DATA PROTECTION AND CONFIDENTIALITY

DOCUMENT NO.:	**POL003 v3.0**
AUTHOR:	**Lorn Mackenzie**
ISSUE DATE:	**09 JUL 2018**
EFFECTIVE DATE:	**23 JUL 2018**

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 General Data Protection Regulation (GDPR) and the Data Protection Act (2018), hereafter referred to as the Data Protection Legislation, applies to all personal data which are held either electronically or in a manual filing system.

1.3 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.

1.4 ACCORD holds personal information about individuals such as Investigators, research staff and ACCORD personnel. Investigators and study research staff may hold personal information about study participants.

2 SCOPE

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

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

3 POLICY

3.1 Principles of Data Protection

3.1.1 The Data Protection Legislation describes how personal identifiable data can be collected and processed in compliance with the law.

3.1.2 'Processing' includes obtaining, recording, holding, transferring or storing/archiving information.

3.1.3 ACCORD staff and researchers who process patient/participant identifiable data or personal information for research purposes will;

- Do so in compliance with Data Protection Legislation, this Policy and

NHSL and/or UoE Data Protection Policies,
- 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,
- Treat personal data with complete confidentiality and store, analyse, transfer and archive this information in accordance with applicable NHSL policies.

3.2 Lawfulness, Fairness & Transparency Principles

3.2.1 ACCORD staff and NHSL/UoE researchers who process patient/participant identifiable data or personal information will;
- Have lawful bases, under the Data Protection Legislation, for doing so, including conditions for processing special category data,
- Consider how the processing may affect the individuals concerned and can justify any adverse impact,
- Only handle people's data in ways they would reasonably expect, or can explain why any unexpected processing is justified,
- Not deceive or mislead people when collecting their personal data,
- Be open and honest, and comply with the transparency obligations of the right to be informed.

3.3 Organisational Responsibilities

3.3.1 NHSL and the UoE have appointed a Data Protection Officer in accordance with Data Protection Legislation.

3.3.2 NHSL has an Information Governance Working Group and one of their tasks is to review the NHSL Data Protection Policy on an annual basis.

3.4 Caldicott Principles

3.4.1 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 Patient Identifiable Information: Caldicott Approval & Information Governance Review). This includes access to records of the deceased.

3.4.2 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.

3.4.3 ACCORD staff and NHLS/UoE researchers are responsible for;

- Ensuring that research records, including patient/participant identifiable data or personal information are handled and stored in compliance with the aforementioned principles and according to ACCORD SOP GS008

(Patient Identifiable Information: Caldicott Approval & Information Governance Review),

- Accuracy and completeness of the records that they collect, process and store,
- Ensuring that provisions are in place to retain study records for the required period.

3.4.4 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.

3.5 Community Health Index (CHI)

3.5.1 The CHI is a population register, which is used in Scotland for health care purposes. The CHI number uniquely identifies a person on the index. Rationale for collecting CHI numbers will be discussed/agreed with the Sponsor/R&D and Caldicott Guardian, if required.

3.5.2 The CHI number should remain within the NHS wherever possible.

3.5.3 Caldicott Guardian approval must be sought via the Caldicott Guardian Office or Public Benefit Privacy Panel (PBPP) if a researcher wishes to transfer CHI (or any person identifiable data) out of the NHS, without explicit patient consent to do so.

3.5.4 When transferring personal identifiable information (including CHI) out of the NHS, the mechanism for transfer, storage and destruction must be considered, and advice will be sought from NHS Lothian R&D and/or eHealth, where appropriate.

3.6 Data Breaches

3.6.1 Breaches in Data Protection Policies and Legislation will be reported to the appropriate Data Protection Officer in accordance with NHSL and UoE Policies and Procedures.

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 2018
- Information Governance Review 2013 (Caldicott2 Review)
- NHS Lothian Records Management Policy
- HRA Guidance on the GDPR

- SOP GS008 Patient Identifiable Information: Caldicott Approval & Information Governance Review

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.
3.0	23 JUL 2018	Updated to align with the new Data Protection Legislation

6 APPROVALS

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