Processing Personal Information: Caldicott Approval & Information Governance Review

Document No.:	GS008 v6.0
Author:	Pavlina Yaneva McGovern
Issue Date:	24 APRIL 2025
Effective Date:	08 MAY 2025

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 (UK GDPR) enforces strict legal rules to the storage, maintenance and access to personal information.

1.3 Pseudonymisation refers to techniques that replace, remove or transform information that identifies individuals, and keep that information separate. Data that has undergone pseudonymisation remains personal data and is in scope of data protection law.

1.4 A Caldicott Guardian is a senior person within NHSL responsible for protecting the confidentiality of people's health and care information and making sure it is used properly, in accordance with the Caldicott Principles. This includes the use of personal identifiable information by NHS staff, partner NHS organisations and non-NHS partner organisations e.g. Universities.

1.5 The Community Health Index (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.

2 Purpose

2.1 The purpose of this SOP is to outline the procedure that Researchers and ACCORD personnel must follow if a research study includes the collection, transfer and storage of any personal information (this includes personal identifiable information' (PII) and pseudonymised data) of NHSL staff or patients, (including CHI numbers) or any other participant or individual involved in the study what we hold.

3 Scope

3.1 This SOP applies to Researchers, the R&D Information Governance Lead, or designee, NHSL and UoE Research Governance staff performing Sponsorship and R&D Governance review of research studies and the R&D Admin team.

4 Responsibilities

4.1 It is the responsibility of the Researcher, or designee, to complete an application for Caldicott or Public Benefit and Privacy Panel (PBPP) approval, if required.

4.2 It is the responsibility of the Researcher, or designee, to provide or arrange provision of information to allow the NHSL Information Governance (IG)/IT Security team to undertake review of IG/IT security arrangements (whether Caldicott/PBPP approval is needed or not), if required.

4.3 It is the responsibility of the Sponsorship Reviewer to determine (in accordance with ACCORD SOP GS003 Sponsorship Approval);

- If personal information is being processed e.g. accessed or collected,
- What PII information is being processed e.g. name, date of birth, CHI, contact details,
- If this data is being transferred/stored out with NHSL or the NHS,
- If PII or pseudonymised data is leaving the UK and/or the EEA i.e. in which country will the data be held,
- How the data will be transferred and where it will be stored,
- Who will access this data and for how long,
- If the data processing involves a mobile device, application, database or cloud-based data capture system,
- Whether Caldicott or PBPP approval is required,
- Whether IG/IT Security review is required,
- Whether data security arrangements comply with NHSL policies (in conjunction with NHSL IG/IT Security where required). Further clarification will be sought from the R&D Information Governance Lead, or designee or IG/IT if required.

4.4 The delegated Caldicott Reviewer is primarily the R&D Information Governance Lead. This role can also be fulfilled by the Deputy R&D Director, the Principal R&D Manager or the Head of Research Governance (NHSL). It is the responsibility of the R&D Information Governance Lead, or designee to:

- Log and review local Caldicott applications and issue approval, where appropriate.
- Track local Caldicott applications and provide quarterly reports to the NHSL Caldicott Guardian detailing all local Caldicott approvals granted.
- Provide guidance to researchers and ACCORD personnel on requirements for NHSL Caldicott and IG/IT Security review.
- Maintain a log of NHSL IG/IT Security reviews undertaken for applications managed under delegated Caldicott review.
- Review (and approve where appropriate) checklists for Caldicott Proportionate Review (Use of Portable Media Checklist).

4.5 The NHSL R&D Governance Reviewer is responsible for ensuring that all items detailed in section 4.3 have been addressed by the Sponsor Reviewer for studies Sponsored by NHSL and/or UoE. If they have not, the NHSL Governance Reviewer must address these prior to R&D Management Approval (SOP GS001 & GS015), in consultation with their Line Manager.

4.6 For studies hosted by NHSL, the R&D Governance Reviewer is responsible for addressing all items detailed in section 4.3, and escalating any issues as described in section 4.5.

4.7 The R&D Information Governance Lead, or designee, is responsible for escalating any issues with the Principal R&D Manager, the Head of Research Governance (NHSL) or Deputy R&D Director, where appropriate.

4.8 The R&D Information Governance Lead, or designee is responsible for filing the authorised Use of a Portable Media Checklist or the Caldicott or IG/IT review approval letter in the appropriate project folder on the NHSL R&D shared drive (Research & Development\Projects) and ACCORD SharePoint (for studies sponsored by UoE/NHS Lothian).

5 Procedure

For research studies reviewed within ACCORD, that are deemed to require further scrutiny in relation to Caldicott principles or IG/IT security issues, the Sponsorship Reviewer and/or the

R&D Governance Reviewer will advise the Researcher to engage with the R&D Information Governance Lead, or designee and/or NHSL IG/IT Security, where appropriate.

5.1 Local Caldicott – Single Site

5.1.1 A Researcher will seek local Caldicott approval 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 CHI where this is not normally identified and processed by the clinical care team through standard procedures) without consent. This includes access to records of the deceased. Caldicott approval is also required where portable media are used to store or transfer PII, including for example USB devices, iPads and recording devices (see section 5.4), even where consent is in place to do so.

5.1.2 The Sponsorship or R&D Governance Reviewer will request that the Researcher submits a Local Caldicott and/or Information Governance Application Form (GS008-F01) to ACCORD (loth.accord@nhs.scot).

5.1.3 The Researcher must complete all sections (A, B and C) of the Local Caldicott and/or Information Governance Application Form (GS008-F01) prior to submission to ACCORD.

5.1.4 On receipt of the completed application, the R&D Information Governance Lead, or designee will allocate a Caldicott reference number and add an entry into the Caldicott Enquiries and Applications tracker held on the NHSL R&D shared drive (Research & Development/Research Governance/Caldicott/Projects & Enquiries). This reference number will be added to the Caldicott application form and included in all correspondence.

5.1.5 The R&D Information Governance Lead, or designee will review the completed form to ascertain if the proposed study procedures comply with the Caldicott principles, the relevant NHSL R&D Generic Data Protection Impact Assessment (DPIA) for Research (see SOP GS001/GS015 R&D Governance Review of Non-Commercial/Commercial Research and GS003 Sponsorship Approval), and the NHSL Digital IT Security Policy and Data Protection Policy.

5.1.6 When compliance is confirmed, the R&D Information Governance Lead, or designee will grant Caldicott approval by letter. The letter will set out any conditions or recommendations and will be e-mailed, together with the approved Caldicott application, to the researcher.

5.1.7 Approval will be issued by the R&D Information Governance Lead, or designee, and the Sponsorship and/or R&D Governance Reviewer will be copied in the e-mail, as will loth.accord@nhs.scot .

5.1.8 Where the original application does not comply fully with the Caldicott principles, the relevant R&D Generic DPIA for Research, and/or the NHSL Digital IT Security Policy and Data Protection Policy, the R&D Information Governance Lead, or designee, Sponsorship or R&D Governance Reviewer will assist the applicant, where possible, to address the outstanding issues to ensure compliance.

5.1.9 Where the application continues to have outstanding issues and/or to be out of scope for delegated review and approval, the researcher will be advised that the Caldicott application needs to be escalated to the NHSL Caldicott Guardian by the R&D Information Governance Lead, or designee (loth.caldicottguardian@nhs.scot).

5.1.10 The rationale for escalation will be documented by the R&D Information Governance Lead, or designee in the Caldicott Enquiries and Application tracker on the NHSL R&D shared drive, and the application provided to the NHSL Caldicott Guardian by e-mail.

5.1.11 The R&D Information Governance Lead, or designee, will record the outcome of the review by the NHSL Caldicott Guardian in the Caldicott Enquiries and Application tracker on the NHSL R&D shared drive, and inform the researcher and the Sponsorship and/or R&D Governance Reviewer, where applicable.

5.1.12 Confirmation of Sponsorship can be issued prior to local Caldicott approval but R&D management approval cannot be issued prior to Caldicott approval unless agreed with the R&D Senior Management Team (SMT). This is a local issue and will not hold up any R&D study-wide reviews.

5.1.13 A summary of each application approved under delegated authority is added to the approvals report maintained on the Caldicott folder on the NHSL R&D shared drive (Research & Development/Research Governance/Caldicott/Projects & Enquiries/Projects-Approved). The reports are flagged to the NHSL Caldicott Guardian by the R&D Information Governance Lead, or designee on a quarterly basis by email sent to loth.caldicottguardian@nhs.scot.

5.2 National Caldicott

5.2.1 If the study is multi-centre involving more than one site in Scotland, and the collection, transfer and storage of NHS patient personal data has not been consented, the researcher must make an application to the PBPP.

5.2.2 The Sponsorship or R&D Governance Reviewer will provide the researcher with details of the PBPP website (http://www.informationgovernance.scot.nhs.uk/pbpphsc/), which contains contact details (phs.edris@phs.scot / 0131 275 7333), guidance and an application form.

5.2.3 If there are sites in England or Wales, the researcher must seek approval from the Confidentiality Advisory Group (CAG).

5.2.4 If there are sites in Northern Ireland, the researcher must seek approval from the Privacy Advisory Committee (PAC).

5.3 NHSL IG/IT Risk Assessment: Personal Identifiable Information (PII)

5.3.1 A study will undergo IT Security risk assessment when it;

- Involves transfer of participant PII out with NHSL (e.g. name, date of birth, CHI, contact information),
- Uses new software on NHSL systems (e.g. eConsent systems),
- Involves storage of PII on mobile devices/online platforms,
- Uses Microsoft Teams (or other videoconferencing systems) for research purposes.
- Involves Artificial Intelligence (AI).

5.3.2 If the Sponsorship or R&D Governance Reviewer believes that a study requires assessment by IG/IT Security, they will refer to the R&D Information Governance Lead, or designee, for further guidance/action. It should be made clear which system(s) require IT Security risk assessment as not all aspects may require review.

5.3.3 The R&D Information Governance Lead, or designee, will check if the system flagged for IT Security risk assessment has been risk assessed previously. If so, the IT Security re-approval of systems process will be followed where possible (Information Governance Approval Process for R&D).

5.3.4 The R&D Information Governance Lead, or designee, can seek further guidance from R&D IT Security Project Manager if required, prior to sending the study for review by IT Security.

5.3.5 The study team will be informed if their study requires an IT Security risk assessment and can contact the R&D IT Security Project Manager directly for updates (contact details will be provided by the R&D Information Governance Lead, or designee, or by the Sponsorship/R&D Governance Reviewer) or by e-mailing loth.informationgovernance@nhs.scot. NHSL personnel can also log a call using the online Assyst portal system (e85050). The reference number issued by NHSL IT Security should be used in all correspondence relating to this query.

5.3.6 The R&D IT Security Project Manager, or designee, will work with the Researcher to complete the necessary NHSL IT Security risk assessment in accordance with NHSL Approval Triage Process for R&D (this is covered under separate NHSL Digital & IT Security SOPs, and out with the scope of this SOP). The outcome of this process is a risk assessment that will be e-mailed to the R&D Information Governance Lead, or designee for review.

5.3.7 The R&D Information Governance Lead, or designee, will send the IT Security risk assessment mandatory requirements to the Researcher (and/or Sponsor or 3rd party provider) via e-mail.

5.3.8 Upon receipt of the mandatory requirements, the Researcher (or Sponsor or 3rd part provider) must provide written confirmation via e-mail on whether the organisation responsible for processing PII is able to comply with any recommendations made by NHSL IG/IT Security or not. If required, additional clarification can be sought on the mandatory requirements by contacting the R&D IT Security Project Manager directly.

5.3.9 Once it has been confirmed that mandatory requirements can be met, the R&D Information Governance Lead, or designee, will issue a NHSL R&D IT Security risk assessment letter including the mandatory requirements from the IT Security risk assessment to the Researcher.

5.3.10 Where the mandatory requirement cannot be met, the R&D Information Governance Lead will escalate this to the R&D SMT for consideration. This may be further escalated to the NHSL Caldicott Guardian if considered appropriate.

5.3.11 Where the IT Security risk assessment is linked to a Caldicott application, this will be taken into consideration by the R&D Information Governance Lead, or designee prior to issue of Caldicott approval.

5.3.12 Confirmation of sponsorship can be issued prior to receipt of NHSL IT Security risk assessment and confirmation that mandatory requirements can be met, however the R&D Information Governance Lead must have received confirmation that mandatory requirements can be met prior to R&D management approval unless agreed with the R&D SMT.

5.3.13 This is a local issue only and should not hold up any study-wide reviews (see ACCORD SOP GS001 & GS015).

5.4 NHSL IG/IT Risk Assessment: Pseudonymised Data

5.4.1 In some instances, an IT Security risk assessment may be required when pseudonymised data is leaving NHSL e.g. where a study is co-sponsored by UoE/NHSL or singly sponsored by NHSL and pseudonymised data is being transferred to another country that does not have a data protection adequacy agreement with the UK government that covers data processing for research (see Appendix 1). Further advice can be sought from the R&D Information Governance Lead.

5.4.2 Where an IT Security risk assessment is required for the transfer of pseudonymised data, it will follow the process detailed in section 5.3.

5.5 Proportionate Caldicott Review for Portable Media

5.5.1 The NHSL Digital and IT Security Policy dictates that any use of portable media to collect personal data requires local Caldicott approval.

5.5.2 Where the R&D Governance Reviewer identifies a study involving the use of portable media, they will complete the Use of Portable Media Checklist (GS008-F02) during the R&D governance review using the information detailed in the study documents. This checklist will only be completed in the absence of a local Caldicott application form where any PII processed as part of the research study will remain within NHSL. If any

PII is transferred and/or stored outside NHSL, the checklist should not be used and instead the study should be referred for IG/IT Security for review (see section 5.3).

5.5.3 The R&D Governance Reviewer will send the completed checklist (GS008-F02) to the R&D Information Governance Lead, or designee.

5.5.4 Where the R&D Governance Reviewer has been able to answer 'Yes' to all questions in the checklist (GS008-F02) and there are no outstanding issues, the R&D Information Governance Lead, or designee will sign off and file the checklist in the appropriate project folder on the NHSL R&D shared drive (Research & Development\Projects).

5.5.5 Where the R&D Governance Reviewer has not been able to answer 'Yes' to all questions and/or there are any outstanding issues, the R&D Governance Reviewer may seek advice from the R&D Information Governance Lead, or designee. If required, the Investigator may be requested to complete a full Caldicott application (as detailed in section 5.1) or liaise with the R&D IT Security Project Manager to complete an IT Security Risk Assessment as detailed in section 5.3.

5.6 Record Retention

5.6.1 All studies referred for Caldicott or IG/IT Security review will be allocated a Caldicott reference number and added to the Caldicott enquiries and applications tracker kept on the NHSL R&D shared drive (Research & Development\Research Governance\Caldicott\Projects and Enquiries). The R&D Information Governance Lead, or designee, will maintain this tracker.

5.6.2 The R&D Information Governance Lead, or designee, will retain all associated correspondence, outcomes of the IT Security risk assessments or completed Caldicott application forms on the NHSL R&D shared drive (Research & Development\Research Governance\Caldicott\Projects and Enquiries\Projects – Approved). The signed approval letters and confirmation of compliance e-mails will be filed in the appropriate project folder on the NHSL R&D shared drive (Research & Development\Projects).

5.6.3 The Sponsorship Reviewer will file a hard copy of the completed application form and approval letter in the Trial Master File/Sponsor File (CTIMPs and studies that have undergone Combined Risk Assessment in accordance with SOP GS002) and/or an electronic copy in the relevant study folder on the ACCORD SharePoint (all studies).

5.7 Review of Data Storage Locations and IT Systems

5.7.1 All NHSL IG/IT Security will maintain an inventory of safe systems, reviewed for research, in accordance with NHSL Digital & IT Procedure for Re-approving systems used by NHSL.

5.7.2 Where the Researcher, Sponsor Reviewer, R&D Governance Reviewer or R&D Information Governance Lead, or designee, is unsure if a system has already been risk assessed by NHSL IT Security, they must contact the R&D Information Governance Lead, the R&D IT Security Project Manager or e-mail loth.informationgovernance@nhs.scot.

5.7.3 Where the system has been risk assessed before, IG/IT Security will issue a Re-approved System Record containing basic information about the service/system gathered during the last assessment to the person who logged the call. That person will be required to confirm that the Re-approved System Record is accurate for this subsequent use of the system and if not accurate, any differences noted and returned to IT Security.

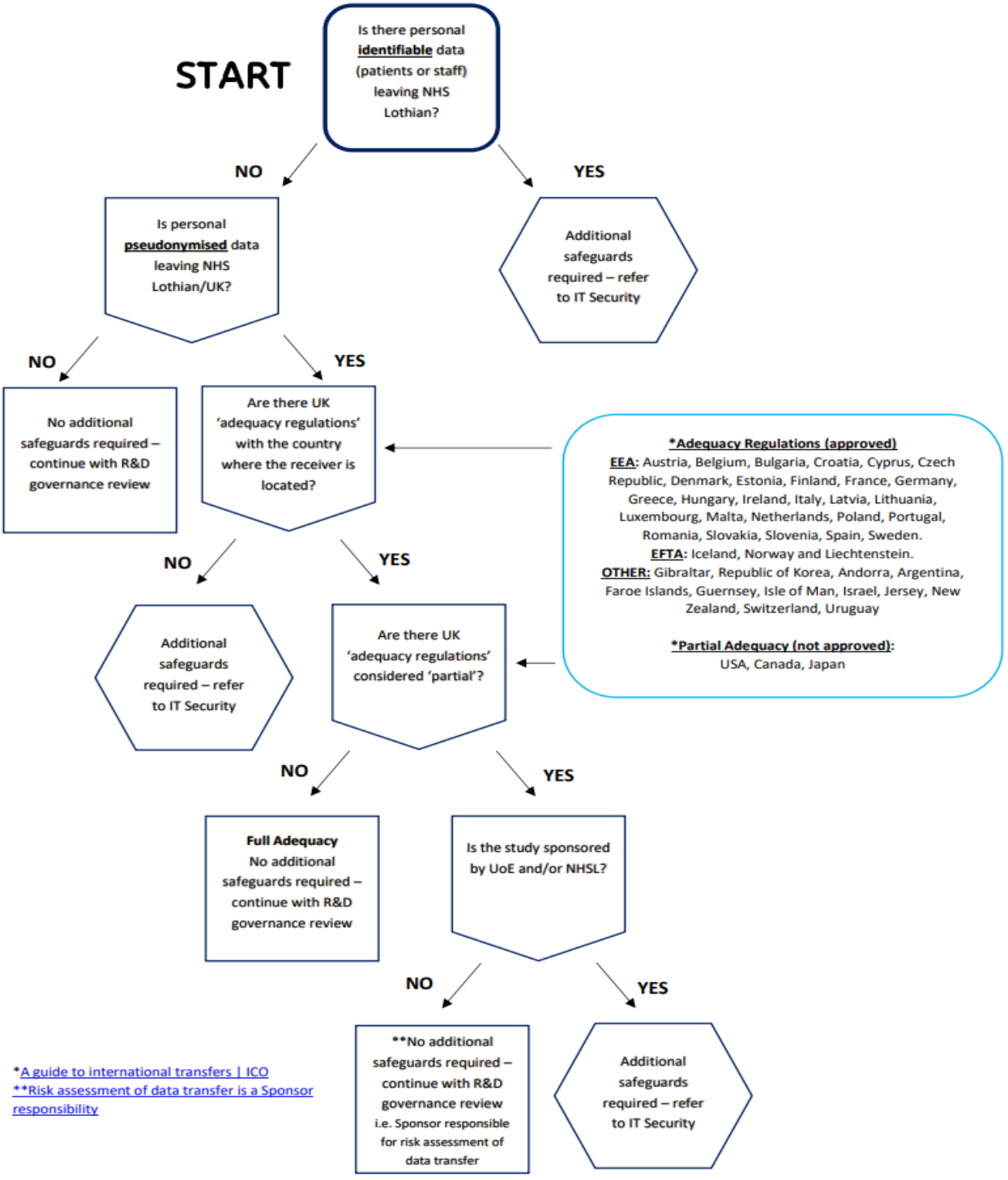
5.7.4 IG/IT Security will confirm if the Researcher can proceed with using the product based on the information provided following review of the Re-approved System Record and any additional information provided.

6 References and Related Documents

- GS008-F01 Local Caldicott and/or Information Governance Application Form
- GS008-F02 Use of Portable Media Checklist
- GS001 R&D Governance Review of Non-Commercial Studies
- GS003 Sponsorship Approval
- GS015 R&D Governance Review of Commercial Studies
- 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 v2.0
- 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

- CEL 25 2012 NHS Scotland Mobile Data Protection Standard http://www.sehd.scot.nhs.uk/mels/CEL2012_25.pdf

7 Appendix 1: Processing Personal Data (Identifiable or Pseudonymised)



8 Document History

Version Number	Effective Date	Reason for Change
1.0	19 SEP 2016	New SOP
2.0	01 AUG 2017	The title and author of this SOP has changed. All sections of this SOP have been updated to reflect current procedure. This includes determining if identifiable data is being collected, transferred, and stored at the Sponsorship review stage where possible and confirmed at R&D review. The procedure has been expanded to include additional requirements with regards to NHSL Information Governance and Security, which includes updated to GS008-F01 and additional guidance added as Appendix 1 & 2.
3.0	23 MAR 2021	Change in SOP title. Changes to all section of this SOP with inclusion of R&D Admin Team responsibilities, reference to Information Governance policies and procedures and the NHSL R&D Generic DPIA. Addition of a section on Proportionate Caldicott Review for Use of Portable Media and associated form.
4.0	11 NOV 2022	Change of author. Sections updated includes reference to the UK GDPR in section 1.2, reference to the term 'personal data' in section 2.1, and reference to the limited use of Microsoft Teams for research purposes in section 5.3.1. The procedure for sharing reports with the Caldicott Guardian has been updated in Section 4.1.13. A new process of escalation has been introduced in sections 4.5 and 5.3. The processes for record retention have been updated in sections 4.7, 5.4 and 5.5. Other minor changes throughout the document.
5.0	01 DEC 2024	SOP title and approver updated. Definition of pseudonymisation added to introduction and clarification around IT Security risk assessment requirements for processing identifiable and

		pseudonymised data and where a study involves AI. Addition of flow diagram in Appendix 1. Minor changes throughout including updates to e-mail addresses. Reference to 3 R&D generic DPIAs for research added to section 6.
6.0	08 MAY 2025	Section 5.4.1 and Appendix 1 updated to clarify when an IT Security risk assessment is required when pseudonymised data is being transferred out with NHSL.

9 Approvals

Sign	Date
Pavlina Yaneva (McGovern) Pavlina Yaneva (McGovern) (Apr 23, 2025 12:19 GMT+1) AUTHOR: Pavlina Yaneva McGovern, R&D Information Governance Lead, ACCORD	23/04/2025
Douglas Young Douglas Young (Apr 23, 2025 12:20 GMT+1) APPROVED: Douglas Young, Principal R&D Manager, NHSL, ACCORD	23/04/2025
Gavin Robertson (Apr 23, 2025 12:52 GMT+1) AUTHORISED: Gavin Robertson, QA Coordinator, NHSL, ACCORD	

GS008 Personal Information_Caldicott Approval and Information Governance Review v6.0

Final Audit Report 2025-04-23

Created:	2025-04-23 (British Summer Time)
By:	Roisin Ellis (v1relli8@exseed.ed.ac.uk)
Status:	Signed
Transaction ID:	CBJCHBCAABAAF2-LOlGksQk2PRp8pTGYhn-QL3RZu3je

"GS008 Personal Information_Caldicott Approval and Information Governance Review v6.0" History

Document created by Roisin Ellis (v1relli8@exseed.ed.ac.uk)
2025-04-23 - 12:08:01 PM GMT+1- IP address: 62.253.82.231

Document emailed to pavlina.y.mcgovern@nhslothian.scot.nhs.uk for signature
2025-04-23 - 12:09:18 PM GMT+1

Email viewed by pavlina.y.mcgovern@nhslothian.scot.nhs.uk
2025-04-23 - 12:17:00 PM GMT+1- IP address: 62.253.82.233

Signer pavlina.y.mcgovern@nhslothian.scot.nhs.uk entered name at signing as Pavlina Yaneva (McGovern)
2025-04-23 - 12:19:02 PM GMT+1- IP address: 62.253.82.232

Document e-signed by Pavlina Yaneva (McGovern) (pavlina.y.mcgovern@nhslothian.scot.nhs.uk)
Signature Date: 2025-04-23 - 12:19:04 PM GMT+1 - Time Source: server- IP address: 62.253.82.232

Document emailed to Douglas Young (douglas.young@nhslothian.scot.nhs.uk) for signature
2025-04-23 - 12:19:06 PM GMT+1

Email viewed by Douglas Young (douglas.young@nhslothian.scot.nhs.uk)
2025-04-23 - 12:19:44 PM GMT+1- IP address: 52.102.16.181

Document e-signed by Douglas Young (douglas.young@nhslothian.scot.nhs.uk)
Signature Date: 2025-04-23 - 12:20:23 PM GMT+1 - Time Source: server- IP address: 62.253.82.233

Document emailed to Gavin Robertson (gavin.robertson@nhslothian.scot.nhs.uk) for signature
2025-04-23 - 12:20:25 PM GMT+1

Email viewed by Gavin Robertson (gavin.robertson@nhslothian.scot.nhs.uk)
2025-04-23 - 12:51:18 PM GMT+1- IP address: 81.79.219.212

Document e-signed by Gavin Robertson (gavin.robertson@nhslothian.scot.nhs.uk)

Signature Date: 2025-04-23 - 12:52:08 PM GMT+1 - Time Source: server- IP address: 81.79.219.212

Agreement completed.

2025-04-23 - 12:52:08 PM GMT+1