Standard Operating Procedure			**61.005**	
Contracting with industry for innovation projects using identifiable, pseudonymised or fully anonymised patient data				
Version	**1.0**			
Prepared by	Ruairidh Davison	Signature	Date	
Approved by	Roma Armstrong	Signature		Date
Released by	Julie Brittenden	Signature	Date	

1. SOP Category

NHS GG&C Sponsor R&I

2. Staff Category

Staff Category	R	A	C	I
R&I Innovation Lead		x		
R&I Senior Managers				x
West of Scotland – Innovation Contracts Manager	x			
Innovation Sponsor Co-ordinators	x			
Sponsor Coordinators	x			
Project Managers (all)			x	
Chief Investigators			x	

3. Scope

This SOP applies to Sponsor representatives during the design, review and approval of projects that require access to patient data, to ensure that data governance, data quality and data security requirements are met. NHSGGC usually acts as sponsor for collaborative innovation projects with industry and/or university partners either as eligible or investigator initiated, industry funded projects. This SOP does not cover financial aspects such as costing, waiver to tender and new supplier request form.

4. Purpose

This SOP outlines the processes that need to be considered by the R&I Office when managing the design, review and approval of innovation projects that requires access to patient data. These projects are split into:

- Those requiring access to identifiable patient data
- Those requiring access to pseudonymised patient data
- Those requiring access to fully anonymised patient data

The SOP specifies what types of Agreement will be required to meet legal requirements and expectations for data governance, data quality and data security. All agreements (draft and fully signed) required for the approval of the project should be stored in the legal folder of the appropriate study e-file. In some cases projects are split into work packages. The appropriate approvals must be in place before the work package or study can start and data made available.

Where appropriate, Agreements are provided as Forms linked to this SOP or the web source provided. Other example contracts/agreements are stored in \\northnet-11\wg-research\common\5. Innovation\11. Example documents

The SOP also covers ethical and regulatory requirements. These procedures are primarily for studies that NHS Greater Glasgow & Clyde (GG&C) sponsor.

4.1 Background

A key element of NHS policy is to accelerate the translation of medtech and digital health innovations into the NHS. Digital transformation requires access to high quality, trusted data – but often in large volume to meet machine learning (ML), artificial intelligence (AI) or digital service requirements.

After the Brexit transition period, the UK Data Protection Act 2018 incorporated EU GDPR requirements, and the UK GDPR came into force in January 2021. Where AI uses personal data it falls within the scope of this legislation. This can be through the use of personal data to train, test or deploy an AI system.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The Data Protection Act 2018 distinguishes between a 'data controller' and a 'data processor'. The data controller controls the purpose for which, and the manner in which, personal data are processed - and carries data protection responsibility for it. The data processor means any party (other than an employee of the data controller) who processes personal data on behalf of the data controller. In reality a data processor can itself exercise some control over the manner of processing and must take liability for this. In situations such as a data breach it will be necessary to determine which organisation has data protection responsibility.

Key differences between UK and EU GDPR that affect medtech and digital health innovations are:

- **Automated Decision making:** The UK GDPR allows automated profiling in cases where there is a legitimate justification for it. This is not the case when it comes to EU GDPR since the EU data privacy legislation gives users the right to reject automated decision-making or profiling.
- **Privacy versus Freedom of expression:** UK GDPR is more supportive than EU GDPR of the processing of a user's personal data for reasons of public interest.

In clinical research, some of the categories of personal data are considered to be sensitive and require a higher level of protection. This is known as 'special category' data e.g. race, origin, genetic, biometric and health data. The UK GDPR only covers structured data but under the Data Protection Act 2018 processing of unstructured text data, e.g. radiology reports, clinic letters etc constitutes personal data.

Some innovation studies follow a research route where informed consent is sought from the patient (SOP 51.002). This is usually the case for regulated trials. But others may have minimal consent (e.g. through a digital service) or no consent (e.g. new technology deployed at a service level). Even when consent is in place, it may not provide the legal basis for processing personal data. The legal basis for processing this personal data is most likely to be under Article 6(1) (e) performance of a public task i.e. the processing is necessary to perform a task in the public interest. With special categories of sensitive personal data, the legal basis is likely to fall under Article 9 (2) (g) - Reasons of substantial public interest. As such, this SOP does not distinguish between the use of consented and un-consented patient personal data. This will be clear for each project and the ethical approach taken. Please discuss the legal basis with Information Governance if you are unsure which would apply.

5. Procedures

It is important that the R&I Coordinator/Project Manager(PM) works with the Chief Investigator (CI) from the outset to understand data flows within a proposed project and data controller/processing responsibilities. Early discussions with GGC Information Governance and Compliance Managers to understand possible concerns and mitigation strategies, are encouraged.

5.1 Projects requiring access to identifiable patient personal data

It is common in collaborative projects with industry that the industry partner needs to process identifiable patient personal information. For example, where 1) patient information is being processed through a decision support algorithm to direct treatment, 2) patient tissue/data undergoes molecular analysis to guide treatment options, 3) patient scans are being analysed by an AI solution, 4) patient videos, clinical information and Patient Reported Outcome Measures (PROMS) are being processed to form a new clinical service and 5) patient information is being processed when a company has to access new technology for trouble shooting or support. Approval of such projects will depend on whether the project is a research project or service development; and if a research project whether it is a regulated trial.

5.1.1 Required Agreements

- **UK GDPR Data Processing Agreement (DPA – Form 61.005A)**
  This is required if the Company is acting as a Data Processor – and is the most likely scenario with identifiable personal data. The Schedule will specify the personal data that will be processed, whether or not the patient has given consent to the use of data, the duration of processing and arrangements at the end of processing. If the company needs to access data remotely from outside the UK, this must be clear in the patient information sheet and this aspect captured in the DPA. Otherwise the Information Commissioner's Office (ICO) International Data Transfer agreement is likely to be required for countries without adequacy regulations eg USA (). The DPA may also include practitioner as well as patient data. Indemnity arrangements are captured in the text of the DPA. There may be equivalent Data Processing clauses in the contract with the Company which would negate the need for a DPA. The Information Governance Manager will decide if this is the case or whether a separate DPA is required.

  If a Clinical Trials Unit (CTU) is involved, a separate DPA will be required for the CTU as well as the industry partner(s). Data is usually pseudonymised prior to transfer to the CTU. If the company is responsible for this, it will be specified in the DPA with the company.

  If National Services Scotland (NSS), NHS Education Scotland (NES) or equivalent public bodies perform a processing role, a separate DPA is required unless the data processing fields can be added to an existing DPA.

  On completion the DPA must be reviewed by Information Governance and signed off by the GGC Service Lead and the Processor.

- **UK GDPR Data Protection Impact Assessment (DPIA –Form 61.005B)**
  In some projects, the Company will require identifiable personal data to leave the NHSGGC network. The benefits versus risk of pseudonymisation and re-identification of a patient needs to be considered. A DPIA is required. This must specify the legal basis for processing data – usually Article 6(1) (e) performance of a public task. This is a living document and risks may change over time. A data flow diagram is required as well as information about mechanisms of data transfer.

  If time is a constraint and the processing relatively low risk, the IG Manager may allow the project to go ahead using the **IG Rapid Data Protection Assessment (Form**

61.005C). In both cases, Transparency aspects must be met eg through use of leaflets, posters and websites.

On completion the DPIA must be signed off by the Information Governance Manager and the GGC Service Lead.

Advice on how to complete the DPA & DPIA can be sought from the Information Governance Team.

- **IT Security/Compliance**
  NHS Scotland has moved from the Information Security Policy Framework to the Scottish Government's Cyber Resilience Framework. A core focus of the new framework is that the responsibility for 3rd party IT/data security assurance sits firmly with the host organisation/data owner and with this, an increased accountability, which is monitored through audit. Supplier assurance should be carried out at the earliest possible stage and should be ongoing throughout the project. The compliance criteria are stipulated as part of the new framework (Cyber resilience: framework and self assessment tool - gov.scot (www.gov.scot)).

  - **System Security Policy (SSP – Form 61.005D)**

  Completion of the SSP Triage Form will determine if an SSP is required, Where possible generic SSPs have. been completed to allow individual projects to progress more quickly eg vCreate and Health Data Exchange (HDE). In addition, if data is going to a cloud environment, a cloud SSP is required (Form 61.005E).

  If data is being held out with the UK or EU such as in the United States, specific contracting is required. Article 44 of the UK GDPR states that any transfer of personal data to a third country or an international organisation can only take place where the conditions set out in Chapter 5 of the regulation are met. These conditions include adequacy regulations, appropriate safeguards and binding corporate rules (see ICO link above).

  - **Third Party Access Agreement**

  If the Company requires access to the NHSGGC network a Third Party Access Agreement is required unless the Company already has access to the Scottish Wide Area Network (SWAN). If the company already has a Third Party Access Agreement in place, this may need revision to ensure the requirements for new projects are captured adequately. Template questions are provided as Form 61.005F

  Both the SSP and Third Party Access Agreement are agreed and signed off by the Compliance Manager

- **Unsupervised Letters of Access (LoA)**
  As detailed in SOP 60.002, access to patient data is usually governed at a named individual level by a LoA (Form 60.002A) signed off by the individual, the Company and NHSGGC. Critically if the project also requires the Company to access pseudonymised information, there must be a separation of function to ensure that the same person cannot access both identifiable and pseudonymised data.

- **Collaboration Agreement**
  The Agreement will capture funding, indemnity, Data Controller/Processing arrangements, intellectual property and benefit sharing. It will be clear if data use is consented or un-consented. For regulated trials, the Agreement will also specify all aspects that the Sponsor requires from the company to meet the requirements of the Regulator (MHRA). Best practice is that the Agreement will include a Data Sharing Agreement (Form 61.005G – CLO template un-consented). This Form needs to be adapted slightly to make it clear when consent is in place. For Controller to Controller Agreements, a Data Transfer Agreement should be used (ICO template).

If a Clinical Trials Unit (CTU) and/or University Chief Investigator or Project Manager is involved, a separate Agreement will be required for the University to capture funding, indemnity and Data Controller/ Processing arrangements. For regulated trials, the Agreement will also specify all aspects that the Sponsor requires from the University to meet the requirements of the Regulator (MHRA). Example Agreements are stored in \\northnet-11\wg-research\common\5. Innovation\11. Example documents

5.1.2 Ethical and quality assurance requirements Research Projects

All research projects which require access to identifiable patient data will require Research Ethics Committee (REC) approval. This is either through IRAS or using delegated REC approving powers eg West of Scotland Safe Haven Local Privacy Advisory Committee (LPAC) or National Public Benefit & Privacy Panel for Health & Social Care (PBPP).

Even when a company is required to process identifiable information, all research data (including results generated by the Company) must be pseudonymised prior to inclusion in a research database. If the Company is responsible for pseudonymisation (eg of data or DICOM headers of images) then the safe haven must quality assure the pseudonymisation process. In addition different named staff from the Company must conduct the pseudonymisation and identifiable work (see LoA above). Similarly any data extracted from NHS systems must be linked and pseudonymised prior to transfer to the research database either by safe haven staff or quality assured by the safe haven.

If projects require access to un-consented data from English sites, an application for 'section 251 support' from the Confidentiality Advisory Group (CAG) may be required. There is a checklist on the Health Research Authority website CAG_pre-application_checklist.pdf

To meet Information Commissioners Office (ICO) requirements, if informed consent is not required in a prospective study, patients must be notified when their data is being processed by an AI or ML algorithm and offered the opportunity to opt out.

Service Development Projects

service development projects may not require REC approval but will still require **Caldicott Guardian** approval for data use (Form 61.005H).

5.1.3 Regulatory requirements

Form 51.010 D (Grant or Investigator Initiated Study with a medical device – checklist) should be completed to understand at the outset (costing stage) whether or not the study is a regulated trial. In some cases advice from the MHRA will be required.

5.2 Projects requiring access to pseudonymised patient personal data

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual. However, pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data. Recital 26 makes it clear that pseudonymised personal data remains personal data and within the scope of the UK GDPR.

It is common in collaborative projects with industry that the industry partner needs to access pseudonymised patient information. At the data discovery stage companies need access to

pseudonymised clinical data and/or images for training and validation of machine learning algorithms. For tissue studies, data (diagnostic, treatment and outcome) if often required to enhance the phenotype and is provided pseudonymised to link to the tissue. These studies often use un-consented tissue and data.

5.2.1 Required Agreements

- **UK GDPR Data Processing Agreement (DPA)**
  Usually a DPA is not required.

  In most cases, when a company accesses linked, pseudonymised data held within a Trusted Research Environment (TRE) the Company is not acting as a data processor. In addition, our partnership through the safe haven with the University of Glasgow (UoG) means that there is a generic DPA and DPIA in place for projects using the UoG TRE. But it is worth noting that if the company accesses the data by VPN from out with the UK, data access constitutes an international transfer of personal data and will only be permitted if the data controller is satisfied that appropriate arrangements are in place to protect the data. An **International Data Transfer Agreement** (ICO template) can be used or our standard Agreement updated to reflect this (see 5.1.1).

  If the Company requires access to pseudonymised data out with a TRE, a DPA will be required if the Company is acting as a data processor (as in 5.1.1). More commonly, a **Data Sharing Agreement** (consented or un-consented) or **Data Transfer Agreement** will be required (as in 5.1.1).

- **Data Protection Impact Assessment (DPIA)**
  If the Data leaves the NHSGGC network, other than to a TRE, a DPIA will be required as in 5.1.1.

- **System Security Policy (SSP)**
  As in 5.1.1

- **Third Party Access Agreement**
  Unlikely to be required.

- **Unsupervised Letters of Access (LoA)**
  Access to data held in a TRE is governed separately. For any other scenario, a Letter of Access will be required - see 5.1.1

- **Collaboration Agreement**
  As in 5.1.1

5.2.2 Ethical and quality assurance requirements

As in 5.1.2

5.2.3 Regulatory requirements

As in 5.1.3

5.3 Projects requiring access to fully anonymised patient personal data

Personal data that has been fully anonymised is **not** subject to the UK GDPR. Personal data must be stripped of sufficient elements that mean the individual can no longer be identified – or more importantly **re-identified**. This rules out any follow up of data subjects. It is also important to recognise that fully anonymising personal data still involves processing to that point. So if a Company does that then the rules in 5.1.1 apply.

6. Referenced documents

- Form 61.005A - UK GDPR Data Processing Agreement
- Form 61.005B - UK GDPR Data Protection Impact Assessment
- Form 61.005C - IG Rapid Data Protection Assessment
- Form 61.005D - System Security Policy
- Form 61.005E - Cloud System Security Policy
- Form 61.005F - Third Party Access Agreement – Template questions
- Form 61.005G - Data Sharing Agreement (CLO template)
- Form 61.005H - Caldicott Guardian Approval Form
- SOP 61.002 - Unsupervised Industry Access to the NHS
- Form 61.002A - NHS Greater Glasgow and Clyde (NHS GGC) Letter of Access for Unsupervised Industry Researchers – VPN only
- Form 51.010D - Grant or Investigator Initiated Study with a medical device – checklist
- SOP 51.002 - Participant Information Sheet and Consent Forms: Design and Approval

7. Related documents

Document templates are stored in \\northnet-11\wg-research\common\5. Innovation\11. Example documents

8. Document History

Version	Date	Description
1.0	21/12/2022	Creation of SOP