Data Protection Impact Assessment (DPIA) Questionnaire for

Hosting of PHS/NSS Data in the National Safe Haven to support COVID-19 Related Research and Analyses

DRAFT V0.1

Data Protection Reference Number: DP20210013

28th September 2020

DOCUMENT CONTROL SHEET

Key Information

Title	Hosting of PHS Data in the National Safe Haven to support COVID-19 Related Research and Analyses
Date Published/ Issued	
Date Effective From	1st April 2020
Version/ Issue Number	Version 2.1
Document Type	DPIA
Document Status	DRAFT
Author	Carole Morris
Owner	Carole Morris
Approvers	PHS Data Protection Officer
Contact	Carole.morris@phs.scot
File Name	DPIA – COVID-19 Research Database – National Safe Haven

Revision History

Version	Date	Summary of Changes
1.0	18/05/2020	Initial draft of full DPIA from rapid COVID DPIA
2.0	30/06/2020	2nd version incorporated DPO 1st review suggestions
2.1	30/03/2021	Minor content updates

Approvals

Version	Date	Name	Designation
2.0	28/09/2020	Richmond Davies	PHS Data Protection Officer

About the Data Protection Impact Assessment (DPIA)

The DPIA (also known as privacy impact assessment or PIA) is an assessment tool which is used to identify, assess and mitigate any actual or potential risks to privacy created by a proposed or existing process or project that involves the use of personal data. It helps us to identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. Failing to manage privacy risks appropriately can lead to enforcement action from the Information Commissioner's Office (ICO), which can include substantial fines. The DPIA is just one specific aspect of risk management, and therefore feeds into the overall risk management processes and controls in our organisation.

A DPIA is not a 'tick-box' exercise. Consultation may take a number of weeks to complete, so make sure that key stakeholders are engaged early, and that you have enough time prior to delivery to iron out any issues.

Carrying out a DPIA is an iterative process. Once complete, a review date within the next 3 years must be set. Should a specific change in purpose, substantial change in service or change in the law occur before the review date, the DPIA must be re-done.

The ICO code of practice on conducting privacy impact assessments is a useful source of advice.

Is a DPIA required?

Firstly, in order to identify whether you need to carry out a DPIA, you must complete the Screening Questions published on Spark. A DPIA must be completed for all processes or projects for which the Screening Questions indicate a DPIA is necessary.

Secondly, you must consider the aspects listed in the table below:

- If the process or project that you are planning has one or more of the aspects listed below then it is a LEGAL REQUIREMENT to complete a DPIA at an early stage, as the processing/ project is legally classified of a risky nature. Failure to carry out a DPIA in these circumstances is ILLEGAL.
- If the process or project that you are planning has none of the aspects listed below, but the Screening Questions indicated a DPIA was necessary, you must still continue with a DPIA. Although deemed to be of a less risky nature, completion of a DPIA is a best practice requirement in these circumstances, and provides evidence of our meeting data protection requirements by design and by default.

		YES/NO
1.	The work involves carrying out a ***systematic and extensive evaluation*** of people's personal details, using ***automated processing (including profiling).*** Decisions that have a ***significant effect*** on people will be made as a result of the processing. Includes: Profiling and predicting, especially when using aspects about people's work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements Processing with effects on people such as exclusion or discrimination Excludes:	YES

		YES/NO
	Processing with little or no effect on people	
2.	The work involves carrying out ***large scale*** processing of any of the ***special categories*** of personal data, or of ***personal data relating to criminal convictions and offences.*** Includes: • Racial or ethnic origin data • Political opinions data • Religious or philosophical beliefs data • Trade Union membership data • Genetic data • Biometric data for the purpose of uniquely identifying a person • Health data • Sex life or sexual orientation data • Data which may generally be regarded as increasing risks to people's rights and freedoms e.g. location data, financial data • Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive To decide whether processing is ***large scale*** you must consider: • The number of people affected by the processing, either as a specific number or as a proportion of the relevant population • The volume of data and/or the range of different data items being processed • The duration or permanence of the processing • The geographical extent of the processing activity	YES
3.	The work involves carrying out ***large scale*** and ***systematic monitoring*** of a ***publicly accessible area.*** Includes processing used to observe, monitor or control people.	NO
4.	The work involves ***matching or combining datasets*** e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset.	YES
5.	The work involves processing personal data about ***vulnerable groups.*** This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data.	YES
6.	The work involves ***significant innovation*** or use of a ***new technology.*** Examples could include combining use of finger print and face recognition for improved physical access control; new "Internet of Things" applications.	NO
7.	The work involves transferring personal data across borders ***outside the European Economic Area.***	NO

		YES/NO
8.	The work involves processing that will ***prevent people from exercising a right*** or using a service or a contract e.g. processing in a public area that people passing by cannot avoid.	NO

Step One – Consultation Phase

Consult with all stakeholders about what you wish to do as early as possible in the process. Stakeholders will normally include:

- Key service staff e.g. those who will be managing the process.
- Technical support, especially if a new system is involved. This may involve the relevant IT supplier.
- Other specialists e.g. Topic specialist clinicians, DP Advisors, Caldicott Guardian, Information Security Officer, Data Protection Officer.

Sometimes it will be necessary to consult with service users. This will be particularly relevant if the change in process will change how they interact with our NHS Board, or what information is collected and shared about them.

Early consultation will ensure that appropriate governance and security controls are built into the process as it is being designed and delivered, rather than being 'bolted on' shortly before the change is launched.

Step Two- DPIA drafting

The responsibility for drafting a DPIA will normally sit with the service area that 'owns' the change, however, all stakeholders will have an input. Depending on the nature and complexity of your proposal, more than one service area and/ or Information Asset Owner (IAO) may be the owner(s).

Step Three- Sign-off

When a DPIA has been fully completed, it must be submitted for formal review by the Data Protection Officer. To submit a fully completed DPIA you must e-mail the NSS Data Protection mailbox phs.dataprotection@nhs.net.

The Data Protection Officer will review the DPIA to ensure that all information risks are fully recognised and advise whether appropriate controls are in place. They will decide, where the DPIA shows a high degree of residual risk associated with the proposal, whether it is necessary to notify the ICO. It may be necessary to inform and/or involve the Board's Senior Information Risk Owner (SIRO) as part of this risk assessment and decision-making.

For DPIAs which relate to processing/ projects of a risky nature (i.e. it has one or more of the aspects listed in the table above) the Data Protection Officer will respond within 10 working days. For DPIAs which relate to processing/ projects of a less risky nature (i.e. it has none of the aspects listed in the table above) the Data Protection Officer will respond within 15 working days.

Once reviewed by the Data Protection Officer, the DPIA will need to be signed off by the Information Asset Owner(s) (IAOs), normally a head of service.

1. **What are you trying to do and why? - present (or attach separately), if applicable, a high level summary visualisation of the data flows.**

a.	**Aim, scope and purpose**	This Data Protection Impact Assessment (DPIA) covers the hosting of a subset of variables from key PHS/NSS controlled datasets within the Scottish National Safe Haven in response to the COVID-19 pandemic. The National Safe Haven infrastructure is managed by PHS and operated by University of Edinburgh EPCC The rationale behind hosting of the data in the National Safe Haven is to link and provision data rapidly to respond to critical COVID-19 related research and analysis by bringing together and hosting subsets of key datasets within the National Safe Haven (NSH) from • Public Health Scotland, • National Records Scotland (NRS), • Scottish Government (currently under discussion and each SG Dataset will have an associated DPIA and DPA developed by the SG), • Open Data • and publicly available data. These are identified as the need arises and once confirmed they are listed on the eDRIS web page at https://www.isdscotland.org/products-and-services/edris/COVID-19/_docs/COVID-19-Research-Database-Dataset-and-Variable-Specification-v3.xlsx The existing system cannot provision linked data at speed to support urgent research during this public health emergency because data is only brought together using a create and destroy model for each project. Datasets are not held centrally for quick and rapid access to provision for research. NHS Scotland Public Benefit and Privacy Panel permission was granted on the 18th May 2020 to host NHS Scotland and NRS Vital Events Data within the National Safe Haven Environment. The eDRIS web pages contains a description of the COVID research database and the datasets and variables: https://www.isdscotland.org/products-and-services/edris/COVID-19/index.asp

		Access Approvals All analyses requiring access to the data will require approvals from the data controllers. For access to NHS Scotland data this will be via the NHS Scotland Public Benefit and Privacy Panel and individual data asset owners where applicable such as Audit Data. Only de-identified data will be transferred into a study folder with restricted access as per existing eDRIS processes. NHS Scotland PBPP has a rapid review process in place for COVID related work and therefore eDRIS must also be able to supply the data rapidly to support these and be able to support the increased workload as a result of these. For other data controllers access routes will be discussed and agreed at the time of the initial request for a dataset. The necessary DPA or other governance paperwork will be agreed and established at the offset of these discussions.
b.	**Context including, if applicable, any supporting national policy or legislation**	The Chief Medical Officer has established a Scientific Advisory Group, chaired by the Director of Health Data Research UK at their request. A Data and Intelligence Network sits under this group, led by the Scottish Government's Chief Statistician, to oversee the need for rapid access to data to support this urgent research. The Director of Digital Driven Innovation (DDI) represents PHS on the Scottish Data and Intelligence Network along with representatives from SG, HDRUK, ADR and Academia. PHS through The Scottish National Safe Haven is also supporting the HDRUK National Core Studies programme commissioned by the UK Government. Their remits will be to understand what the research needs are to support the COVID response and recovery phases, identify key datasets required to assist in COVID related rapid research and analyses and how to optimise the infrastructure to support these. Then work with data controllers to identify a research dataset, ensuring due diligence is done around information governance
c.	**Assets e.g. hardware, software used, data flows**	**The Scottish National Safe Haven** The NSH is managed by Public Health Scotland, via the eDRIS team, and operated by University of Edinburgh EPCC under an existing IT Services Agreement since 2015. Data will be transferred regularly from organisations and hosted in SQL databases within an established secure data management zone. Data will be transferred using the approved SERV-U Managed File Transfer into the National Safe Haven.

The data requested will contain fields to allow linkage to take place within the secure data management zone. This includes the Encrypted UPI (Unique Person Identifier) number for linkage at an individual level and full postcode for geography based linkages. This will allow us to link rapidly on demand to other datasets as they are brought in to support the pandemic. For example, clinical trial cohorts.

PHS / NSS Data – Encrypted UPI Number
Where UPI is available on health datasets this will be replaced with the Encrypted UPI Number. NSS Digital & Security (DaS), who manage all of PHS's IT services, has provided eDRIS with access to the Encrypted UPI Number, where available, on datasets held in the NSS Corporate Data warehouse which are controlled by PHS. Where not available, eDRIS analysts can run the CHI Number against a CHI to Encrypted UPI look up table via the Data Virtualisation Platform NSS DaS has established for eDRIS. Thus removing the need to host CHI number for linking within the national safe haven.

Data Virtualisation uses the Denodo Tool, which is software that allows views of datasets held within the corporate data warehouse to be set up as a way of extracting data.

Other Data – Encrypted UPI Number
The identifiers for non-Health data will be processed by the National Records Scotland (NRS) Indexing Team. They will receive only the personal identifiers to allow a probability matching to the population spine. Personal Identifiers are matched and replaced with an Index Number the Index Number is returned to the data provider and attached to the content data. This file is then sent into EPCC via ServU. NRS indexing team will then send in the same index number plus the CHI to eDRIS and eDRIS will run against the Encrypted UPI look up table maintained and updated by NSS DaS. eDRIS will then send in the Encrypted CHI plus the Index Number to EPCC and EPCC will re-attach the Encrypted UPI to the content data in the secure data management zone for the data holding.

NRS have sought CHI advisory Group Approval to send the CHI number to eDRIS.

Extraction and Linkage
Within the National Safe Haven environment, eDRIS analysts will use R Studio to extract the data and link the data for each specific project. This will be done by connecting a Virtual

		machine to the secure data management zone. Individual project data will be extracted, linked and transferred into a study folder within a separate zone of the NSH, known as the analytical environment, for use by the researcher. The researchers will only see de-identified data they have permission to analyse.
d.	**Benefits**	This database will support research and analyses such as: • clinical trials looking at interventions and treatments for COVID-19, • observational studies, • vaccine effectiveness and safety work, • transmission and surveillance • immunity and longitudinal studies • epidemiological studies • modelling • and analyses as required. This will in turn support areas such as rapid decision making on treatments and interventions, understanding the risks to shielded populations, modelling of the impact of COVID-19, influencing policies and planning as the pandemic progresses and during the recovery phases. Encrypted UPI will be required in order to link data “on the go” as new datasets are brought into the database or cohorts are received from external sources.

2. What personal data will be used?

Categories of individuals (data subjects)	Categories of personal data	Any special categories of personal data [see Guidance Notes for definition]	Sources of personal data
Patients	*Encrypted UPI Number (derived from CHI Number), postcode, date of birth, gender, sex, as recorded in a patient record*	*Ethnicity* *Health Data e.g. injury, disease, medical history, diagnosis and clinical treatment; medical examination data, test results.*	*National Datasets held by PHS . As these are identified and confirmed they are listed at* *https://www.isdscotland.org/products-and-services/edris/COVID-19/_docs/COVID-19-Research-Database-Dataset-and-Variable-Specification-v3.xlsx*

Categories of individuals (data subjects)	Categories of personal data	Any special categories of personal data [see Guidance Notes for definition]	Sources of personal data

3. **What legal condition for using the personal data is being relied upon? [see Guidance Notes for the relevant legal conditions]**

Legal condition(s) for *personal data* [see Guidance Notes]	Legal conditions for any *special categories of personal data* [see Guidance Notes]
6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest	9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

4. **Describe how the personal data will be:**

a.	**collected**	Where Encrypted UPI Number is not available, CHI number will be extracted from the source data file. Where CHI number is not available Personal Identifiers will be provided to the PHS indexing team, eDRIS or NRS to probability match to the CHI data / Population Spine and replaced with the Encrypted UPI

b.	**transferred**	CHI Number will be transferred securely to NRS via NSS DaS Approved Globalscape SFT
c.	**accessed and used**	Personal Identifiers will be accessed by PHS analysts and used to probability match a CHI Number and subsequently an Encrypted UPI number. Personal Identifiers will only be provided where governance paperwork such as PBPP approval is in place or will be accessed from PHS datasets under the Access to Data Rules.
d.	**kept up to date, if necessary**	N/A

5. What information is being provided to the people to whom the data relate to ensure that they are aware of this use of their personal data? – This is the ‘right to be informed’ and information such as links to privacy notices (e.g. PHS Privacy Notice) and information leaflets may be included).

There is a national publicly available source of information on how the National Health Service handles personal health information at the NHS Inform website. The PHS Privacy Notice provides information on why PHS process personal information, the legal basis for doing so, how we protect the personal information we use and an individual’s rights.

The eDRIS webpages have outlined how COVID research is being supported through the creation of this website. We are working with Scottish Centre for Administrative Research to use their public panels to get their views on the use of data to support COVID related research.

https://www.isdscotland.org/products-and-services/edris/COVID-19/index.asp

Research Data Scotland have published their web pages in advance of its launch in December 2020 to advise how it’s working with its partners to response to COVID-19

https://blogs.gov.scot/statistics/2020/05/28/our-response-to-covid-19/

https://www.researchdata.scot/our-response-covid-19

Health Data Research UK (HDRUK) are publishing weekly reports on the UK wide response of the research community to support COVID-19.

https://www.hdruk.ac.uk/covid-19/

6. How will people's individual rights in relation to the use of their personal data be addressed by this process? (*Rights are not applicable to all types of processing, and expert advice on this may be necessary*)

- Right of access:

  Individuals have the right of **access** to:
  - Confirm that their personal information is being held or used by us
  - Access their personal information if it is not subject to any access restrictions under data protection law
  - Additional information about how we use their personal information

  Individuals wishing to access their personal information should email the PHS Data Protection Officer at phs.dataprotection@nhs.net. Our physical address is:

  Data Protection Officer
  Public Health Scotland
  Gyle Square (1st floor)
  1 South Gyle Crescent
  Edinburgh
  EH12 9EB
  Tel: 0131 275 6000

If an appropriate health professional deems that access to health data will likely cause serious harm to the physical or mental health of the individual, we will use an exemption for the provisions on the right of access regarding the processing of this data. We will only use this exemption if the conditions are met from paragraph 2(1) of Schedule 3, Part 2 of the Data Protection Act 2018.

- Right to rectification:

Individuals have the qualified right to rectification of personal information we hold about them if they believe it to be inaccurate. To exercise this qualified right, individuals should contact the Data Protection Officer at the address given above. We will consider each request on a case-by-case basis and any rectification will be done in conjunction with the data supplier.

Where such requests are upheld, following agreement with the data suppliers, the individual line listed data entry will be replaced by the rectified entry and, where reasonably practicable, our analysis will be re-run to reflect this change.

Where it is not possible for PHS to uphold this request, such as when historic data has already been used as part of the published aggregated official statistics OR research aggregated outputs in compliance with Data Protection Act 2018, Schedule 2, Part 6 or if the restriction request is excessive or manifestly unfounded, the individual will receive a response from PHS which will include the reasons PHS is not taking action and the individual's right to make a complaint to the ICO.

- Right to object (where applicable):

The provision of de-identified data to researchers is subject to approval from the NHS Scotland Public Benefit and Privacy Panel (PBPP) for health data and by data controllers of any non-health datasets held. PBPP assess each research study to ensure the research is in the public interest. Making information available for research that is in the public interest is part of PHS' legal basis for using personal information. This is covered by the PHS Privacy Notice .

Individuals have the qualified right to object to processing in certain circumstances. To exercise this qualified right, individuals should contact the Data Protection Officer at the address given above. PHS will consider each request on a case-by-case basis. It is highly unlikely that such a request will be upheld. This is because we rely on our lawful basis of public task because it is necessary for the performance of a task carried out in the public interest for processing personal data. In addition, we rely on our lawful processing operations for scientific, historical research and statistical purposes as set out in this DPIA.

- Right to restrict processing (where applicable):

Individuals have the qualified right to restrict the use of their data in certain circumstances, for example, if the individual is awaiting the outcome of their rectification request which is not **excessive or manifestly unfounded**. To exercise this qualified right, individuals should contact the Data Protection Officer at the address given above.

If circumstances allow and a decision is made to uphold the right to restrict processing, then the few authorised PHS staff who have access to the data will incorporate statistical codes in their analysis to isolate the affected record. The individuals will then be informed in accordance with our **notification obligation**.

If a decision is made to set aside this right for reasons such as our lawful processing for scientific, historical research or statistical purposes, then the individual will receive a response from PHS which will include the reasons PHS is not taking action and the individual's right to make a complaint to the ICO.

- Right to data portability (where applicable):

Individuals have the qualified right to data portability in certain circumstances. However, for this data processing work described in this DPIA, PHS is processing personal data under the lawful basis as described in this DPIA which is neither based on consent nor on performance of a contract and so the right to portability does not apply.

- Right to erasure (where applicable):

Individuals have the qualified right to erasure in certain circumstances. However, for this data processing work described in this DPIA, PHS is processing personal data under the lawful basis which is not based on consent and described in this DPIA. Therefore, the right to erasure does not apply.

- Rights in relation to automated decision-making and profiling (where applicable):

  Individuals have the qualified right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them in certain circumstances. As the processing described in this DPIA does not involve automated processing or profiling which neither produces legal effects on individuals nor significantly affect individuals, this right does not apply.

7. For how long will the personal data be kept? (*reference our Records Management, Document Storage and Retention Policy*)

The COVID Research Data holding will be held for the duration of the pandemic and the recovery phases. Discussion will be held with NHS Scotland, PBPP and other data controllers when the pandemic is declared over by the Scottish Government as to whether there is a need to retain the data for longer to support the recovery phases more rapidly or longer term COVID related research. However, retention periods will comply with the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020

Data will be disposed of in accordance with PHS Data Destruction policy. Disposal will be carried out by suitably qualified staff. Evidence of destruction will be provided by EPCC when requested by eDRIS to delete the stored data.

8. Who will have access to the personal data?

Access by eDRIS staff will be required:

- Extract data from the national health data sources held by PHS / NSS
- Replace the CHI number with the Encrypted UPI Number
- Extract, link and provision the data for each individual project within the National Safe Haven environment

Access will be strictly monitored and individuals will be required to complete IG training if they have not already done so.

Data transfer and IT administration

EPCC IT staff that administer and maintain the National Safe Haven environment will have access to the servers on which the data is stored. They will be subject to the terms laid out in the IT Services Agreement between NSS and University of Edinburgh (UoE). Staff have completed appropriate IG training.

Access by EPCC will be required:

- to assist with the resolution of IT issues, such as disk corruption, any necessary maintenance of the server and monitoring of the ongoing data transfer

9. Will the personal data be routinely shared with any other service or organisation? – if yes, provide details of sharing agreement(s) and any other relevant controls. Advice on data sharing requirements is in the Scottish Information Sharing Toolkit.

No

10. Will the personal data be processed by a Data Processor e.g. an IT services provider? – [see Guidance Notes for the definition of Data Processor]. If yes, provide details of selection criteria, processing instructions and contract (may be attached separately).

Yes

NSS DaS powers all of PHS's IT and security arrangements via a shared services arrangement between NSS and PHS. An IT Services Agreement is in place between NSS and UoE. This is also referred to as "the contract" between NSS and UoE. This Agreement has been updated in line with GDPR and was signed off by both parties in August 2018.

11. Describe what *organisational* controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary.)

Type of Control – examples	**Description**
Information security and related policy(ies)	Our security principles deployed adhere to the NHS Scotland Information Security Policy framework (DL (2015)17). Reference: IT Acceptable Use Policy System Security Policy – As this document is highly confidential a copy of his policy is available on request should the panel require it.

Type of Control – examples	Description
	IT Services Agreement between NSS and UoE
Staff training	All staff have GDPR compliant information governance training within a training cycle in place in accordance with two-yearly PHS IG training policy. All members of the eDRIS team, IT admin staff and those IT developers working on the SMI project must have completed a PBPP approved IG training course and provided evidence of this to eDRIS. All eDRIS RCs and IT admin staff are bound by confidentiality clauses in their employment contract with their employing organisation. Note: no researcher has access to the personal data. However, all researchers (users) must be an approved researcher. They must have completed a PBPP approved IG training course and provided evidence of this to eDRIS. All researchers must also sign the eDRIS User Agreement which describes acceptable use of the National Safe Haven and outlines the penalties for misuse.
Adverse event reporting and management	All perceived or actual breaches will be reported to the relevant organisation and, in PHS, managed in line with the adverse events management policy Reference: Adverse Events Management Policy (including Duty of Candour) IT admin staff would raise through the UoE adverse event reporting process. They would also notify eDRIS of any breach. Researchers are expected to notify their eDRIS RC in the event of a breach. This is covered in the eDRIS User Agreement (2.1.3).
Physical access and authorisation controls	PHS staff have controlled authorisation of access to personal data. Staff have a 6-

Type of Control – examples	Description
	monthly authorisation cycle of access to patient personal data as well as user authentication methods for accessing personal data. The personal data is physically held within the University of Edinburgh's Advanced Computing Facility (ACF). This is a stand-alone secure facility with access generally limited to University staff who operate the facility and contractors but only in the presence of University staff. Visitor access is not encouraged and is strictly supervised.
Environmental controls	NHS Scotland office locations, including PHS, implement environmental and physical security good practice including security perimeters around buildings, building access control, CCTV, internal access control using staff ID cards. The ACF has alternative power supplies available in the event of a major power outage. There is also fire and flood protection. PHS home working policy applies during the COVID-19 pandemic and staff will securely and remotely access the PHS networks through a 2 factor authentication process.
Information asset management including management of backups and asset disposal	This work will have an entry in the information asset register. (IAR-PHI-2829) Management of asset disposal will be in accordance with our Records Management, Documents Storage and Retention Policy. Our servers, which are powered by NSS Digital and Security, have their contents backed up daily and backups up to a week can be recovered.
Business continuity	PHS complies with the NSS resilience management plan which covers strategic management response to significant or major business continuity incidents. It details actions to ensure business can continue to operate at acceptable levels until such time as normal operations are restored.

Type of Control – examples	Description
	In the event of failure data can be restored from the backups. This is not an immediate, failover system; there will be a delay in recreating the environment and restoring the data.
Add others where applicable	

12. <u>Describe what *technical* controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary).</u>

Type of Control – examples	Description
System access levels and user authentication controls	All users of patient personal identifiers in Public Health Scotland have authentication controls for user access and identity. RCs access the safe haven using two-factor authentication. A random PIN is sent to a user for each session login. The RC then enters their username and password to access the data. IT admin staff have direct access to the safe haven in case of major failures that require this access path. Researchers do not have access to the personal data, they also access the safe haven using two-factor authentication. The only difference is that they have a separate project login for each study they are working on.
System auditing functionality and procedures	Our data systems have audit functionality which records user access to confidential data items. Authorised staff have their access controlled by individual user identifiers and passwords and their access is revised six monthly. NSS Digital and Security, who powers our data security, has procedures in place to investigate unauthorised access. All access to the National Safe Haven is logged. IT admin staff receive event notification and take appropriate action if necessary which may include raising a breach.

Type of Control – examples	**Description**
Operating system controls such as vulnerability scanning and anti-virus software	Anti-malware application exists across all laptop and desktop devices. This application is updated automatically with up to date IDEs. Software patch management to device operating system and standard applications (e.g. Microsoft, etc) are carried out in line with NSS Digital and Security policy. All physical servers have anti-virus installed. Project specific VMs, in the National Safe Haven, which contain a project's own software also have anti-virus.
Network security such as firewalls and penetration testing	Patient personal data are stored on our secure servers which are managed by NSS Digital and Security. The servers are at the NSS approved Data Centre. It is a secure facility with restricted access and is managed, operates and is audited through the NHS Scotland contract. Servers are secured through patch management, anti-virus checking and are secured behind firewalls. Perimeter firewall to the National Safe Haven. Access is only allowed from whitelisted IP addresses from approved institutions such as academia and NHS. Internal firewalls create separate secure areas for researchers doing analysis on de-identified data and the storage and processing of personal data. The National Safe Haven is subject to an annual penetration test
Encryption of special category personal data	PHS relies on access controls rather than encryption at rest to enhance data security. However, approved methods of transfer of data within NHS Scotland involve encryption within the Scottish wide area network. Data is encrypted during transfer but not at rest within the National Safe haven.
Cyber Essentials compliance (if applicable)	NSS Digital and Security powers the PHS data security. NSS is undergoing reaccreditation of its cyber essentials certificate.

Type of Control – examples	**Description**
System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available)	SSP including full risk and threat assessment covers the entire National Safe Haven infrastructure Residual risks of 8 or higher have been accepted (section 9.1.4 of SSP) by SIRO. This is important in relation to the risks and their residual risk scores identified in section 15 below. All these risks fit into the threat categories highlighted in 9.1.4.
Details of ISO27001/02 accreditation (if applicable)	We are not required to comply with ISO 27001, but with the NHS Scotland Information Security Policy which is in line with ISO 27001. NSS Digital and Security, which powers PHS data security, is regularly audited to ensure compliance with the policy. The National Safe Haven meets the requirements of the NHSS Information Security Policy. This is aligned to ISO27001.
Add others where applicable	

13. Will personal data be transferred to outside the United Kingdom or countries without an European Commission-designated adequate level of protection? – if yes, provide details of the safeguards that will be in place for the transfer(s).

No

14. Describe who has been consulted in relation to this process – e.g. subject matter experts, service providers, service users.

This Data Protection Impact Assessment (DPIA) has been developed in consultation with:

- Information Governance colleagues – PHS
- Public Benefit and Privacy Panel
- Senior managers in PHS

- Scottish Government Scientific Advisory Group

15. In light of what is proposed, indicate what level of risk has been identified in relation to the following data protection principles:

Principle	***Low/ Green***	***Medium/ Amber***	***High/ Red***
Personal data is processed in a fair, lawful and transparent manner	x		
Personal data is collected for specific, explicit and legitimate purposes	x		
Personal data is adequate, relevant and limited to what is necessary	x		
Personal data is accurate, and kept up to date	x		
Personal data is kept no longer than necessary		x	
Personal data is processed in a manner that ensures adequate security	x		

16. **Risks and actions identified [see Guidance Notes for more information]. List all that you have identified and ensure that these integrate properly with our NHS Board's risk management process ('IRMA'):**

Description	**Likelihood**	**Impact**	**Overall Risk rating (L x I)**	**Mitigation/ Actions** *(i.e. steps taken to reduce the likelihood which will result in a reduced residual risk)*	**Residual Risk** *(new 'Likelihood' score x 'Impact' score)*	**Name of Risk Owner**	**Date**
Access to Data held by PHS is no longer available through Data Virtualisation	2	4	8	Data will be extracted by NSS DaS or another access route established	4	Head of eDRIS (Carole Morris)	
Serv-U secure file transfer which is recognised and is incorporated in an annual security penetration testing is not available for use	2	4	8	NSS Globalscape file transfer tool could be utilised if needed	4	Head of eDRIS (Carole Morris)	
Data is accessed by unauthorised users	**2**	**5**	**10**	Recognised security assessed environment with strictly governed access and technical measures. 2FA process from whitelisted IP Addresses only is used. Annually penetration tested and reviewed by NSS DaS security	**5**	Head of eDRIS (Carole Morris)	

Description	**Likelihood**	**Impact**	**Overall Risk rating (L x I)**	**Mitigation/ Actions** *(i.e. steps taken to reduce the likelihood which will result in a reduced residual risk)*	**Residual Risk** *(new 'Likelihood' score x 'Impact' score)*	**Name of Risk Owner**	**Date**
				Only agreed data will be added as identified by the key COVID response groups such as Scottish Data and Intelligence Network, HDRUK National Core Studies, SAGE, PHS. All projects will be governed under existing approvals processes or agreements with data controllers.			
Data Controllers do not provide approval for access to data for a specific project	**3**	**3**	**9**	Established eDRIS processes will be adhered to. All data controllers must agree access and the relevant paperwork arranged. For example, NHS Scotland data is governed by the NHS PBPP. Where a data controller does not agree to access to data the data will not be provisioned.	**3**	Head of eDRIS (Carole Morris)	
Risk of holding non-NHS data	**2**	**3**	**6**	Data controllers will have to agree for us to host the data	**3**	Head of eDRIS	

Description	Likelihood	Impact	Overall Risk rating (L x I)	Mitigation/ Actions *(i.e. steps taken to reduce the likelihood which will result in a reduced residual risk)*	Residual Risk *(new 'Likelihood' score x 'Impact' score)*	Name of Risk Owner	Date
				and they will advise what governance framework is required to support this and define the approval mechanism for access to the data for specific projects. Secure environment recognised by external data controllers who have provided data on a project by project basis previously		(Carole Morris)	

17. **Review and Sign-Off**

Role	Advice/ Action/ Sign-Off	Date
Others, if necessary e.g. Caldicott Guardian, Senior Information Risk Owner (SIRO)		
DPO opinion on whether residual risks need prior notification to the ICO	None	
Information Asset Owner(s) (IAO(s)) Sign Off	Carole Morris	28/09/2020

18. **Recommended Review Date:** 01/10/2022 or earlier if there are material changes to what is described in this DPIA or new risks emerge