DATA PROTECTION AND CONFIDENTIALITY

DOCUMENT NO.:	**POL003 v2.0**
AUTHOR:	**Lorn Mackenzie**
ISSUE DATE:	**15 September 2016**
EFFECTIVE DATE:	**29 September 2016**

1 INTRODUCTION

1.1 The Academic & Clinical Central Office for Research & Development (ACCORD) is a joint office comprising clinical research management staff from NHS Lothian (NHSL) and the University of Edinburgh (UoE).

1.2 The Data Protection Act 1998 (DPA) applies to all personal data which are held either electronically or in a manual filing system. The NHS Scotland Confidentiality Code of Practice and the Caldicott principles apply to health and social care organisations, with respect to the way patient/participant identifiable data or personal information is handled.

1.3 ACCORD staff members hold personal information about individuals such as investigators, other research staff members and ACCORD staff members. Investigators and study research staff may hold personal information about study participants.

1.4 Such data must only be processed in accordance with this policy, UoE Data Protection Policy and NHSL Data Protection Policy, where applicable. The UoE Data Protection Policy and NHSL Data Protection Policy set out the purposes for which the UoE and NHSL holds and processes personal data respectively.

1.5 It is the responsibility of ACCORD staff to maintain up-to-date information security and governance training in accordance with the requirements of the institution that employs them i.e. NHSL or UoE, ensuring that NHSL requirements are followed when patient information is processed.

1.6 It is the responsibility of researchers, with permission to access patient information, to treat data with complete confidentiality and to store, analyse and process patient information in accordance with applicable NHSL policies.

2 SCOPE

2.1 This policy is applicable to researchers working within NHSL and/or UoE, conducting research involving NHSL participants, who have access to patient/participant identifiable data or personal information.

2.2 This policy is also applicable to ACCORD staff members who have access to patient/participant identifiable data or personal information.

3 POLICY

3.1 Principles of the Data Protection Act

3.1.1 The principles describe how data can be processed in compliance with the law. 'Processing' includes obtaining, recording, holding, transferring or storing information and carrying out any operations on the data, including adaptation, alteration, use, disclosure, transfer, erasure, and destruction. All ACCORD staff and researchers who process patient/participant identifiable data or personal information will comply with the eight data protection principles:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subject under the DPA.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.
8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.2 Responsibility for Data Protection

The responsibility for upholding the DPA and adhering to this policy resides with all ACCORD staff and researchers who process data and have access to personal information.

3.2.1 NHSL has appointed a Data Protection Officer from the Information Management and Technology (IM&T) Department. NHSL has also set up an Information Governance Steering Group and one of their tasks is to review the NHSL Data Protection Policy on an annual basis. NHSL will regularly review and audit the way data is processed. In addition, NHSL has committed to ensuring that anyone wishing to enquire about their personal data knows whom to approach. Furthermore, NHSL has committed to ensuring that such queries are dealt with promptly and courteously.

3.2.2 UoE has appointed a Data Protection Officer and any request for access to personal data held by UoE must be forwarded to the Data Protection Officer. Responsibility for UoE compliance with the DPA is delegated to relevant Heads of Schools. UoE will audit DPA compliance on a periodic basis.

3.3 Caldicott Principles

3.3.1 The 7 Caldicott Principles for handling patient/participant identifiable data or personal identifiable information are:

Principle 1. Justify the purpose(s) for using confidential information
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2. Don't use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4. Access to personal confidential data should be on a strict need-to-know basis.
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5. Everyone with access to personal confidential data should be aware of their responsibilities.
Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7. The duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information in the best interest of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

3.3.2 Investigators and ACCORD staff are responsible for ensuring that study operational records, including patient/participant identifiable data or personal information are handled and stored in compliance with the aforementioned principles and according to SOP GS008 (Caldicott Application Process). More specifically, records must be protected from unauthorised access; they also must be robust and held in a secure fashion with appropriate audit trails in place. Records must also be accessible to appropriately delegated individuals, competent authority inspectors, auditors and monitors appointed by the study sponsor, where participant consent has been given.

3.3.3 Investigators are also ultimately responsible for the accuracy and completeness of the records that they collect, process and store. Moreover, investigators must ensure that provisions are in place to retain study records for the required period.

3.3.4 Each NHS organisation is required to have a Caldicott Guardian. The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian also plays a key role in ensuring that the NHSL satisfies the highest practicable standards for handling patient identifiable information. If the circumstances of a study dictate that there will be access to patient identifiable data for research purposes other than by the direct care team, or transfer of identifiable data out with NHSL without the patient's knowledge or consent, then Caldicott approval will be sought (GS008 Caldicott Application Process). This includes access to records of the deceased.

3.4 Community Health Index (CHI)

3.4.1 CHI numbers have unique status and contain additional identifiable information. CHI numbers should not be used outside the NHS. CHI Guardian approval for CHI numbers to leave NHSL must be sought via the Caldicott Guardian Office or Public Benefit Privacy Panel (PBPP) if permission is sought for CHI to be transferred out of the NHS from more than one NHS Health Board in Scotland.

4 REFERENCES AND RELATED DOCUMENTS

- University of Edinburgh Data Protection Policy

- NHS Lothian Data Protection Policy
- NHS Scotland Confidentiality Code of Practice
- The Data Protection Act 1998
- Information Governance Review 2013 (Caldicott2 Review)
- NHS Lothian Records Management Policy
- SOP GS008 Caldicott Application Process

5 DOCUMENT HISTORY

Version Number	Effective Date	Reason for Change
1.0	23 DEC 2010	Minor administrative corrections
1.1	10 MAR 2011	Minor administrative corrections
2.0	29 SEPT 2016	Revised Caldicott Principles and NHSL policy on the transfer for CHI numbers.

6 APPROVALS

Sign	Date
Signature kept on file AUTHOR: Lorn Mackenzie, QA Coordinator, NHSL, ACCORD	
Signature kept on file APPROVED Susan Shepherd, Head of Research Governance, NHSL, ACCORD:	
Signature kept on file AUTHORISED: Heather Charles, QA Manager, NHSL, ACCORD	