

**BRAIN UK**  
**UK Brain Archive Information Network**  
**Existing Holdings**  
**DATA CONFIDENTIALITY POLICY**

<b>SOP Reference</b>	BUK SOP 2
<b>Version number</b>	1.0
<b>Date created</b>	10 March 2009
<b>Date of last review</b>	10 March 2010
<b>Date of next review</b>	10 March 2011

**Author:**

**Name** Mr Neil Bailey

**Signature**

**Authorised by:**

**Name** Prof. James A R Nicoll

**Signature**

**THIS PAGE IS BLANK**

## Table of Contents

<b>1. Purpose</b>	5
<b>2. Policy Declaration</b>	5
<b>3. Principles of the Caldicott Report</b>	5
<b>4. The Data Protection Act 1998</b>	6
<b>5. Strategy and Implementation</b>	7
<b>6. Staff Responsibilities</b>	7
<b>7. Key Policy Elements</b>	8

**THIS PAGE IS BLANK**

## **1. Purpose**

The creation and maintenance of the UK Brain Archive Information Network (*BRAIN UK*) database relies upon access to and disclosure from the medical records of deceased individuals who have been subjected to post mortem examinations (either Coronal/Procurator Fiscal or hospital) to determine their cause of death. The extraction and anonymisation of relevant data is to be performed primarily by Healthcare Professionals employed by the NHS (e.g. Biomedical Scientists, Laboratory Managers, Neuropathologists) within each participating centre although there is scope for this to be performed by a member of the *BRAIN UK* research team holding an honorary contract and relevant approvals with each NHS Trust should the need arise. This places a legal obligation upon such individuals to adhere to the data protection policies of individual NHS Trusts and to maintain a common law duty of confidentiality in relation to patient-specific information they may be privy to.

Information security and the common law duty of confidentiality is of the utmost importance and so this policy has been formulated to relate to these areas and it should augment those policies and directives already established by participating NHS Trusts.

## **2. Policy Declaration**

It is the policy of *BRAIN UK* not to store what amounts to *patient* sensitive data on its database or within any paper records. Data such as names, addresses, post codes, dates of birth and dates of death are therefore excluded. However, to facilitate the process of case identification at each participating centre it has been decided to include laboratory numbers (or equivalent) linked to each case. Although the use of such linked anonymised ('pseudonymised') data can conceivably be used to identify an individual it can only be done so with extreme difficulty and only then with the connivance of the individual centre maintaining the key to such data. It is therefore the opinion of *BRAIN UK* that the use of laboratory numbers represents a 'reasonable level' of anonymisation and that data subsequently maintained on the database is anonymous for all subsequent practical purposes.

As data is disclosed from the medical records of the deceased there is no mechanism in law to ensure that the common law duty of confidentiality be maintained and important pieces of legislation, such as the Data Protection Act 1998 which refers only to living individuals, do not apply. In addition, there is a lack of case law regarding the right to confidentiality of the deceased. However, with no legal framework to protect the privacy and confidentiality rights of the deceased this does not mean that there is not an ethical onus to ensure that the deceased should have such rights maintained in death as they would be during life. It is therefore the policy of *BRAIN UK* that all reasonable measures should be taken to ensure that the common law duty of confidentiality is maintained by all staff and that there are mechanisms in place to mitigate against the inappropriate disclosure of patient sensitive data, whether that occurs inadvertently or with intent. In essence, it is the intention of *BRAIN UK* to apply the spirit of the Data Protection Act 1998 to the processing and storage of data, be it held electronically or as part of a paper record, and to incorporate the principles of the Caldicott Report in the use of confidential information.

In addition to data derived from deceased donors, data will also be collected from living individuals in the form of applicants wishing to obtain access to the tissue archives of participating centres for research purposes. The data obtained from this source will be limited to that required for *BRAIN UK* to be able to reach an informed opinion regarding the nature and quality of any proposed research. In this case the Data Protection Act 1998 does apply and this legislation will be adhered to in line with guidance and policies issued by the University of Southampton.

## **3. Principles of the Caldicott Report**

The Caldicott 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 additional documentation (*SOP 3: Information Technology Security Policy*).

#### **4. The Data Protection Act 1998**

The Data Protection Act sets out eight Data Protection Principles which are as follows:

- I. Personal data shall be processed fairly and lawfully,
- II. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes,
- III. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed,
- IV. Personal data shall be accurate and, where necessary, kept up to date,
- V. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes,
- VI. Personal data shall be processed in accordance with the rights of data subjects under the Act,
- VII. Appropriate technical and organisational measures will be undertaken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data,
- VIII. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or area ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

*BRAIN UK* is committed to abide by the not only the letter but also the spirit of the Data Protection Act 1998 (the 'Act') and to promote the highest possible standards of conduct mandated by the Act. **It is important to note that the *BRAIN UK* database will be using data solely derived from the deceased 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.** 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.

## **5. Strategy and Implementation**

The *BRAIN UK* Data Confidentiality and Security Policy, along with other relevant policy documents, should be effectively communicated to all staff through the following measures:

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 a signed copy is maintained in his or her training file.
3. Ensuring all staff with access to confidential data have an Honorary contract and relevant permissions with any participating NHS Trust.
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 both printed and electronic formats.

## **6. Staff Responsibilities**

All individuals working with sensitive or person-identifiable data should be aware of the following responsibilities:

- Locations where records are held should be secure at all times *e.g.* locking of doors, restriction of access, shutting down of computers if they are to be left for protracted periods of time.
- Access to information held on a computer should be controlled through the use of passwords. The sharing of passwords is forbidden even if the password holder is present during any access session.
- Identifiable material should not be left in locations where unauthorised personnel may gain access to it nor should such information be discussed in inappropriate locations.
- Sensitive and person-identifiable data should not be recorded on unauthorised computers *e.g.* home 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.
- It is every staff member's responsibility to ensure confidentiality and to be aware that any breaches may amount to gross misconduct and may lead to disciplinary action up to and including dismissal.
- Staff members must co-operate in training programmes provided and maintain an awareness of confidentiality and data security issues at all times.

## **7. Key Policy Elements**

This policy is based upon a number of core policy documents relating to patient confidentiality:

- Information Security Management: NHS Code of Practice (Department of Health, April 2007)
- NHS Information Governance: Guidance on Legal and Professional Obligations (Department of Health, September 2007)
- Confidentiality: NHS Code of Practice (Department of Health, November 2003)
- The Caldicott Committee: Report on the Review of Patient-Identifiable Information (Department of Health, December 1997)
- Protecting Patient Confidentiality (The Confidentiality and Security Advisory Group for Scotland, April 2002)

It is advisable that staff also familiarise themselves with the content of these documents and other key legislation (e.g. Access to Medical Records Act 1990) as part of their professional development plans.