

**Public Health Scotland (PHS)
eDRIS User Agreement**

eDRIS Generated Project Dataset

[INSERT NAME OF RESEARCH PROJECT]

[INSERT PROJECT NUMBER]

Table of Contents

1. INTRODUCTION	3
THE PARTIES	3
eDRIS	3
RESEARCH PROJECT	3
USER	3
2 RESPONSIBILITIES	4
USER RESPONSIBILITIES	4
AUTHORISING ORGANISATION	5
3 ACCESS TO THE NATIONAL SAFE HAVEN	5
REQUIREMENTS FOR ACCESSING DATA IN THE NATIONAL SAFE HAVEN BOTH VIA A SAFE SETTING AND VIA REMOTE ACCESS.	5
SAFE SETTING AT NINE BIOQUARTER	6
4 DATA SECURITY	7
HANDLING OF DATA	7
STORAGE AND COPYING OF DATA	7
5 RELEASE OF ANALYTIC OUTPUT	8
RELEASE OF ANALYTIC OUTPUT	8
OUTPUT CLEARANCE	8
6 GENERAL PROVISIONS	9
INTERPRETATION	9
NON-COMPLIANCE	9
7 OFFENCES AND PENALTIES	9
OFFENCES AND SANCTIONS	9
STATUTORY PENALTIES	10
USE OF ANY eDRIS GENERATED PROJECT DATASET FOR PERSONAL OR COMMERCIAL GAIN	11
RIGHT OF APPEAL	11
CLAIMS BY INDIVIDUALS	11
8 REVIEW	11
9 DECLARATIONS AND AGREEMENT	12
9.2 PHS eDRIS USER (YOU)	12
9.3 YOUR AUTHORISING ORGANISATION	12
9.4 STUDENT SUPERVISOR	13
9.5 PUBLIC HEALTH SCOTLAND	13
APPENDIX A	14
GLOSSARY	14
APPENDIX B	16
GUIDING PRINCIPLES FOR DATA LINKAGE	16
APPENDIX C	18
DATA PROTECTION PRINCIPLES	18
APPENDIX D	19
THIS APPENDIX SETS OUT PENALTIES FOR BREACH OF THIS AGREEMENT	19

1. INTRODUCTION

General

1.1 This document is the legal document that individual researchers using eDRIS (as explained below) and their sponsoring or employing organisations enter into prior to the researcher accessing any data. It also contains information on the current legal framework and the penalties that may apply should the individual researcher breach the terms of the legal agreement formed when all Parties to this document sign it (this “**Agreement**”). This Agreement includes various definitions. These are included throughout the document and for ease of reference, are also restated in the Glossary attached as Appendix A to this Agreement.

The Parties

1.2 Parties to this Agreement are:-

1.2.1 The individual researcher named in Clause 9.2 on page 12 (referred to in this Agreement as “**You**”, and “**Your**” shall be construed accordingly).

1.2.2 Public Health Scotland for the Scottish Health Service, a statutory body constituted pursuant to the National Health Service (Scotland) Act 1978 (as amended) and having its headquarters at Gyle Square, 1 South Gyle Crescent, Edinburgh, EH12 9EB (“**PHS**”); and

1.2.3 Your sponsoring or employing organisation named in Clause 9.3 on page 12 (referred to in this Agreement as the “**Authorising Organisation**”).

eDRIS

1.3 The Electronic Data Research and Innovation Service (“**eDRIS**”) is a service delivered by PHS designed to provide a single point of contact and to assist researchers in study design, approvals and procurement of data and access thereto via a secure analytical environment (such secure analytical environment being the “**National Safe Haven**”). eDRIS is designed to assist researchers in upholding the “**Guiding Principles for Data Linkage**” set out in Appendix B attached to this Agreement.

Research Project

1.4 This Agreement relates to the study known as [•] (research project number [•]) which PHS has approved in principle can be conducted in the National Safe Haven via eDRIS (Your “**Research Project**”).

User

1.5 Prior to being provided with appropriate access to any study data which PHS has agreed to make available to You for the purposes of Your Research Project (“**eDRIS Generated Project Dataset**”) and becoming a User (as defined below), You must:

1.5.1 demonstrate that You have satisfactorily completed a mandatory PHS approved training course on privacy, data protection and freedom of information (“**IG Training Course**”), obtained the relevant training

- certificate confirming same ("**Training Certificate**") and provided this to PHS;
- 1.5.2 be aware of the sanctions which may apply should You breach this Agreement or compromise the security, availability or confidentiality of the eDRIS Generated Project Dataset;
 - 1.5.3 understand that the Research Project you are working on must have the approval of all relevant authorising bodies, for example, the Public Benefit and Privacy Panel ("**PBPP**"), Community Health Index Advisory Group ("**CHIAG**"), ethics where appropriate and a copy of such approval must be provided to PHS;
 - 1.5.4 have read and understood the NHS Confidentiality Code of Practice;
 - 1.5.5 be affiliated with a public sector organisation approved by PHS (e.g. University in the European Economic Area ("**EEA**"), NHS organisation, local authority in the UK, Scottish Government etc ("**Approved Organisation**") and have a valid email address associated with the official network of such Approved Organisation ("**Approved Email Address**"); and
 - 1.5.6 sign, date and complete the declaration in Clause 9 agreeing to be bound by the requirements of this Agreement and return it to PHS prior to being given access to any eDRIS Generated Project Dataset. The declaration must also be signed by an authorised signatory from Your Authorising Organisation.
- 1.6 Once you have satisfied the requirements of Clause 1.5 above, You will become a "**User**".

2 RESPONSIBILITIES

User Responsibilities

- 2.1 You are required to familiarise yourself with and comply with the contents of this Agreement, including the Data Protection Principles (see Appendix C hereto). You are obliged to follow the Guiding Principles for Data Linkage and uphold the security and confidentiality of the data and IT resources made available to You as a User.
- 2.2 You are responsible for ensuring that the eDRIS Generated Project Dataset You are working on is not read, viewed or handled by anyone not named in the relevant approvals for the Research Project. If it appears that anyone is deliberately attempting to view, read or handle data not within their authorised duties, the facts must be reported by You immediately to the research coordinator at eDRIS employed by PHS who has been allocated to You ("**Research Coordinator**").
- 2.3 If You are responsible for, or aware of the occurrence of an unintentional disclosure of any eDRIS Generated Project Dataset, You must report this without delay to the Research Coordinator.

- 2.4 You should not discuss information which could breach an individual's privacy in public places and in this context, a public place may be taken to be anywhere where people not directly involved with the Research Project may be present.
- 2.5 You must satisfactorily complete another IG Training Course within 2 weeks of the expiry of the Training Certificate You last provided to PHS if such expiry occurs within the time period of Your Research Project and provide the new Training Certificate to PHS.

Authorising Organisation

- 2.6 The Authorising Organisation agrees to abide by the terms of this Agreement and takes responsibility for ensuring that You comply with the provisions of this Agreement.
- 2.7 The Authorising Organisation acknowledges that any breach of this Agreement may lead to the withdrawal of access to eDRIS for the Authorising Organisation and its staff, and that PHS may report serious legal or regulatory breaches to the appropriate authorities (such as the Information Commissioner and professional regulatory bodies).
- 2.8 The Authorising Organisation acknowledges that any analytic or other software licences which You need must be provided to You entirely at its own expense.

3 ACCESS TO THE NATIONAL SAFE HAVEN

Requirements for accessing data in the National Safe Haven both via a Safe Setting and via remote access

- 3.1 Prior to being given access to any eDRIS Generated Project Dataset, You and Your Authorising Organisation must have read and signed this Agreement. If you have any questions about the contents of this Agreement You should raise them with Your Research Coordinator.
- 3.2 At the start of the Research Project, You will be allocated a user name and password which will provide you with access to the Research Project folder in the National Safe Haven which contains the eDRIS Generated Project Dataset.
- 3.3 You must only access the National Safe Haven from Nine BioQuarter (as explained below) or from another safe physical location approved by PHS (Nine BioQuarter and such approved physical settings being each a "**Safe Setting**") or, if permitted by PHS, from workstations forming part of, located at and managed by Your Authorising Organisation. If Your Authorising Organisation is a local authority, a Safe Setting must be used. You must not login, or attempt to login to the National Safe Haven by any other route.
- 3.4 At each login to the National Safe Haven, You will be required to re-affirm Your undertaking to uphold data confidentiality and security in terms of this Agreement.
- 3.5 Telephone conversations should not be held while accessing the National Safe Haven. The only exception being to contact the Research Coordinator or a member of the research team for the relevant Research Project at the Authorising Organisation.

- 3.6 Whilst accessing the National Safe Haven, You must not leave Your workstation unattended for any reason unless You ensure that You either log out or activate the screen saver.
- 3.7 All reports and analyses (including research findings) arising from the eDRIS Project Generated Dataset (“**Analytic Outputs**”) produced by You must be stored in the National Safe Haven and cleared with the Research Coordinator prior to export from the National Safe Haven to ensure that they do not breach an individual’s privacy. Under no circumstances will uncleared Analytic Output be released (see Clause 5 below).

Safe Setting at Nine BioQuarter

- 3.8 The national Safe Setting is located at Nine BioQuarter, Little France Road, Edinburgh (“**Nine BioQuarter**”). When You are visiting Nine BioQuarter to access the National Safe Haven, this Clause 3.8 applies:
- 3.8.1 Your visit to Nine BioQuarter must be pre-arranged and take place within normal working hours (08.30 - 16.30 Monday to Thursday, 08.30 – 15:30 Friday). Your visit is at PHS convenience and may be cancelled or rescheduled at any point;
- 3.8.2 on arrival at Nine BioQuarter You will come up to the 2nd floor. Please ask at the main building reception for the location of the lifts or stairs. Access to the eDRIS office is via the buzzer at the main office door on the 2nd floor;
- 3.8.3 You will be met by the Research Coordinator or another member of the eDRIS team. They will ask to see Your Photo ID and You will be asked to sign the visitors book. You will be issued with a visitor’s pass;
- 3.8.4 whilst at Nine BioQuarter, You will abide by all local policies pertaining to visitors to the site e.g. car parking, smoking, health and safety, fire evacuation, etc. These will be explained to You by Your eDRIS Research Coordinator or eDRIS team member;
- 3.8.5 the use of landlines / mobile phones or any other mobile device within the National Safe Haven room / booth located at Nine BioQuarter is not allowed. Phones and other devices must be switched off and stored in a locker along with any bags. Only paper, pen and reference books are allowed in the room or booth;
- 3.8.6 if You need to make or receive a call please do so in the kitchen area. Having telephone conversations in the National Safe Haven room / booth where data access is provided is not allowed;
- 3.8.7 CCTV is in operation in each National Safe Haven room / booth recording behaviour. No audio is recorded. Images are retained for 30 days before being overwritten. CCTV is not optional; and
- 3.8.8 at the end of Your visit, You will be escorted back to reception where You must sign out from the visitors’ book and return Your visitor’s pass.

3.9 Other Safe Settings

If You are using a Safe Setting other than Nine BioQuarter. You must comply with the relevant user access terms which are prescribed by the organisation that is responsible for such Safe Setting.

4 DATA SECURITY

Handling of data

4.1 You are required to maintain the security and confidentiality of the eDRIS Generated Project Dataset in accordance with this Agreement and:

- 4.1.1 will not reuse the eDRIS Generated Project Dataset for purposes outside the scope of the Research Project;
- 4.1.2 will not share the eDRIS Generated Project Dataset with anyone who is not a named user on the approvals granted for the Research Project;
- 4.1.3 will not attempt to link the eDRIS Generated Project Dataset to any other data without explicit permission from PHS;
- 4.1.4 will not attempt to identify any individual within the eDRIS Generated Project Dataset; including facial recognition reconstruction;
- 4.1.5 will not attempt to reuse the eDRIS Generated Project Dataset for commercial purposes beyond those stated (if any) in the approvals granted prior to the Research Project commencing;
- 4.1.6 will not share Your National Safe Haven login details with any other person;
- 4.1.7 if permitted to access the National Safe Haven otherwise than from a Safe Setting in terms of Clause 3.3 above, only do so in suitable locations where work cannot be read by anyone not named on the approval request as described in Clause 2.2 above;
- 4.1.8 will not attempt to access the National Safe Haven from a location outside the EEA or a country deemed by the Information Commissioner's Office to have inadequate levels of protection unless you have received permission to do so and are accessing via an approved authorising institution network (VPN) in the UK who is assuming responsibility;
- 4.1.9 will not discuss information which could breach an individual's privacy in a public place, in this context a public place may be taken to be anywhere where people not directly involved with the Research Project may be present.

Storage and copying of Data

4.2 The storage of or copying of all or any of the eDRIS Generated Project Dataset outwith the National Safe Haven is strictly forbidden.

4.3 Under no circumstances should all or any of the eDRIS Generated Project Dataset be copied by hand from the workstation screen or attempts made to save screen shots or photograph the screen.

- 4.4 Under no circumstances should attempts be made to use removable data storage devices (e.g. USB storage devices, memory pens/sticks, personal digital assistants (PDAs), etc) whilst accessing the National Safe Haven. The National Safe Haven includes software to monitor system use.
- 4.5 PHS will securely archive the eDRIS Generated Project Dataset, syntax and Analytic Outputs associated with the Research Project when the Research Project is complete and will retain same for a period of five (5) years.

5 RELEASE OF ANALYTIC OUTPUT

Release of Analytic Output

- 5.1 All Analytic Output produced by You will be reviewed by the Research Coordinator and will only be released from the National Safe Haven by the Research Coordinator in line with the relevant Controllers' disclosure control requirements. A "**Controller**" is a Controller in terms of the European General Data Protection Regulation (2017/679) (GDPR) and is a person or organisation who decides on the purposes and means of the processing of personal data. At the end of Your session during which You access the eDRIS Generated Project Dataset, You must request that any Analytic Outputs created by You are disclosure cleared by Your assigned Research Coordinator. The Research Coordinator will review Your Analytic Outputs to ensure that they do not contain any information which identifies or which could be used in conjunction with other data, to identify an individual. Thereafter, if cleared for release, the Research Coordinator will send them to You via email using Your Approved Email Address. Be aware that the security measures forming part of the National Safe Haven do not allow You to export any data, documents or other work from the National Safe Haven. Only Your Research Coordinator can do this for you.

Output Clearance

- 5.2 You agree to meet the requirements of safe, non person identifiable Analytic Outputs.
- 5.3 Only Analytic Outputs which have been approved by PHS as non person identifiable can be used as part of presentations, publications, papers and analyses. If the approval granted by PHS stipulates a requirement that You share Analytic Outputs with the relevant Controller, it is Your responsibility to ensure that You comply.
- 5.4 In the event that PHS decides not to release the requested Analytic Output, You will have an opportunity to demonstrate to eDRIS and, where appropriate, the Controller(s) for the eDRIS Generated Project Dataset, that the Analytic Output is anonymised and safe for publication or release. However, the final decision to release any Analytic Output remains with PHS and not You.
- 5.5 On request from the Research Coordinator, You must provide a description of variables used, new variables/measures/indices created, documentation of datasets and programs used in producing Your Analytic Output to ensure that the Research Coordinator has the information needed to make a decision on the request for Analytic Output release.
- 5.6 You shall ensure that all publications in any format relating to the Research Project should acknowledge PHS. Depending on the content of the eDRIS Generated Project Dataset, it may also be courteous to acknowledge the Controller(s) associated with

that Research Project. Abstracts/papers intended for journal publication may be required to be reviewed for clearance by Your Research Coordinator. If it is intended to present any unpublished data at a conference/seminar, an abstract may be required for clearance. Whether or not You are required to obtain such clearance will be at the discretion of the relevant Controller(s) and will be confirmed to You prior to the Research Project commencing.

- 5.7 All reports and analyses created by PHS from the eDRIS Generated Project Dataset which are provided to You will already be cleared for disclosure.

6 GENERAL PROVISIONS

Interpretation

- 6.1 If You require additional information in relation to this Agreement, You should discuss the matter with Your Research Coordinator.

Non-Compliance

- 6.2 Any breach of this Agreement may result in You and Your Authorising Organisation being subjected to investigation and imposed with relevant sanctions (as described in Clause 7 below).

7 OFFENCES AND PENALTIES

Offences and Sanctions

- 7.1 Your signing of this Agreement and the signature of Your Authorising Organisation demonstrates that You and Your Authorising Organisation understand the seriousness of the undertakings and the penalties that may be imposed hereunder for breaches of this Agreement. Such penalties are set out in Appendix D.
- 7.2 PHS has discretionary powers over the application of penalties for self-reported, unintentional breaches.
- 7.3 Application of the penalties for intentional breaches of this Agreement is non-discretionary.
- 7.4 If You take full and prompt action to report an unintentional breach, You and Your Authorised Organisation may not be penalised but You may be asked to repeat training. Penalties for repeated, self-reported but unintentional, breaches will increase at PHS's discretion with each breach committed.
- 7.5 Penalties may be imposed at the discretion of PHS for other offences not listed in Appendix D that are considered by PHS to breach the terms and conditions of this Agreement. Penalties for such other offences will be proportionate to the offence (and cannot be determined in advance) but will include the full range of sanctions listed in Appendix D.
- 7.6 Under this Agreement, and if an obligation agreed by all Parties hereto prior to the Research Project commencing (see Clause 5.6 above) You agree to inform the Research Coordinator of any publications (external conferences, journal articles,

reports) using Analytic Outputs and also of any errors found in the eDRIS Generated Project Dataset, Analytic Outputs or publications. Whilst there is no formal penalty hereunder for not informing PHS, You may be contacted by the Research Coordinator to provide such information.

- 7.7 All breaches and the penalties applied will be reported in full by the Research Coordinator to the PHS Executive Team and other interested parties.

Statutory Penalties

- 7.8 PHS believe that penalties will only be an effective deterrent if they are fully understood, and it should also be clear that PHS is much more concerned about prevention than punishment. In relation to statutory penalties:

7.8.1 The Statistics and Registration Services Act 2007 (“**SRSA 2007**”) states, in Section 39(9) that a person who contravenes subsection (1) (which states that any person who has directly or indirectly received personal information from the Statistics Board must not disclose it) “is guilty of an offence and liable — (a) on conviction on indictment, to imprisonment for a term not exceeding two years, or to a fine, or both; (b) on summary conviction, to imprisonment for a term not exceeding twelve months, or to a fine not exceeding the statutory maximum, or both.” However, section 39(9) of SRSA 2007 does not apply when the person making the disclosure “reasonably believes” that either personal information is not specified in the information which is disclosed, or that a person's identity cannot be deduced from the information, or that a person's identity cannot be deduced from the information taken together with any other published information;

7.8.2 nevertheless, the extraction of personal information from the National Safe Haven remains a breach of this Agreement, regardless of whether You had ‘reasonable belief’. You are advised through this Agreement that You should regard only the Analytic Outputs which have been procured by the Research Coordinator or PHS member of staff, to be non-disclosive, and that receiving such an Analytic Output from the Research Coordinator or PHS member of staff is the basis for their ‘reasonable belief’;

7.8.3 You are made aware through this Agreement that PHS will always seek prosecution for any breach of SRSA 2007. Under SRSA 2007, the only exceptions are where the disclosure was unintentional and self-reported, or the ‘reasonable belief’ defence is unambiguously relevant. However, the reasonable belief defence is effectively removed in light of the information provided in this Agreement and

7.8.4 Section 170 of the Data Protection Act 2018 states that knowingly or recklessly obtaining or disclosing personal data without the consent of the Controller, or procuring the disclosure of personal data to another person without the consent of the Controller, or after obtaining it, retaining it without the consent of the person who was the Controller of it when it was obtained, is a criminal offence. It is also an offence to knowingly or recklessly re-identify information that is de-identified personal data without the consent of the Controller responsible for de-identifying it (Section 171). PHS will inform the appropriate authorities if it believes an offence has been committed.

Use of any eDRIS Generated Project Dataset for personal or commercial gain

- 7.9 Unless stated in the approvals granted prior to the Research Project commencing, the selling on, and any other commercial exploitation of, the eDRIS Generated Project Dataset or Analytic Outputs created as part of the Research Project for any personal financial or commercial exploitation or gain, and such use of eDRIS by You acting as paid 'agents' of businesses, are strictly forbidden.

Right of appeal

- 7.10 If You consider a penalty following a self-reported, unintentional breach is unfair, the right of appeal is to the Director of Data Driven Innovation, NHS Public Health Scotland.

Claims by Individuals

- 7.11 It should be noted that whilst eDRIS Generated Project Dataset subjects are not the owners of the eDRIS Generated Project Dataset for the purposes of this Agreement, they have the right to take independent civil action against any offender who causes them harm by release of their personal information.

8 REVIEW

This Agreement will be reviewed by PHS every two years or more frequently if appropriate, to take into account changes to legislation that may occur, and/or guidance from the Scottish Government and/or PHS.

9 DECLARATIONS AND AGREEMENT

9.1 Please ensure that Clauses 1.4, 9.2 and 9.3 are completed before returning this form to eDRIS. Where relevant, 4 should also be completed.

9.2 PHS eDRIS User (You)

By signing and dating below, You confirm that You have read, understood and agree to comply with all the provisions of this Agreement. Any breach by You of this Agreement may result in Your access to the National Safe Haven being restricted and You and/or Your Authorising Organisation may be subject to sanctions. PHS has a duty, and is entitled hereunder, to report legal or regulatory breaches to the appropriate authorities (such as the Information Commissioner and professional regulatory bodies).

Name: _____
Position: _____
Organisation: _____
Signature: _____
Date signed: _____
Research Project Number: _____

9.3 Your Authorising Organisation

(Note: Must be signed by a Head of Department, Information Custodian, or equivalent.)

“We declare that the above named researcher is a bona fide researcher engaged in the Research Project which is a reputable study for which all relevant permissions have been granted, and that the data requested can be entrusted to this person in the knowledge that they will conscientiously discharge their obligations in regard to the confidentiality of the data. We, the Authorising Organisation, agree to abide by all the terms of this Agreement and shall ensure that the above named researcher complies with all the provisions of this Agreement.

We declare that we understand that any breach of this Agreement by us or by the above named researcher may lead to the withdrawal of access for this Authorising Organisation and its staff, and that PHS has a duty, and is entitled hereunder, to report legal or regulatory breaches to the appropriate authorities (such as the Information Commissioner and professional regulatory bodies).”

Name: _____
Position: _____
Signature: _____
Date signed: _____
For and On behalf of _____ (Name of Authorising Organisation)

9.4 Student Supervisor

(Note: Where You are a student, the following declaration must be signed by Your supervisor.)

By signing and dating below, the student's supervisor confirms that he/she will ensure that the above named researcher has read, understood and will comply with all the provisions of this Agreement.

Name: _____
Position: _____
Signature: _____
Date signed: _____
For and On behalf of _____ (Name of Authorising Organisation)

9.5 Public Health Scotland

(Note: This section must be completed by the eDRIS Team for all User Agreements.)

Name: _____
Position: _____
Signature: _____
Date signed: _____
For and On behalf of Public Health Scotland for the Scottish Health Service

APPENDIX A

Glossary

Agreement – this whole document, as signed by all the parties to it. (Clause 1.1)

Analytic Output - all reports and analyses (including research findings) arising from the eDRIS Project Generated Dataset. (Clause 3.7)

Approved Email Address – a valid email address used by the researcher associated with the official network of the researcher's Authorising Organisation. (Clause 1.5.5)

Approved Organisations - public sector organisations approved by PHS (e.g. Universities in the EEA, NHS, local authorities and Scottish Government). (Clause 1.5.5)

Authorising Organisation - is the employing or sponsoring organisation named in Clause 9.3 and signing this Agreement in support of the User. The Authorising Organisation shall ensure that the User complies with the provisions of this Agreement. (Clause 1.2)

CHIAG – Community Health Index Advisory Group. (Clause 1.5.3)

Controller – a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. (Clause 5.1)

eDRIS Generated Project Dataset – the study data PHS has agreed to provide You. (Clause 1.5)

EEA – European Economic Area. (Clause 1.5.5)

Guiding Principles for Data Linkage – those principles set out in Appendix B.

IG Training Course – a PHS approved training course on privacy, data protection and freedom of information. (Clause 1.5.1)

National Safe Haven – the secure analytical environment procured by PHS and related procedures for providing secure access to data whilst maintaining the utmost confidentiality. (Clause 1.3)

Nine BioQuarter – the National Safe Setting located at Nine BioQuarter, Little France Road, Edinburgh. (Clause 3.8)

PHS – Public Health Scotland. (Clause 1.2)

PBPP – the Public Benefit and Privacy Panel which scrutinises applications for use of NHS controlled data. (Clause 1.5.3)

Research Coordinator – the eDRIS research coordinator employed by PHS who ensures that researchers have completed an IG Training Course, the declarations and this Agreement are signed by the User and the Authorising Organisation (and, if the researcher is a student, by the student's supervisor). Such research coordinator is also responsible for approving Analytic Outputs before release to the User. (Clause 2.2)

Research Project – the study named in Clause 1.4 of this Agreement which PHS has approved in principal can be conducted in the National Safe Haven via eDRIS.

Safe Setting – a safe physical location for accessing the National Safe Haven approved by PHS. (Clause 3.3)

SRSA 2007 – The Statistics and Registration Services Act 2007. (Clause 7.8.1)

Training Certificate – a certificate confirming that the researcher has satisfactorily completed an IG Training Course. (Clause 1.5.1)

User – an individual who is permitted access to study data within the National Safe Haven as defined in the requirements of Clause 1.5.

You or Your – individual researcher named in Clause 9.2 on page 11. (Clause 1.2)

APPENDIX B

Guiding Principles for Data Linkage

The [Guiding Principles for Data Linkage](#) are designed to support the safe and appropriate use of data for research and statistical purposes. This ensures that data linkage is undertaken within a controlled environment and that the research carried out is legal, ethical, secure and efficient.

Before undertaking a data linkage project using eDRIS, researchers must consider and address the Guiding Principles as part of the application process, overseen by eDRIS. These are:

1. **Public Interest** – Ultimately, any data linkage work must be in the public's interest. That is to say, society may benefit from the findings of the work. Protection of privacy, efficient use of data, and scientifically sound and ethically robust research and statistics are all in the public interest.
2. **Governance and Public Transparency** – Having accountable governance structures which are transparent to the public is essential to ensure that data is being accessed and linked in an appropriate and responsible manner. Clear decision making processes that are open will help to ensure the appropriate balance of privacy protection, efficient use of data and scientifically sound and ethically robust research and statistics.
3. **Privacy** – The law does not give absolute value to privacy and therefore a balance is needed between respect for privacy, through the proportionate mitigation of risk, and the potential benefits to all through the use of data for statistical and research purposes. Methods for mitigating risks to privacy include anonymisation and security. Where data subjects consent to their personal data being shared or linked, privacy risk must still be considered. Particular attention should be given to:
 - a) **Consent** – Consent of data subjects is an important consideration, although it is not a necessary requirement for data linkage under data protection legislation. The consent principles should be departed from only where there is a strong justification and approval has been granted by an appropriate oversight body.
 - b) **Anonymisation** – There are degrees of data anonymisation and it may not be possible to completely remove the risk of re-identification. Nevertheless, data can be anonymised sufficiently (often referred to as pseudoanonymised) for data controllers to make a reasonable risk-based judgement that data can be shared. The anonymisation principles may have less importance if consent for linkage of non-anonymised data has been given or if linkage has been approved by an appropriate oversight body.
 - c) **Security** – Security of data transfer, storage and use is vital for the protection of privacy, especially where there is any risk of re-identification.
4. **Access and Personnel** – Anyone who applies to access or link data using the National Safe Haven or another Safe Setting must have undergone appropriate training which is necessary to gain 'approved researcher' status. Further security measures can be

taken to prevent any single person or organisation having unrestricted access to data, for example the establishment of an Access Control Policy or Data Access Agreement.

5. **Clinical Trials** - Data linkage as a method to support or enhance clinical trials presents specific requirements which must be considered if appropriate to the project.
6. **Sanctions** - Where organisations or individuals break the law, legal sanctions will apply. Additional sanctions should be considered where the Guiding Principles for Data Linkage are breached.

APPENDIX C

Data Protection Principles

1. Personal Data shall be:-
 - 1.1 processed lawfully, fairly and in a transparent manner;
 - 1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - 1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - 1.4 accurate and, where necessary, kept up-to-date;
 - 1.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
and
 - 1.6 processed in a manner that ensures appropriate security of the personal data.
2. The Controller shall be responsible for, and be able to demonstrate, compliance with the Principles.

APPENDIX D

This Appendix sets out penalties for breach of this Agreement. Reference to “suspension” means suspension from use of eDRIS.

OFFENCE	PENALTY	NOTES/EXAMPLES
Attempt to use data for purpose not specified in the application	INDIVIDUAL permanent suspension INSTITUTION 6 months suspension	An example includes using eDRIS Project Generated Dataset obtained for a new research study that has not been approved or for commercial use or gain.
Attempt to access datasets to which not authorised	INDIVIDUAL permanent suspension INSTITUTION – 6 months suspension	
Deliberately making an identifiable eDRIS Project Generated Dataset available to others	INDIVIDUAL permanent suspension INSTITUTION – 6 months suspension Making an identifiable eDRIS Project Generated Dataset available to others is a criminal offence and breaches may be subject to prosecution. Identifying a relevant individual and providing that information to another party for personal gain is a serious criminal offence in terms of the SRSA 2007, with potentially a 2 year jail term, a £2000 fine, and a criminal record. See Clause 7.8.4 in relation to Section 170 of the Data Protection Act 2018 which states that the knowing or reckless obtaining or disclosure of personal data without consent of the controller etc is a criminal offence.	

eDRIS User Agreement v16

OFFENCE	PENALTY	NOTES/EXAMPLES
Attempt to identify individuals	INDIVIDUAL permanent suspension INSTITUTION – 6 months suspension See Clause 7.8.4 in relation to Section 171 of the Data Protection Act 2018 which states that knowingly or recklessly re-identifying de-identified personal data without the consent of the controller is a criminal offence.	This is where You attempt to identify an individual, household or business in the data.
Infringing security requirements	INDIVIDUAL permanent suspension INSTITUTION – 6 months suspension	See e.g. Clause 4 (Data Security).
Transferring log in details to any other user	INDIVIDUAL - First offence 1 year access suspension Second offence permanent suspension INSTITUTION – for second offence, 6 months suspension	This includes sharing login details (whether user name, password or both) with someone else, even someone working on the same project or a supervisor.
Providing false information on the PHS eDRIS User Agreement or Declaration	INDIVIDUAL - first offence 6 months suspension Second offence permanent suspension INSTITUTION – second offence 6 months suspension	
Failure to report a disclosure	INDIVIDUAL – first minor infringement written warning First offence (more than a minor infringement) - 6 months suspension (individual) Second offence (whether minor or not) - permanent suspension (individual);	An example includes where there has been an unintentional disclosure and You have become aware and have chosen not to inform the Research Coordinator

eDRIS User Agreement v16

OFFENCE	PENALTY	NOTES/EXAMPLES
	INSTITUTION – second offence 6 months suspension	
Sharing any eDRIS Project Generated Dataset which has not been disclosure cleared.	INDIVIDUAL - minor infringement written warning First offence (more than a minor infringement) - 6 months suspension (individual) Second offence (whether minor or not) - permanent suspension (individual); INSTITUTION – second offence 6 months suspension	This includes, for example, data transcribed, written or photographed from the screen
Infringing Safe Haven requirements not listed above	INDIVIDUAL - minor infringement written warning First offence (more than a minor infringement) - 6 months suspension (individual) Second offence (whether minor or not) - permanent suspension (individual); INSTITUTION – second offence 6 months suspension	