BRAIN UK
UK <u>Br</u>ain <u>A</u>rchive <u>I</u>nformation <u>N</u>etwork

Information Governance

Contents

1.   Document Rationale

1.1   Background

The UK Brain Archive Information Network (BRAIN UK) is a system that catalogues the tissue archival holdings of participating NHS Neuropathology Centres around the UK in order to provide a 'virtual' brain tissue bank. This information resource facilitates high quality medical and biomedical research by identifying sites holding tissue of relevance to their existing and future research studies. Key to this system is a database storing the information on neuropathology tissue and associated information relevant to tracking for audit and ethical purposes. The data of interest to BRAIN UK is derived primarily from the medical records from living and deceased individuals. As a consequence of providing a research tissue bank service, BRAIN UK also collects data on researchers who are either using or enquiring about the potential to use the BRAIN UK service. This document sets out the data collected and how it is processed and secured.

1.2   Legal and Ethical Considerations

This section briefly discusses the legal and ethical considerations around storing data from the BRAIN UK participants. There are different legal obligations regarding the storage and use of data dependent on whether a participant is living or deceased; the date the record was created; and whether they have consented to research and/or disclosure.

Consent to research is more fully discussed in the Protocol document, Sections 3.3 Use of Human Tissue for Research and 3.4 Use of Data and/or Tissue in BRAIN UK. Briefly, the three component arms of BRAIN UK:

- BRAIN UK 1 tissues, defined as part of an 'Existing Holding' under the Human Tissue Act 2004[1] and Human Tissue Act (Scotland) 2006[2], there is no mandatory requirement for informed consent for the use of this tissue for research purposes as long as the tissue is supplied in an anonymised format and that any research is subject to approval by a UK Research Ethics Committee.

- BRAIN UK 2 there is a mandatory requirement for informed consent for the use of this tissue for research purposes.

- BRAIN UK 3 there is no mandatory requirement for informed consent for the use of this tissue for research purposes, as long as tissue is supplied in an anonymised format and that any research is subject to approval by a UK Research Ethics Committee.

The General Data Protection Regulation (EU) 2016/679 (GDPR)[3] sets out the key principles, rights and obligations for most processing of personal data. The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK. This, along with the Data Protection Act 2018 and Access to Medical Records Act 1990, below, are discussed more fully in in the Protocol document, Section 3.4.2 Data Protection Act 2018.

The Data Protection Act 2018[4] sets out the framework for data protection law in the UK. It sits alongside the GDPR, and tailors how the GDPR applies in the UK - for example by providing exemptions. This Act describes the regulations for processing of information relating to individuals, including the obtaining, holding, use or disclosure of information and applies to the living. Although the Act does not apply to the deceased, BRAIN UK also commits as far as possible to adhere to the principles for the deceased participants of BRAIN UK.

Access to Medical Records Act 1990[5] covers access to the records from living individuals and in part from the deceased. For the deceased, it primarily relates to access by those who may have a claim arising from the patient's death and only applies to records created since 1st November 1991.

---

[1] Human Tissue Act 2004 http://www.legislation.gov.uk/ukpga/2004/30/contents
[2] Human Tissue (Scotland) Act 2006 http://www.legislation.gov.uk/asp/2006/4/contents
[3] General Data Protection Regulation (EU) 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[4] Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[5] Access to Health Records Act 1990 http://www.legislation.gov.uk/ukpga/1990/23/contents

The Freedom of Information Act 2000[6] provides public access to information held by public authorities. The University of Southampton, BRAIN UK's sponsoring organisation, has adopted the Model Publication Scheme[7] prepared and approved by the Information Commissioner.

Principles of the Caldicott Report

The Caldicott[8,14] recommendations apply specifically to patient-identifiable information, and emphasise the need for controls over the availability of such information, and access to it. There are considerable similarities and overlaps between the requirements of the Data Protection Act 1998 and the recommendations of the Caldicott report and they combine to inform the conduct of individuals in handling confidential personal data. The Caldicott report sets out a number of key principles:

1. There should be justification for the purpose for which information is required.
2. Person-identifiable information should not be used unless it is absolutely necessary.
3. The minimum necessary person-identifiable information should be used to satisfy the purpose.
4. Any access to person-identifiable information should be on a strict 'need-to-know' basis.
5. Everyone with access to person-identifiable information should be aware of his or her responsibilities with regard to the maintenance of confidentiality.
6. All individuals with access to patient-identifiable information must be aware of, understand and comply with the law.

The two key components of maintaining confidentiality are the *integrity* of information and its *security*. Integrity is achieved by safeguarding the accuracy and completeness of information through proper processing methods. Security measures are needed to protect information from a wide variety of potential threats. These elements are covered in this document.

1.3   Strategy and Implementation

The BRAIN UK policies, should be effectively communicated to all staff by:
1. Introducing data confidentiality and data security issues through induction and the provision of relevant training.
2. Ensuring that this, and related policies are read by all staff and that electronic acknowledgement is received and stored.
3. Ensuring all staff with access to confidential data owe a duty of confidentiality and relevant permissions with any participating NHS Trust as well as the permission of Health Research Authority's Confidentiality Advisory Group, as appropriate.
4. Maintaining staff knowledge of confidentiality and security issues and disseminating any changes through regular update sessions.
5. Making this, and related policies, available in accessible formats.

1.4   Staff Responsibilities

All individuals working with sensitive or person-identifiable data have the following responsibilities:
- Person identifiable patient information is not to be printed out.
- Locations where records are held should be secure at all times *e.g.* locking of doors, restriction of access, screen locking of computers.
- Sharing of passwords is forbidden.
- Identifiable material should not be left in locations where unauthorised personnel may gain access to it or be discussed in inappropriate locations.
- Sensitive and person-identifiable data should not be accessed on unauthorised computers *e.g.* personally owned computers.
- Any suspected or actual breach of confidentiality must be reported to a line manager immediately and the responsible Data Protection Officer for the University must also be informed.
- Staff members must co-operate in training programmes provided and maintain an awareness of confidentiality and data security issues.

---

[6] Freedom of Information Act 2000 http://www.legislation.gov.uk/ukpga/2000/36/contents
[7] Freedom of Information Act 2000. Definition document for universities and other higher education institutions. https://ico.org.uk/media/for-organisations/documents/1245/definition_document_for_universities_and_higher_education_institutions.pdf
[8] Information: To share or not to share? The Information Governance Review. 2013 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_Info Governance_accv2.pdf

2.   Data Processing

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

> 1. Data derived from the medical records, creating the 'BRAIN UK Database'. This is a large number of records, currently around 100,000 and aiming to be around 500,000.

> 2. Data derived from the researcher enquiries, applications, annual reports and closing reports, resulting in the 'Researcher Data Set'. A smaller set of records, typically less than 1000.

2.1   BRAIN UK Database

The 'BRAIN UK Database' is the term used to describe the data stored that has been derived from the medical records of the:
- Deceased.
- Living (participants who have undergone a surgical or diagnostic procedure).

These are processed and maintained:
- To construct a central research tissue bank database which facilitates high quality research in neuromedicine and allied fields.
- To enable efficient communication between applicants, BRAIN UK and Participating Centres.

This is the primary resource that BRAIN UK uses to support researchers. The data was not primarily collected for the purpose of research and is considered to be sensitive by the GDPR[3].

2.1.1 BRAIN UK Database Confidentiality

The creation and maintenance of the BRAIN UK Database relies upon access to and disclosure from the medical records. The advice from the Department of Health is that anonymisation requires the removal of name, address, full postal code and any other detail or combination of details that might support identification[9]. In practice, assessing the risk that additional relevant information will be used by others to reveal identity is difficult because of lack of reliable information about the variables influencing risk[10].

To maintain confidentiality, BRAIN UK uses a minimal dataset that excludes directly identifiable fields. The inclusion of a specimen laboratory number (or equivalent) will by definition make the data stored on the database linked anonymised ('pseudonymised')[11] in nature. From feedback received from Participating Centres there was a common feeling that the inclusion of laboratory numbers would make it more efficient for them to locate specific tissue and medical data of interest. Although a laboratory number is potentially a personal identifier, the key relating to core personal details (*e.g.* patient name, date of birth, address, NHS number) will be held and maintained only by the participating host centre in question. No inference about the identity of an individual represented by a particular laboratory number can therefore be reasonably or easily deduced by BRAIN UK or others. The data is therefore linked anonymised which is considered as anonymised for practical purposes when the key to patient identity is not held by the researcher as is the case here and that there is neither compromise to patient privacy nor a common law requirement to seek consent for their use under these circumstances[12],[13].

BRAIN UK follows the Caldicott principles[14,8] for populating the BRAIN UK Database, that is, using the minimum necessary dataset to satisfy the identification of tissue for potential research purposes and restricting and securing access to the information.

---

[9] Confidentiality. NHS Code of Practice. November 2003. Department of Health.
[10] Anonymisation Standard for Publishing Health and Social Care Data. Supporting Guidance: Drawing the line between identifying and non-identifying data. 2013. NHS and The Information Centre for Health and Social Care. http://webarchive.nationalarchives.gov.uk/+/http://www.isb.nhs.uk/documents/isb-1523/amd-20-2010/1523202010guid.pdf
[11] British Medical Association (April 2007) Guidance on secondary uses of patient information. http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records
[12] Scottish Executive (July 2003) NHS Scotland: NHS Code of Practice on Protecting Patient Confidentiality
[13] British Medical Association (2019) Requests for disclosure for secondary uses of data. https://www.bma.org.uk/-/media/files/pdfs/practical%20advice%20at%20work/ethics/releasingdataforsecondaryuses.pdf?
[14] Report on the Review of Patient-Identifiable Information. The Caldicott Committee. Department Of Health. December 1997. http://www.wales.nhs.uk/sites3/Documents/950/DH_4068404.pdf

BRAIN UK's approach to confidentiality is based upon a number of core policy documents:
- Information Security Management: NHS Code of Practice[15]
- NHS Information Governance: Guidance on Legal and Professional Obligations[16]
- The Caldicott Committee: Report on the Review of Patient-Identifiable Information[17]
- Protecting Patient Confidentiality: Final Report[18]

It is advisable that staff familiarise themselves with the content of these documents and other key legislation.

2.1.2 BRAIN UK Database Dataset

A defined dataset, obtained from the Participating Centres, gives information concerning the nature, format and simple demographics of available tissue to facilitate its identification for research applications. The defined dataset is as follows:
- Geographical location
- Laboratory/Post Mortem Number
- Age at procedure
- Sex
- Tissue format
- Diagnostic details
- Matched clinicopathological data availability (e.g. pathology reports and autopsy reports)
- **Flag in the database cases involved in other national ethically approved initiatives (e.g. 100,000 genomes project, UK biobank)**

It is noted that different Participating Centres use differing diagnostic coding systems. As part of the integration of the dataset into the BRAIN UK Database the data set is standardised, within reason, to facilitate searching. However, this uses the least manipulation possible to minimise effort and ensure data integrity. A copy of the dataset prior to any manipulation is always stored.

2.1.3 Data retrieval and processing for the BRAIN UK Database

The identification of participants to include on the BRAIN UK Database is performed electronically using standard query functions, which are incorporated into laboratory computer systems and are based on medical records stored in Neuropathology Archives across the UK. 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[19].

During the process of accessing the medical records individuals may be privy to personal identifying information. Linked anonymisation occurs as soon as is practicable and this process is preferably undertaken by the original custodians of the data or, as a contingency measure, by a nominated individual within the BRAIN UK research team or, in exceptional circumstances, a researcher, subject to the necessary permissions. See below for further details.

Primary Care Team
The access to the medical records of the patients is, in the first instance, undertaken by a member of a patient's care team as the most ethical means of maintaining the common law duty of confidentiality. This is typically interpreted as being a Consultant in Neuropathology, Laboratory Manager or a Biomedical Scientist.

Members of BRAIN UK Team
BRAIN UK aims to provide a comprehensive coverage of diseases and conditions; this requires as many suitable neuropathology centres as possible. At times some centres cite resource difficulties, such as staff time, as a reason not to participate. In these situations a nominated member of the BRAIN UK team may be offered to undertake this duty.

---

[15] Information Security Management: NHS Code of Practice (Department of Health, April 2007)
https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice
[16] NHS Information Governance: Guidance on Legal and Professional Obligations (Department of Health, September 2007). https://www.gov.uk/government/publications/nhs-information-governance-legal-and-professional-obligations
[17] The Caldicott Committee: Report on the Review of Patient-Identifiable Information (Department of Health, April 2013). https://www.gov.uk/government/publications/the-information-governance-review
[18] Protecting Patient Confidentiality: Final Report (The Confidentiality and Security Advisory Group for Scotland, April 2002). https://www.sehd.scot.nhs.uk/publications/ppcr/ppcr.pdf
[19] Department of Health NHS Information Governance (July 2008) Guidance note: Security of NHS patient data shared for research purposes.

BRAIN UK would anonymise the data as soon as is practical, resulting in a linked anonymised data set. As nominated individuals would have this task this would present minimal risks of personal data being disclosed inappropriately and it would greatly reduce any scope for the infringement of the common law duty of confidentiality. This measure makes potentially sensitive personal data available to the least number of individuals possible and greatly reduces the scope for legal or ethical objection. The BRAIN UK team member would be bound by a duty of confidentiality as per the relevant policies produced by the University of Southampton and would be liable to the sanctions set out in such policies should inappropriate breaches of data security or confidentiality occur for whatever reason.

This work will only be performed once the relevant permissions have been obtained from each Participating Centre (e.g. Honorary Contract, Research Passport) and only with an individual owing a duty of confidentiality. In addition, an application will be made to Health Research Authority's Confidentiality Advisory Group for their permission to access patient records on a case-by-case basis.

External Individuals
In exceptional circumstances, when a specific research study requires additional information to be obtained from the hospital records and the staff of the Participating Centre and BRAIN UK are unable to extract this information, the research team may do this, after the necessary approvals for 'Section 251 support' have been sought and local data custodians have also granted relevant management approvals.

Access to relevant existing medical records (e.g. clinical history, medication history, X-ray and imaging) would permit an increase in both the quantity and quality of data available for a particular research project as well as improving the scope of study types potentially supportable. Given the additional workload in undertaking this work on behalf of the research community it is doubtful whether Participating Centres or BRAIN UK would have the time or resources available. BRAIN UK will therefore encourage researchers to seek evidence-based Section 251 support from the Health Research Authority's Confidentiality Advisory Group should they wish to augment their studies with additional data and ensure that relevant local conditions and approvals are met. This data would only be made available in an anonymised format and the anonymisation process would be undertaken within a Participating Centre with no participant identifiable data leaving these locations.

2.2 Researcher Data Set

The 'Researcher Data Set' is the term used to describe the data stored that is as a consequence of providing the BRAIN UK service. The data is primarily collected for the purpose of supporting research for this study and is not considered to be sensitive by the GDPR[3]. It involves a much smaller quantity of data records and is derived from the enquiries, applications, annual reports and closing reports from researchers to BRAIN UK.

The 'Researcher Data Set' is a loose term used to describe the creation of datasets which are processed and maintained to:
- Make the information more accessible, searchable and reportable.
- Enable efficient communication between applicants, BRAIN UK and Participating Centres.
- Enable an audit trail, to comply with our ethical approval conditions.

2.2.1 Researcher Record Dataset

The Researcher Data Set records are an undefined dataset derived from the enquiries, applications, annual reports and closing reports from researchers to BRAIN UK. These are either supplied to BRAIN UK in email, electronic document or paper format. Data records will primarily be identified by a unique code assigned by a member of the BRAIN UK Team. The dataset typically includes:
- Work contact details of the researchers involved
- Details of the tissue either provided to the studies or enquired about
- A summary of the progress of the enquiry or application
- Details required for the purpose of reporting for ethics purposes, such as breaches of ethics, incidents
- Outputs

As part of the integration of the dataset into the Researcher Data Set the dataset may be standardised, within reason, to facilitate searching and reporting. However, this will be using the least manipulation possible to minimise effort and ensure data integrity. A copy of the dataset prior to any manipulation is always stored.

2.2.2 Data retrieval and processing for the Researcher Data Set

The identification of data items to include on the Researcher Data Set is performed manually by members of the BRAIN UK team. The identification is dependent on the type of reporting required, for example, outputs generated by the studies supported.

Only members of the BRAIN UK team will be able to access, populate and process data for the Researcher Data Set.

2.2.3 Data Confidentiality in the Researcher Data Set

The creation and maintenance of the Researcher Data Set relies upon access to and disclosure from information that enquirers and researchers may consider confidential. To maintain confidentiality and confidence in BRAIN UK, a minimal dataset will be used that supports the continuity of the service. Information will not be disclosed to anyone outside of the BRAIN UK team and committee that could identify either an individual or study without their express permission, except for the purpose of audit or regulatory control.

Access by data subjects to any personal data held by the University will be facilitated in accordance to the University of Southampton's Data Protection Policy[20].

---

[20] University of Southampton's Data Protection Policy May 2018
http://www.southampton.ac.uk/assets/sharepoint/intranet/ls/Public/Information%20Governance%20Policies/Data%20Protection%20Policy.pdf

3. System Level Security

BRAIN UK maintains a large amount of useful data. This section aims to outline the approach to protecting the data against loss, unauthorised access and modification, inadvertent destruction and to ensure that the integrity and quality of stored data is maintained and to help demonstrate an understanding of information governance risks and commitment to address the security and confidentiality needs of the system.

In the context of this document "System" relates to the complete data handling solution (electronic or otherwise)

3.1 System Details

The System's responsible owner shall be Academic Unit of Clinical Neurosciences, Clinical and Experimental Sciences, Faculty of Medicine, University of Southampton ("the University").

The System shall be implemented by the University of Southampton's IT service iSolutions (underlying operating system and database software) with the application software being developed and maintained by BRAIN UK, with technical support provided by iSolutions.

The System's authorised users shall be the BRAIN UK team and relevant members of the iSolutions Serviceline Response Team. The iSolutions Serviceline Response Team maintain a role based access policy, where members have permissions that are necessary and proportionate to perform their role only. These are managed on a group member basis so that when people change position they are removed efficiently.

3.2 System Security

The University of Southampton is currently reviewing its corporate Information Security policy with the intention of aligning working practices to the UCISA Information Security Toolkit which is based upon ISO27001:2005, using a subset of the controls specified in ISO27002:2005. Many policies and processes are already in alignment or are newly implemented within the spirit of the updated ISO27001:2013, although formal capability matching has not yet taken place.

A number of applicable University of Southampton policies are in place[21] that shape BRAIN UK's practices and include:
- Management of Deviations and Serious Breaches of GCP and/or the Study Protocol
- Data Protection Policy
- Electronic Communications Policy
- Regulations for the use of Computers and Voice and Data Communications Networks
- Regulations for the Use of iSolutions Resources

The system's responsible Security Manager shall be the BRAIN UK Project Manager. The Security Manager's duties shall include:

- Identification of all appropriate statutory, regulatory and best practice requirements relating to Information Security
- Identification and assessment of system related risks in liaison with the iSolutions Head of Information Security
- Implementation of appropriate security controls to satisfactorily address identified risks.
- Accreditation of security measures, including external validation as required, with the assistance of the iSolutions Head of Information Security
- Communication of security responsibilities to other parties using the system
- Maintenance of the risk register relating to the system, with the assistance of the iSolutions Head of Information Security.

The system shall incorporate the security controls in the following subsections (with reference to the guiding elements of ISO27002:2013 code of practice where appropriate; this does not however imply compliance with all aspects of ISO27002:2013).

---

[21] University of Southampton Legal Services Information Governance and Policies
https://www.southampton.ac.uk/legalservices/policy-and-guidance.page

3.2.1 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, there is CCTV monitoring in corridors and the office is locked outside of working hours.

Any paper documents that may contain sensitive data will not be left in a position as to facilitate casual browsing by unauthorised individuals and will be kept out of sight where practicable. When not in use, paper documents will be filed in a locked cabinet in this office.

3.2.2 System Access Control

User access will be via Windows based PCs provided by the University of Southampton. The System shall be accessible from any staff University PC with permitted access control. PC Windows Firewall will be enabled (ISO 27002:2013 13.1.3) and Symantec Endpoint Protection anti-virus/malware enabled (ISO 27002:21013 12.2.1) as per University policy. Access permissions will be 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). Access is restricted by Active Directory permissions to authorised staff (ISO27002:2013 9.4.1). The system will only be accessed by the BRAIN UK team on a routine basis and will be made available to the BRAIN UK Director and Co-Director/s upon request.

There are 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).

3.2.3 Data Storage

BRAIN UK data will be stored electronically, by the provision of a folder, on networked storage (SAN: Storage Area Network)dedicated to University of Southampton research data in a secure University data centre. By storing the data on networked storage, risk of theft or loss of data on the client PCs is minimised. Paper records of data will not be routinely kept, to reduce risk of loss of data and improve data integrity.

3.2.4 Backup and Recovery Plan

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

3.2.5 Encryption and Data Transfer

Link anonymised data can be transferred:

- Physically, using secure and accredited courier services, or collected in person by BRAIN UK, with data suitably encrypted on electronic storage media (e.g. encrypted USB drive or PCs employing full disk encryption) to maintain security should incidents of loss or theft occur. Encrypted USB drives need to conform 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).
- Electronically, by using an encrypted Zip file and either the use of the University's 'Safesend' service (https://safesend.soton.ac.uk/) or from a NHS.net account to a NHS.net account (held by BRAIN UK staff with honorary NHS contract) 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 to either the NHS.net account or the email account used for the 'Safesend' process.

Current encryption guidance for NHS organisations can be found in Approved Cryptographic Algorithms Good Practice Guideline[22], and we would expect any electronic solution for the handling of patient identifiable/sensitive data to comply with this guidance as a minimum.

---

[22] Approved Cryptographic Algorithms Good Practice Guideline. Version 4.0. NHS Digital.
https://webarchive.nationalarchives.gov.uk/ukgwa/20161021125701/http:/systems.digital.nhs.uk/infogov/security/infrasec/gpg/acs.pdf

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)

The linked-anonymised dataset is unlikely to be used for identifying an individual, but BRAIN UK still considers it 'sensitive'. It will be sent from the originating site to the University of Southampton by using an encrypted Zip file (AES-256 encryption; many Zip programs offer this functionality). The password for the zip file shall be communicated via another medium, for example, telephone or email to an alternative email to either the NHS.net account or the email account used for the 'Safesend' process.

3.2.6 Data Quality and Accuracy

Data entered onto a relevant database will be logged electronically to indicate user name, time and date. This is inherent in the operation of the managing software by use of version controls. In addition for the BRAIN UK participant database a 'Version History' will be maintained to indicate the reason for the change.

3.2.7 Data Retention

BRAIN UK follows the University of Southampton Research Data Management Policy[23] and its associated Record Retention Schedule[24]. In summary:
- General Research Project Files
  There is a business need that research data should be held for a minimum period of 10 years from collection, creation or generation or publication of the research results (whichever is the later).
- Data derived from the medical records and researchers
  The University has statutory obligations and the data has a public interest or heritage value and, as such, will be stored for 30 years.
- Any study involving minors (under 18 years)
  The University has statutory obligations to meet and stores this data for at least 21 years.

3.3 System Audit

Reviews of the SLSP will be initiated by the Security Manager and the iSolutions Head of Information Security on a regular basis. (ISO27002:2013 18.2.1).

An internal review of the system and associated risk register will be undertaken on an annual basis in conjunction with the iSolutions Head of Information Security, in the spirit of ISO27001:2013 9.2. Where unacceptable risks are identified, improvements shall be undertaken. Continual improvement activities will be undertaken to ensure the continued effectiveness of security controls on the system.

3.4 Operational Processes

When the system or its data has completed its purpose or is otherwise no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data:

- Network storage will be deleted; following this deletion, data will remain in backup systems for 90+ days until expired.
- Keys relating to encrypted storage media will be intentionally destroyed.
- Non-working media will be physically destroyed.
- Optical media will be physically destroyed.

---

[23] University of Southampton Research Data Management Policy 2018-2019
http://www.calendar.soton.ac.uk/sectionIV/research-data-management.html
[24] University of Southampton Record Retention Schedule June 2018
http://www.southampton.ac.uk/assets/sharepoint/intranet/ls/Public/Information%20Governance%20Policies/Record%20Retention%20Schedule%20Final%20June%202018.pdf

4 Data Protection Registration

The sponsoring organization holds a Data Protection Registration,
https://ico.org.uk/ESDWebPages/Entry/Z6801020

Registration number: Z6801020
Date registered: 21 June 2002
Registration expires: 20 June 2023 (renewed annually)
Payment tier: Tier 1
Data controller: UNIVERSITY OF SOUTHAMPTON
Address:
HIGHFIELD
SOUTHAMPTON
HAMPSHIRE
SO17 1BJ

Freedom of information statement:
This data controller states that it is a public authority under the Freedom of Information Act 2000 or a
Scottish public authority under the Freedom of Information (Scotland) Act 2002

5 Amendment History

Amendment No.	Version no.	Date approved	Author(s) of changes	Details of changes made
-	2.0	11/06/2019	C. Mitchell	Created 01/04/2019. Preparation for new ethics application: updated to include GDPR changes, and amalgamation of documentation to ensure consistency and remove duplication.
8375.A3	3.0	08/08/2022	T. Bloom	Created 01/05/2022. Preparation for substantial amendment request to include change of PI, staff changes, centre changes and updated application form