Private sector access to public sector data

Operational Framework for research data access

Research Data Scotland

23/03/2026

Research Data Scotland

Scottish Government
Riaghaltas na h-Alba

Contents

1. Introduction

Research using Scotland’s public sector data has immense potential to drive transformational outcomes in our nation’s health, economy, and public services, provided that it is used in ethical and transparent ways that maintain public trust.

Access to public sector data for research is currently approved on a case-by-case basis, however this is often a frustrating and time-consuming experience for researchers and innovators, which impedes innovation for public good.

Realising the full value of public sector data to support research and innovation requires the creation of streamlined access arrangements, with appropriate safeguards in line with robust legal and ethical standards. This Operational Framework is a key step towards creating these conditions for ethical data-driven research.

We want Scotland to have data that empowers research and innovation. This means giving researchers and innovators from the public and private sectors clear, ethical and efficient routes to access and use data to take forward projects that support the modernisation of services and deliver public benefit. However, we are committed to allowing safe access to data strictly where intended public benefit is clearly demonstrable.

1.2 Purpose / objective

This Operational Framework is designed to support informed, consistent decision-making by Scotland’s public sector data controllers, when managing access requests by industry for research using de-identified data.

This will contribute to a broader objective: to develop a more effective approach to private sector access to public sector data across Scotland, to better realise social, economic, and environmental benefits.

1.3 Audience

This Framework is designed primarily for Scotland’s public sector data controllers and others involved in decision-making regarding access to public sector data. However, the Framework can also be of value to researchers and innovators.

1.4 Scope

The scope of the Framework covers Scotland’s public sector, but initial testing and evaluation of the Framework will be within the healthcare sector. This will be limited to accessing de-identified healthcare data for research purposes. The intention is to broaden the scope to encompass non-healthcare related data in the future.

1.5 Outline of approach

This is a first version of the Operational Framework. It will be further developed with data controllers and other relevant stakeholders, in phases. Each iteration will be shaped through cross-sector collaboration and will incorporate lessons learned from applying the Framework in an operational context. The Framework draws on existing good practice in Scotland, the UK and internationally. The intention is to further refine and develop the Framework, undertake regular reviews, and develop materials which support the operationalisation of the Framework.

1.6 Background

The Scottish Government commissioned Research Data Scotland (RDS) to develop an Operational Framework to support secure, streamlined access to public sector de-identified data, by the private sector, for ethical research and innovation.

This supports the aim of the Scottish Government's Unlocking the Value of Data (UVOD) programme, to better utilise Scotland's public sector personal data when used with, or by, the private sector for public benefit. The UVOD programme highlighted the need for a Framework to enable research and innovation by private sector organisations using public sector data in Scotland, ensuring that there are clear and tangible public benefits and meeting critical ethical thresholds.

This document is informed by the work of the Independent Expert Group for the UVOD programme; other UK initiatives on the use of public sector data for research; an RDS review of operational practice; and insights drawn from engagement with Scotland's public sector, industry, and the public.

The Framework has been shaped by, and aligns with, the updated Safe Havens Charter, the Five Safes framework, NHS Scotland's Caldicott Guardians principles, and the National Information Governance Framework (see annex one for list of reference documents).

Insights from engagement with the public and private sector highlighted the need to address the current inefficiencies in data use and encourage a consistent approach to data access, regardless of sector. This Operational Framework provides a way to access data in accordance with UK-wide initiatives, while ensuring transparent and fair use of public sector data for the public good.

2. Guiding principles

This Framework is underpinned by a set of guiding principles. While the precise approach adopted by data controllers will need to be considered on a case-by-case basis, these principles provide key criteria to support public sector organisations in adopting a more consistent, streamlined approach to decision making.

2.1 Public interest and public benefit

All access to public sector personal data must be done in the public interest and be expected to result in public benefit or value. Public engagement (a targeted narrative review and wider engagement) shows that there is public support for private sector use of public sector data, with acceptability conditional on public benefit.

The public benefit evaluation process should require the applicant to provide a transparent assessment of how the commercial interests are proportionately balanced and how they are expected to accrue tangible benefits to the public.

There is no single internationally accepted definition of public benefit for the use of data. However, the RDS website sets out the definition of public good to be used across Scotland.

It is for applicants to align their research project with one or more of the following outcomes. Research projects should:

- Help the system to better understand the health and care needs of populations
- Lead to the identification or improvement of treatments, interventions, or health and care system design, to improve health and care outcomes or experiences
- Help to manage the response to communicable diseases and other risks to public health, such as pandemic planning and research
- Advance understanding of regional and national trends in health and social care needs
- Advance understanding of the need for, or effectiveness of, preventative health and care measures for particular populations, or conditions such as obesity and diabetes
- Better inform those planning health services and programmes, for example, initiatives to improve equity of access experience and outcomes in the short or long term
- Inform decisions about how to effectively allocate and evaluate funding according to health needs
- Support knowledge creation or exploratory research (and the innovations and developments that might result from that exploratory work)
- Advance understanding of the needs of carers supporting family members
- Add to the evidence base for public policy decision-making
- Add to the evidence base for public service delivery
- Replicate and validate or challenge existing research
- Improve the quality, coverage or presentation of existing statistical information

These incorporate the public good criteria within the UK Digital Economy Act's Research Code of Practice. However, what exactly constitutes public benefit will continue to be determined on a case-by-case basis in specific contexts and take account of the need to engage the public in a way that ensures transparency and accountability.

2.2 Cost recovery and public sector benefit

Equitable benefit-sharing models for public-private collaboration are important in ensuring that any benefits accruing from personal data use by commercial entities can return to or be reinvested in the public sector.

For now, this principle will be met through charges to private sector companies on a recovery basis, for the costs of servicing and provisioning the data access. Private sector companies should meet the direct data access costs of their project and contribute to the indirect costs of the public sector services and infrastructure, to enable safe data access.

2.3 Transparency

As for all research using data about the public, the highest levels of transparency should be maintained throughout the data and project lifecycle.

There must be transparency regarding the following:

- Which public sector personal data is being accessed from which public body?
- Which organisation is sponsoring the research?
- Which organisation is accessing the data?
- For what time period is access to data approved?
- What are the specific public benefits, interest and value proposed?
- What does the organisation intend to use those data for?
- How are decisions made by the public sector to grant access to personal data?
- How is access managed and what controls are in place? (e.g., Trusted Research Environments (TREs), which panel(s) review and approve research projects, approvals for researchers, etc.)
- To what extent did the use of data produce the anticipated public benefit in practice, and was this value shared back with the people of Scotland?

This can be achieved, for instance, with a project/data use register online, with a short summary in accessible language.

2.4 Public engagement and involvement

Public support for research is central to building trust and underpins the ethical and responsible use of data in research. Evidence for public support can come from a range of sources including engagement activities specific to the research project, for example with a public interest panel or advocacy group, existing public engagement evidence, or other evidence demonstrating that the research is likely to be supported and valued, including by the specific groups that are the subject of the research. Involving public members in the research project proposed can also add accountability, transparency and ensure outputs are communicated in a clear public-friendly way. As with all researchers and research sponsors, private sector organisations will need to provide the necessary evidence and consider incorporating the necessary degree of public involvement proportionate to the scale, risk and nature of the personal data involved, as well as the nature of the research itself. Applicants should justify the chosen scale and approach.

This also means using feedback and input from the public to adapt approaches and practice. Private sector organisations should demonstrate trustworthiness by having the capability to incorporate feedback from the public in a meaningful way into their research plans.

2.5 Managing risks

Allowing access to de-identified, minimised personal data by companies should be safe and do no harm.

Risks need to be identified and managed before private sector organisations can access (and continue to access) public sector personal data, to the satisfaction of data controllers and others involved in decision-making and governance. Risks and mitigating actions will be documented as part of a contractual arrangement. Projects will need to evidence their adherence to the Five Safes framework (see section three and annex two).

Partnership with an academic institute and/or public sector organisation can build trust with data controllers and their approval panels. Academic sponsorship of research will engender the highest levels of trust. However, academic involvement is not mandated in cases where independent private sector research can meet all ‘Safe Project’ and ‘Safe People’ standards.

UK legislation does not require organisational accreditation in addition to safe researcher accreditation. However, it is recognised that the public is concerned about their data being accessed by companies that do not balance profit with a strong ethical and public good ethos. As such, a safe organisation assessment should be carried out before advice to data controllers on access is provided.

Requests for access to Scottish data can sometimes come from outside the UK. Where this is the situation, there needs to be a specific assessment of any additional risk involved.

There is no current standard way to assess organisations. Good practice and guidance will be developed for future iterations of this Framework. There are existing processes and risk assessments, for instance within the Scottish Safe Haven Network, which assess safe organisations and work with international organisations, from which we can learn and build.

2.6 Conclusion

Used well, public sector data can power the change in services that significantly improve the social, economic and environmental wellbeing of the population. As such, research will be allowed to proceed, unless the researchers fail to: demonstrate their proposed work is ethical; ensure total anonymity at all times; engage with relevant parts of the public; and demonstrate benefit to society. Any use of public sector data must be transparent about who is accessing what data, for what purpose, and the likely public benefit that will be created.

3. Five Safes framework

The Five Safes framework must be followed to enable safe research access to data. This framework builds on international best practice for making effective use of case-level data. All Scottish Safe Haven TREs operate with processes that align with the Five Safes (See annex two for details).

In line with UK legislation, the application of standards using the Five Safes framework is predominantly the same for researchers from the private sector and other researchers. However, there may be additional challenges for private sector researchers to meet standards in relation to some aspects of that framework.

The Five Safes are:

- **Safe Data**: Specify data protection measures and de-identification requirements. Has confidential information been removed so that the level of detail of the data is appropriate to answer the specified research question(s)?
- **Safe Projects**: Clearly define the project purposes and public benefits. Is this use of the data appropriate, lawful, ethical and in the public interest?
- **Safe People**: Requires user accreditation and training. Can the user be trusted to use it in an appropriate manner?
- **Safe Settings**: Describe secure environments for data access. Does the Safe Haven prevent unauthorised use of the data?
- **Safe Outputs**: Outline processes for checking and managing data outputs for confidentiality. Is the confidentiality maintained for research outputs coming out of the Safe Haven?

4. Data governance

The purpose of this section is to outline minimum principles, in terms of best practice, for the governance of data in the context of this Operational Framework.

4.1 Assessment of purpose

Key principles of Information Governance are proportionality and data minimisation, with the controls proportionate to the level of risk involved. An assessment of purpose is based upon whether:

A. The applicant is asking for individual-level data to be brought together where there is no need or attempt to re-identify individuals, and that all outputs are 'Safe Outputs.' This is categorised as scientific research.

B. Case level data is brought together and where there will, or may be, the need to re-identify individuals as part of the research. This may be clinical research, where there are strong ethical reasons to retain the ability to identify individuals as part of the study. It may also be other research, where re-identification of individuals is needed, such as drawing a sample for a survey.

4.2 Scientific research

1. This will need independent assurance that the sharing of the data:

- Is likely to lead to a net public good/public benefit
- Will avoid harm to individuals
- Will avoid a risk of re-identification, set out under the Five Safes framework
- Will lead to research with scientific merit

This independent assurance could be given by a panel of experts and/or public representatives, or by a relevant NHS Caldicott Guardian.

2. Data for scientific research can be classed as anonymous under the conditions created by the Five Safes framework. This means that pieces of research need:

- A project licence for use of the data, agreed by data controllers
- A user agreement, signed by the researcher, that outlines their responsibilities for safe data use in a Safe Haven environment

Research needing to identify individuals will also require:

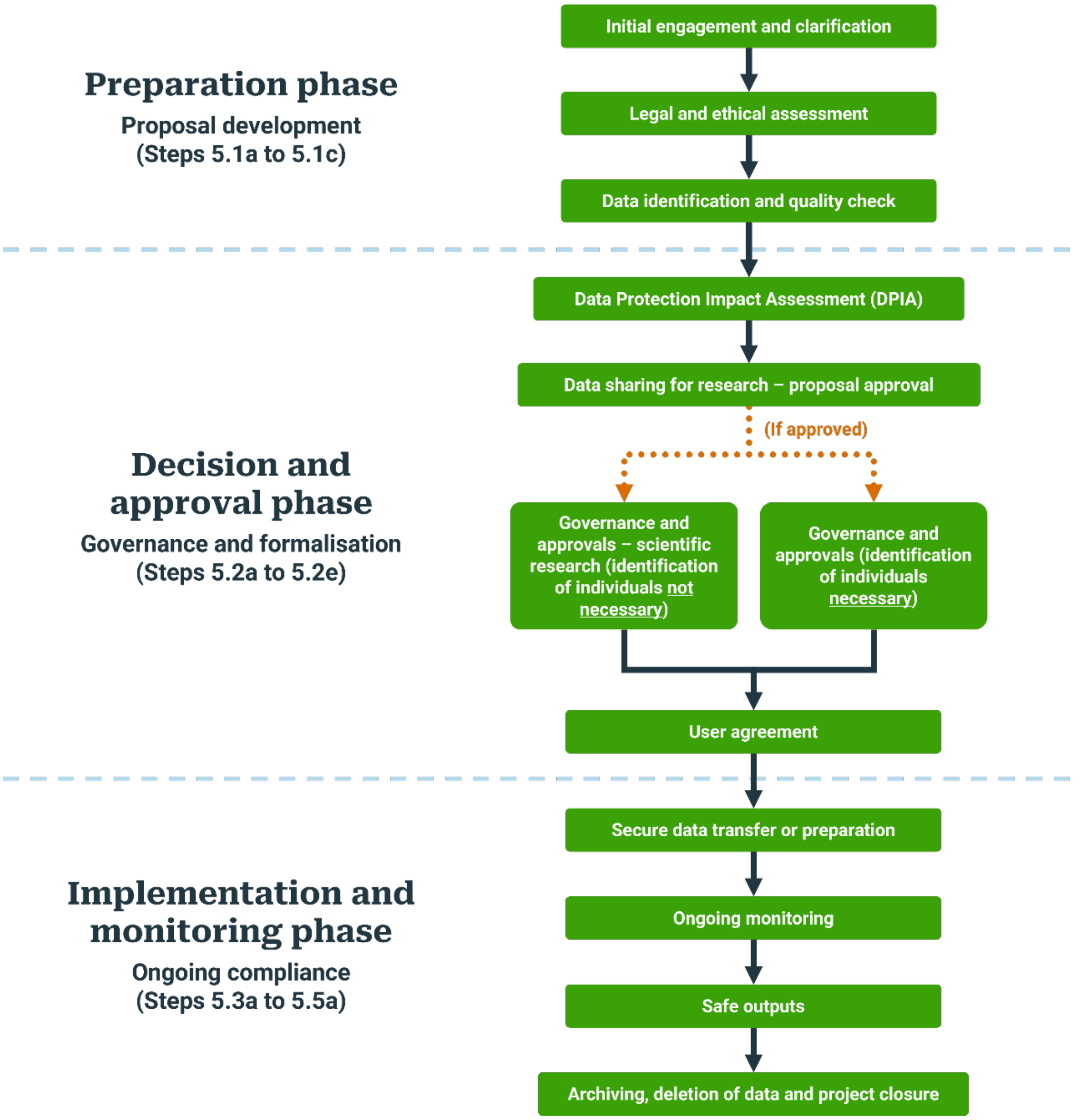
- An agreed Data Protection Impact Assessment (DPIA)
- An external independent scientific peer review
- NHS ethics for research on health matters
- Stage-gated approval with requirements to return for further review and approval, e.g., for benefit-sharing negotiation and agreement when identified potential for this is realised

4.3 Accountability

It is crucial that the User Agreement is carefully considered and that specific roles and responsibilities are clearly laid out. An assessment of any breach may result in the incident being reported to the Information Commissioner's Office (ICO). The ICO has various powers depending on the severity, implications and response to any incidents related to personal data. These include enforcement notices, fines or, in extreme cases, imprisonment.

5. Process flow for data access

Data controllers play a vital role in managing data access requests under UK GDPR and Safe Haven governance frameworks. There are several steps that the data controller is expected to follow in managing requests for data access from the private sector.


Preparation phase
Proposal development
(Steps 5.1a to 5.1c)
Initial engagement and clarification
Legal and ethical assessment
Data identification and quality check
Decision and approval phase
Governance and formalisation
(Steps 5.2a to 5.2e)
Data Protection Impact Assessment (DPIA)
Data sharing for research – proposal approval
(If approved)
Governance and approvals – scientific research (identification of individuals not necessary)
Governance and approvals (identification of individuals necessary)
User agreement
Implementation and monitoring phase
Ongoing compliance
(Steps 5.3a to 5.5a)
Secure data transfer or preparation
Ongoing monitoring
Safe outputs
Archiving, deletion of data and project closure

The steps under 5.1a to 5.1c are about preparing a proposal for sharing data. This can be delegated to a data access service, who would liaise with any data controller who is part of the project.

Step 5.2b is about determining the proposal for sharing data. The best practice is to have an independent panel who would review the proposal, either alongside data controllers or with delegated authority. This is needed for all data sharing. There are existing panels in Scotland that could be used to carry out this task.

Steps 5.2a, 5.2c and 5.2d are for formalising a decision of approval to share data.

Step 5.2c and 5.2e are needed for scientific research.

Steps 5.2a, 5.2d and 5.2e are needed for research that may, or needs, to identify individuals.

Step 5.3 is about monitoring compliance with the governance documents, following approval of a data share for research. Again, this can be delegated to a data access service.

5.1a Initial engagement and clarification

- **Engage with the applicant** to clarify:
    - The purpose of the request
    - The terms of the request (if required)
    - Intended outcomes
    - The **public benefit** anticipated from the data use (a key requirement)
- Confirm whether the request aligns with **public interest principles** and if necessary resources are available to advise on the definition of public benefit.

5.1b Legal and ethical assessment

- Identify the **lawful basis** for sharing under UK GDPR and the Data Protection Act 2018. For research purposes, this is likely to rest on legitimate interest.
- Consider whether additional legislation or frameworks apply (e.g., **The Digital Economy Act**, or sector-specific laws).
- Conduct an **ethical review**. This could be done through an established Research Ethics Committee that is part of the NHS or a university, or through an ethics assessment that is built into the application and data access processes. This will:
    - Assess potential benefits and harms
    - Ensure transparency and fairness
    - Confirm that the arrangement has the potential to deliver **public benefit** and will **protect privacy**

5.1c Data identification and quality check

- Identify relevant datasets/data items and confirm:
    - Data availability
    - Completeness and quality
    - Appropriate metadata and documentation

5.2a Data Protection Impact Assessment (DPIA)

- Each data controller must complete an appropriate DPIA
- The DPIA should document mitigations for privacy and ethical risks

5.2.b Data sharing for research – proposal approval

- If refused, record reasons and communicate clearly to the applicant
- Ensure compliance with **records management obligations** under the Public Records (Scotland) Act 2011

There are several independent panels who provide scrutiny over applications for data sharing for research purposes. A data access service can provide advice on the best route for supporting the type of data sharing that is required.

5.2.c Governance and approvals – scientific research, e.g., where data is used for public good research where it is not necessary to identify individuals

- Prepare a project licence, outlining:
    - The purpose and scope of the data share
    - Security measures
    - Roles and responsibilities
- Obtain internal approvals from the Information Asset Owners of relevant datasets.

5.2.d Governance and approvals – identification of individuals necessary

- Prepare a **Data Sharing Agreement** outlining:
    - The purpose and scope
    - Security measures
    - Roles and responsibilities
- Obtain internal approvals from the:
    - Legal team
    - Data Protection Officer
    - Information Asset Owners
- This is only required for research in which it is necessary to identify individuals.

5.2.e User agreement

The researcher signs a user agreement that outlines the responsibilities and behaviours expected of them whilst accessing and using the data. It describes the consequences for users if not adhering to the agreement, which can include immediate withdrawal of data access, a fine, or imprisonment.

5.3a Secure data transfer or preparation

If the proposal for data sharing is approved and the Project Licence or Data Sharing Agreement and user agreement are fixed, protocols must be implemented to transfer the data securely to the agreed place where the researcher can access data.

If the proposal for data sharing is approved and Project License or Data Sharing Agreement and User Agreement are in place, the Safe Haven/TRE proceeds with secure data protocols within the secure infrastructure.

The data access service prepares the research data within a staff-only secure area, and once all quality control checks have been performed, transfers the data into the secure research project workspace in the Safe Haven. No row-level data is permitted to be removed from the environment, via robust technical and procedural controls.

If the data is already curated in a Safe Haven, the data access service staff will arrange to prepare the data in a secure setting for that specific researcher team and for that specific project.

5.3b Ongoing monitoring

- Actively monitor compliance with the Project Licence or Data Sharing Agreement
- Actively monitor compliance with the Researcher User Agreement
- Review outcomes against the stated public benefit
- Publish the details of approved research in a discoverable data use register. This should cover the items covered in section 2.3 above
- Maintain contact with the research team and ensure the outcomes from the research are published as part of the register
- Ensure there is clear guidance on how data will be returned or destroyed once it is no longer required by the project, or on project closure

5.4a Safe outputs

Only aggregated, rounded analysed data is permitted to be released, and undergoes robust statistical disclosure, controlled by trained staff, to protect patient confidentiality and privacy.

5.5a Archiving, deletion of data and project closure

There are strict rules around the access dates of data, and the data must be archived according to length required and then deleted. Certificates of destruction should be provided, and project closure must meet all ethical requirements required by sponsor.

6. Finance and contracting

We will develop template language for use in contractual agreements in the next stage of this project. This is key, and important to ensure appropriate costing and contractual arrangements that are also practical.

7. Governance / ownership

The Scottish Government retains ownership of this Operational Framework. RDS will be responsible for reviewing, updating, and implementing the Framework.

The Framework will be reviewed and updated on an annual basis as a minimum, or in response to any change that may materially affect its application.

This may include, but is not limited to:

- Enhancements informed by user feedback
- Changes to legislation
- Changes in governance requirements, policy, and standards

This Framework was approved on 16 March 2026.

Next review date: By March 2027

Annex 1: UK standards and frameworks for data security and other areas – November 2025

There are several relevant UK-wide and international best practices which are available for consideration:

- Scottish Safe Haven Charter
- National (Scottish) Information Governance Framework
- The Five Safes framework
- Standard Architecture for Trusted Research Environments (SATRE) specification
- Digital Economy Act (DEA)
    - UK Statistics Authority (UKSA) Research Code of Practice https://code.statisticsauthority.gov.uk/
- Data Protection Act 2018 (PBPP legislation and principles)
    - S19 of the Data Protection Act 2018
- UK General Data Protection Regulation (UKGDPR)
    - *Article 6(1) (e) - e) *Performance of a task that is in the public interest* (pulled from PBPP legislation and principles)
- Articles 84(A-D) of UKGDPR
- ICO’s guidance on anonymisation; and also, ICO guidance on research provisions (currently under review).

Annex 2: The Five Safes framework

1. Safe Data

All the individual-level data accessed by researchers is de-identified and is strictly limited to the data approved for use in the specific research project.

2. Safe Projects

In addition to being able to demonstrate public good, all projects need to have:

- An assessment of the ethics of the use of data proposed
- A risk-based assessment of research methodology
- A completed Data Protection Impact Assessment (DPIA) to assess risks in processing personal data
- A user agreement, signed by all researchers accessing data, that stipulates the terms on which data access is given / sanctions for breaking the terms of use

Partnership with an academic institute and/or public sector organisation is likely to strengthen and support considerations by data controllers and/or their approval panels when assessing project safety, particularly when led by an academic partner with Research Sponsor responsibilities. However, providing the above requirements are met, academic involvement is not mandated, and independent private sector research can meet ‘Safe Project’ standards.

3. Safe People and Organisations

In line with UK legislation, direct access to data is only allowed for accredited researchers who have demonstrated suitable research qualifications and/or experience and completed compulsory Office of National Statistics/Medical Research Council accreditation training. Researchers employed or contracted by private sector companies:

- must be accredited before they can access data directly and maintain up-to-date training accreditation throughout the project
- are encouraged to undertake additional training for safe data
- must retake safe data handling accreditation assessments before they can access data directly, if they change to a new private sector organisation

Where private sector companies are involved, the default arrangement for data access is based on those companies being part of a research partnership, led by an academic or public sector organisation. This must be formalised through a project, partnership or consortium agreement, outlining the project, data access/processing roles and responsibilities of the parties involved.

UK legislation does not require organisational accreditation in addition to researcher accreditation. However, we know the public is concerned with their data being accessed by companies that may not appropriately balance profit/sustainability with a strong public good ethos. As such, a test to determine a safe organisation will be developed.

Where access to Scottish data from outside the UK is requested, the NHS Grampian associated Safe Haven, DaSH, has designed an International Access Requests process for NHS Grampian local data. The NHS Lothian associated Safe Haven, DataLoch, have adopted this same process to deal with these requests in their area.

4. Safe Settings

The Scottish Safe Havens operate procedures that meet the Five Safes framework set out in the Safe Haven Charter, and are designed as safe settings.

Therefore, the default is that:

- All analysis of individual-level data takes place in one of the five Scottish Safe Haven Trusted Research Environments (TREs) or an equivalently accredited TRE elsewhere in the UK
- The data is not released to any private sector company. Where accredited and approved, researchers will be able to access, but not remove, data
- Access to data can either be done remotely via a SafePod[1] or at the Safe Haven[2] itself, depending on the sensitivity of the data

For all other research institutions, private sector companies can request that their own analytical/data processing software be imported or installed into the Safe Haven environment. Any data or software which a researcher wishes to bring into a secure environment must first undergo a disclosure check and IT security review, prior to ingest/installation. In this situation, the company would pay for the set-up costs to review, establish and maintain this data or software.

By exception, it may be possible for data to be moved into a secure computing environment outside a Safe Haven TRE, potentially including a secure computing environment run by a private sector company. This might be where Safe Haven TREs do not have the infrastructure to support the software/methods required for planned analysis, or where data cannot be moved into one of the TREs.

In these situations, the secure computing environment would need to meet security standards (as laid out in the SATRE specification), and access restrictions equivalent to TREs. The feasibility of adapting a Safe Haven TRE would need to be fully assessed, particularly in terms of achieving public benefit.

Where the analysis cannot be completed within a Scottish Safe Haven TRE, and the anticipated public benefit justifies an alternative secure computing environment (that meets Safe Settings standards), approval will be based on data-sharing agreements, a Data Protection Impact Assessment and a full System Security Policy Assessment.

5. Safe Outputs

Any outputs from the data analysis must be checked for disclosure risk (i.e., whether it might be possible to identify individuals) before they can be released outside the Safe Haven TRE (or exceptionally, other approved secure computing environment). Currently for Safe Haven TREs, these are checked by two members of staff of the Safe Haven, and this standard is the same regardless of who the researcher might be. Outputs will only be released if there is minimal disclosure risk.

[1] Home - SafePod

[2] Scottish Safe Haven Network | Research Data Scotland

Outputs are typically analytical results, but can also take the form of code or software such as AI/machine learning models. These are rapidly developing technologies, and additional expertise is required to check for potentially disclosive materials.

Implementing this framework for these outputs will require the development of additional Safe Haven capacity.

Annex 3: Caldicott Guardians principles

NHS Scotland's Caldicott Guardians principles must be followed to regulate the use of patient-identifiable information in UK health and social care, with the aim of ensuring data is only shared for specified purposes and with the minimum necessary information shared.

Caldicott Guardians have the responsibility of ensuring that both NHS and partner organisations meet the highest possible standards for processing patient-identifiable data, according to the principles.

The Caldicott Guardians principles:

Principle 1: Justify the purpose(s) for using confidential information

Principle 2: Only use it when absolutely necessary

Principle 3: Use the minimum that is required

Principle 4: Access should be on a strict need-to-know basis

Principle 5: Everyone must understand his or her responsibilities

Principle 6: Understand and comply with the law

These principles apply to patient-identifiable data. Data for research is de-identified and minimised, but best practice is to apply Caldicott Guardian principles regardless.

Annex 4: Glossary of terms

- **Benefit-sharing model:** Benefit-sharing is a general term used to define the fair and equitable sharing of the monetary and non-monetary benefits that arise from data research.
- **Data controller:** A natural or legal person, agency, public authority, or other body which, alone or jointly, determines the purpose and means of processing data. Controllers make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing.
- **Deidentified data:** De-identified data, otherwise known as safe data, is data that has removed or disguised details that could lead to someone's identity being revealed, such as their name, date of birth, and address. Examples of de-identified data include anonymised data, which completely removes personal information, and pseudonymised data, which replaces identifiable information with a string of numbers and letters. The process of de-identification ensures that data can be used safely in research.
- **Individual level data:** Data collected about specific individuals, including personal characteristics, behaviours, and responses, which are crucial for detailed analysis in various fields.
- **Personal data / personally identifiable information:** Information that can directly identify an individual person without reference to any other information. For example: name, date of birth, postcode, genetic information.
- **Pseudonymised data:** The ICO defines pseudonymisation as a technique that replaces information that directly identifies individuals, or de-couples that information from the resulting dataset. This means that identifying details are replaced with reference numbers or codes, while still allowing the data to be linked back to the individual if necessary. Pseudonymised data remains personal data, as the link to the individual's identity is still retained within the organisation.
- **Public benefit, also known as public good:** Refers to the net positive impact that research can have on society. It encompasses both the benefit aspect, which requires identifiable good outcomes, and the public aspect, which necessitates that these benefits accrue to the public or a segment of it. Researchers must demonstrate how their work will contribute to the public good, adhering to ethical standards and governance principles.
- **Safe Havens / Trusted Research Environments (TREs):** Secure facilities that provide a controlled environment for accessing and processing personal data.

A number of other definitions and other information are available on the RDS website.