue application form.

2.6 Physical Security

The *BRAIN UK* office is located within a secure area accessible via doors with card activated magnetic locks at both entrances to adjoining corridor (ISO27002:2013 11.1.2). Access to this area is by accredited University identity card and access is restricted between the times of 0800 to 1800 on weekdays; weekend access is by application only. In addition, this office is also locked using a combination lock (via keypad (ISO27002:2013 11.1.2)) which is known to the users of the office and senior management within the Division of Clinical Neurosciences.

All paper documents that may contain sensitive data will not be left in such a position as to facilitate casual browsing by unauthorised individuals and will be kept out of sight where practicable. When not in use, such paper documents will be filed in a locked cabinet in this office. A fire-proof safe will be installed in which to store any documentation deemed to be of a highly sensitive nature. This will be accessible by a combination lock and key and will be securely fastened to prevent theft.

2.7 Data Quality and Accuracy

2.7.1 Data Entry

All data entered onto a relevant database will be logged electronically to indicate user name, time and date.

2.7.2 Data modification and Deletion

The action of modifying and deleting any data will be logged electronically to indicate user name, time and date. This log will also include a field to indicate the reason for any change.

2.8 System Specification

A dedicated stand-alone desktop PC will be used for the storage and processing of all data associated with the *BRAIN UK* project. This PC will utilise an encrypted partition drive for the storage of all data and personal information and a dedicated removable hard drive for the purposes of backing up data at regular intervals.

3. References

1. NHS Connecting for Health: Guidelines on use of encryption to protect person identifiable and sensitive information: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/encryptionguide.pdf/view

4. Supporting Documentation

The following documents augment policy areas and procedures contained within this document:

a. *Regulations for the Use of iSolutions Resources*

University Calendar 2013 iSolutions Regulations 040214 v1.0.pdf

b. *Regulations for the Use of Computers and Voice and Data Communications Networks*

University Calendar 2013 Data Communications Networks Regulations 040214 v1.0.pdf

c. *Incident Management v1.0*

Incident management 040214 v1_0.pdf

d. *Systems Level Security Policy v1.2*

SLSPe.docx