

Data Protection and Confidentiality

DOCUMENT NO.:	POL003 v5.0
AUTHOR:	Pavlina Yaneva McGovern
ISSUE DATE:	10 DEC 2024
EFFECTIVE DATE:	20 DEC 2024

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 UK 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 hard copy 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 health data and/or personal identifiable information about study participants.

2 Scope

- 2.1 This policy is applicable to researchers working within NHSL and/or UoE, conducting research involving healthy volunteers, NHSL staff or patients (i.e. research participants), who have access to personal information (this includes 'personal identifiable information' (PII) and pseudonymised data)
- 2.2 This policy is also applicable to ACCORD personnel who have access to personal information (this includes 'personal identifiable information' (PII) and pseudonymised data) of research participants and NHSL/UoE staff.

3 Policy

3.1 Principles of Data Protection

- 3.1.1 The Data Protection Legislation describes how personal/identifiable information can

be collected and processed in compliance with the law.

3.1.2 In relation to personal data, 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means), such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

3.1.3 ACCORD staff and researchers who process 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/identifiable information with complete confidentiality and store, analyse, transfer and archive this information in accordance with applicable NHSL/UoE policies.

3.2 Lawfulness, Fairness & Transparency Principles

3.2.1 ACCORD staff and NHSL/UoE researchers who process patient/participant personal/identifiable 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 personal information in ways they would reasonably expect, or can explain why any unexpected processing is justified,
- Not deceive or mislead people when collecting their personal information,
- Be open and honest and comply with the transparency obligations of the right to be informed.

3.2.2 ACCORD office Privacy Notices can be accessed on the ACCORD website; <https://www.accord.ed.ac.uk/data-protection/our-privacy-notices>

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 information for research purposes other than by the direct care team, or transfer of identifiable information out with NHSL without the patient's knowledge or consent, then Caldicott approval will be sought (GS008 Processing Personal Information: Caldicott Approval & Information Governance Review). This includes access to records of the deceased.
- 3.4.2 The 8 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.

Principle 8. Inform patients and service users about how their confidential information is used

Steps should be taken to ensure patients and service users understand how and why their confidential information is used. They should always be provided with accessible, relevant and appropriate information.

- 3.4.3 ACCORD staff and NHLS/UoE researchers are responsible for;
 - Ensuring that research records, including NHSL staff or patient personal information is handled and stored in compliance with the aforementioned principles and according to ACCORD SOP GS008 (Processing Personal 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 Caldicott Guardian Approval

- 3.5.1 Caldicott Guardian approval must be sought for any study where there will be access to NHS patient personal data, or transfer/storage of NHS PII out with NHSL (which may include processing the Community Health Index (CHI) number without consent. This includes access to records of the deceased.
- 3.5.2 The CHI number has unique status in Scotland. CHI is a unique identifier that is disclosive (includes date of birth, gender and other information). If CHI is requested, rationale for collecting CHI numbers should be discussed/agreed with the Sponsor/local R&D and Caldicott Guardian, where appropriate.
- 3.5.3 The CHI number should remain within the NHS wherever possible.
- 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 approval will be sought from NHS Lothian R&D and/or eHealth, where appropriate.

3.6 Data Protection Impact Assessment (DPIA)

- 3.6.1 A DPIA is not mandatory for each individual research study.
- 3.6.2 ACCORD will determine whether the design of a study and how personal data is processed, complies with local policies and procedures detailed in the NHSL R&D generic DPIAs. Where compliance in all these areas is confirmed, the relevant generic DPIA will apply.
- 3.6.3 A study specific DPIA may be required depending on study design and personal data processing requirements.

3.7 Data Breaches

- 3.7.1 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 General Data Protection Regulation (EU) 2016/679 as implemented under the Data Protection Act 2018
- Information Governance Review 2013 (Caldicott2 Review)
- NHS Lothian Records Management Policy
- SOP GS008 Processing Personal Information: Caldicott Approval & Information Governance Review
- Terms of Reference: Delegation of Authority from the NHS Lothian Caldicott Guardian to NHS Lothian R&D for Review and Approval of Caldicott Applications for Research
- [Our Privacy Notices | Accord](#)
- Research & Development (R&D) Generic Data Protection Impact Assessment – NHS Lothian and the University of Edinburgh Co-Sponsored Studies
- Research & Development (R&D) Generic Data Protection Impact Assessment – Studies Singly Sponsored by NHS Lothian
- Research & Development (R&D) Generic Data Protection Impact Assessment – Studies Hosted by NHS Lothian

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 NHS Lothian policy on the transfer for CHI numbers.
3.0	23 JUL 2018	Updated to align with the new Data Protection Legislation
4.0	05 AUG 2022	Reference to data protection legislation amended in sections 1.2 and 4. Change of author and approver. Update to title of SOP GS008 in sections 3.4.1, 3.4.3 and 4. Minor changes when referring to personal/identifiable data throughout.
5.0	20 DEC 2024	Information on Data Protection Impact Assessment (DPIA) added to 3.6. Reference to ACCORD privacy notices also added at 3.2.2. Minor changes throughout

6 Approvals

Sign	Date
<p><u>P.Y. McGovern</u> P.Y. McGovern (Dec 9, 2024 13:49 GMT)</p> <p>AUTHOR: Pavlina Yaneva McGovern, R&D Information Governance Lead, NHSL, ACCORD</p>	Dec 9, 2024
<p><u>Heather Charles</u> Heather Charles (Dec 9, 2024 13:40 GMT)</p> <p>APPROVED: Heather Charles, Head of Research Governance, NHSL, ACCORD</p>	Dec 9, 2024
<p><u>L. Mackenzie</u></p> <p>AUTHORISED: Lorn Mackenzie, QA Manager, NHSL, ACCORD</p>	Dec 9, 2024

POL003 Data Protection and Confidentiality











v5.0

Final Audit Report

2024-12-09


Created:	2024-12-09 (Greenwich Mean Time)
By:	Roisin Ellis (v1relli8@exseed.ed.ac.uk)
Status:	Signed
Transaction ID:	CBJCHBCAABAAEKbBerenLQxLhaPIOUBsvBCyt2lpbcmP

"POL003 Data Protection and Confidentiality v5.0" History

-  Document created by Roisin Ellis (v1relli8@exseed.ed.ac.uk)
2024-12-09 - 1:24:50 PM GMT- IP address: 62.253.82.232
-  Document emailed to pavlina.y.mcgovern@nhslothian.scot.nhs.uk for signature
2024-12-09 - 1:26:12 PM GMT
-  Document emailed to heather.charles@nhslothian.scot.nhs.uk for signature
2024-12-09 - 1:26:12 PM GMT
-  Document emailed to Lorn Mackenzie (lorn.mackenzie@nhslothian.scot.nhs.uk) for signature
2024-12-09 - 1:26:12 PM GMT
-  Email viewed by Lorn Mackenzie (lorn.mackenzie@nhslothian.scot.nhs.uk)
2024-12-09 - 1:35:00 PM GMT- IP address: 52.102.18.37
-  Document e-signed by Lorn Mackenzie (lorn.mackenzie@nhslothian.scot.nhs.uk)
Signature Date: 2024-12-09 - 1:35:10 PM GMT - Time Source: server- IP address: 82.4.25.149
-  Email viewed by heather.charles@nhslothian.scot.nhs.uk
2024-12-09 - 1:40:20 PM GMT- IP address: 52.102.18.53
-  Signer heather.charles@nhslothian.scot.nhs.uk entered name at signing as Heather Charles
2024-12-09 - 1:40:35 PM GMT- IP address: 62.253.82.231
-  Document e-signed by Heather Charles (heather.charles@nhslothian.scot.nhs.uk)
Signature Date: 2024-12-09 - 1:40:37 PM GMT - Time Source: server- IP address: 62.253.82.231
-  Email viewed by pavlina.y.mcgovern@nhslothian.scot.nhs.uk
2024-12-09 - 1:49:01 PM GMT- IP address: 62.253.82.232

 Signer pavlina.y.mcgovern@nhslothian.scot.nhs.uk entered name at signing as P.Y.McGovern

2024-12-09 - 1:49:27 PM GMT- IP address: 62.253.82.232

 Document e-signed by P.Y.McGovern (pavlina.y.mcgovern@nhslothian.scot.nhs.uk)

Signature Date: 2024-12-09 - 1:49:29 PM GMT - Time Source: server- IP address: 62.253.82.232

 Agreement completed.

2024-12-09 - 1:49:29 PM GMT