**Public Benefit and Privacy Panel for Health and Social Care**

**Guidance for Applicants**

**Contents**

[Introduction 3](#_Toc61969653)

[When is an application appropriate? 3](#_Toc61969654)

[Application Process 4](#_Toc61969655)

[Definitions Used 4](#_Toc61969656)

[Information Governance Training 6](#_Toc61969657)

[UK-wide studies and other approval processes 6](#_Toc61969658)

[Supporting Documents 7](#_Toc61969659)

[Completing the Application Form 8](#_Toc61969660)

[Section 1: Safe People Involved 9](#_Toc61969661)

[1.1 Applicant 9](#_Toc61969662)

[1.2 Academic Supervisor 9](#_Toc61969663)

[1.3 Clinical Lead 10](#_Toc61969664)

[1.4 Information/Data Custodian 11](#_Toc61969665)

[1.5 Others with access to identifiable or potentially identifiable data, including pseudonymised data 11](#_Toc61969666)

[1.6 Others involved in proposal 12](#_Toc61969667)

[Section 2: Safe Organisations & Bodies 13](#_Toc61969668)

[2.1 Organisation or Body Leading Proposal 13](#_Toc61969669)

[2.2 Main Contact for Lead Organisation 13](#_Toc61969670)

[2.3 Organisation or Body Funding Proposal 13](#_Toc61969671)

[2.4 Research Sponsor 14](#_Toc61969672)

[2.5 Other Relevant Organisations or Bodies 14](#_Toc61969673)

[Section 3: Safe Proposal Overview 15](#_Toc61969674)

[3.1 Proposal Essentials 15](#_Toc61969675)

[3.2 Statutory and Regulatory Context 18](#_Toc61969676)

[3.3 Research Ethics Governance 20](#_Toc61969677)

[3.4 Safe Havens 20](#_Toc61969678)

[Section 4: Safe Data, Data Subjects and Methodology 22](#_Toc61969679)

[4.1 New Data yet to be collected 22](#_Toc61969680)

[4.2 All Other Existing Datasets / sources 22](#_Toc61969681)

[4.3 Data Variables 22](#_Toc61969682)

[4.4 NRS / NHSCR Data Sources 23](#_Toc61969684)

[4.5 Making Contact with Individuals 24](#_Toc61969685)

[4.6 Community Health Index (CHI) Database 24](#_Toc61969686)

[Section 5: Safe Data Processing and Security 26](#_Toc61969687)

[5.1 Access 26](#_Toc61969688)

[5.2 Storage & Use 27](#_Toc61969689)

[5.3 Transfer 29](#_Toc61969690)

[Section 6: Safe Outputs and Review 30](#_Toc61969691)

[6.2 Retention and Disposal of data 30](#_Toc61969692)

[6.3 Review 31](#_Toc61969693)

[Section 7: Declarations 32](#_Toc61969694)

[Contacts 32](#_Toc61969695)

[Appendix A: Reference lists for applicants 33](#_Toc61969696)

[Appendix B: The Caldicott Principles, Data Protection Principles and Law 35](#_Toc61969697)

# Introduction

This guidance document is for use by applicants who are completing application forms for submission to the Public Benefit and Privacy Panel for Health and Social Care (HSC-PBPP). The HSC-PBPP undertakes information governance scrutiny of requests to access NHSScotland (NHSS)- or NHS Central Register (NHSCR)-originated data for a variety of purposes. You should read the Introduction section in full before beginning to complete your application form. You should refer to the Completing the Application Form section whilst filling out your application form.

Your application form (and supporting evidence) is your opportunity to explain your study, project, audit or other piece of work (your ‘proposal’) in detail, to show that it is a carefully considered, well-designed piece of work which will be of demonstrable value to society and will safeguard the privacy rights of those whose information it seeks to use. Please be aware that those reviewing the application are Information Governance leads from NHSS who will not have an intimate knowledge of your proposal, nor an in-depth knowledge of your subject and its background.

Full information about the panel (for applicants, members of the public, and participants in the panel process) is available from the [**HSC-PBPP website**](http://www.informationgovernance.scot.nhs.uk/pbpphsc).

# When is an application appropriate?

An application to HSC-PBPP is primarily for the **secondary** use of individual-level administrative health data, collected by NHSS in the course of normal patient care. If your application is for the use of NHSS data for **direct patient care**, please contact your **local** **NHS Board Information Governance team** for advice **before** completing an application, as it is likely that HSC-PBPP application will not be required.

You must complete an application if your proposal requires any NHSS originated data relating to individuals, derived from information relating to individuals, or of a sensitive nature. Examples are:

* Access to administrative health data for a purpose other than direct patient care.
* Linkage of administrative health data (except within Public Health Scotland (PHS) or NHS National Services Scotland (NSS) where Standard Operating Procedures are followed to assess and mitigate risk).
* Linkage of administrative health data to administrative data from other sectors.
* Linkage of administrative health data to primary data collected by researchers **with or without consent.**
* Transfer of any of these data outside NHSS.
* Commercially sensitive NHS Organisation data.
* Use of administrative data that have been collected and stored for purposes other than direct individual patient care. Examples of administrative health data include the Scottish Morbidity Records and similar data held by PHS or NHS NSS.
* Access **without consent** to data held in individual patients’ clinical records to be used for research either linked or unlinked.

You may complete an application for:

* Any other use of NHSS originated data which you consider to be complex, contentious, having wider national implications, or requiring the scrutiny of the panel (including use of data from a single NHSS board).
* Use of data originating from primary care providers, and from beyond NHSS, but with a relevant implication for the service (for example social care information use).

The following factors do not remove the requirement to complete an application (and should be fully explained at the relevant point in the application form):

* Consent of data subjects, even where consent has been obtained for access to clinical records as part of a clinical study.
* Status of data subjects as patients / non-patients.
* Whether data subjects are alive or deceased.
* Purpose of the proposed work: audit, management, performance, research or other.
* Statutory or regulatory requirement for the proposed work.

# Application Process

You are strongly advised to seek the input of your eDRIS coordinator before completing your application form. Contact the eDRIS Team: [phs.edris@phs.scot](mailto:phs.edris@phs.scot).

You must submit your application via your eDRIS coordinator, who will be your single point of contact throughout the application process.

Once submitted, your application will be passed to Tier 1 information governance (IG) colleagues who will conduct a proportionate IG review of your application. They may approve your application (with or without conditions), seek further information or clarification from you, ask for a resubmission, or refer your application for review by Tier 2 panel members.

If your application is approved (with or without conditions), then you will be issued with an approval letter. The normal expectation is that the application process will be concluded within 30 working days of submission, not including any time that has elapsed while waiting for a response from you. Please note that you should submit evidence that is requested to satisfy any conditions that have been applied to your approval in order to receive a final approval letter from the Panel. If further information or clarification is requested, this will be communicated to you by your eDRIS coordinator, along with a recommended deadline. Your response will be considered by IG colleagues and an outcome determined. Again, if your application is approved, you will be issued with an approval letter. The timescale for the conclusion of an application is dependent upon the timeliness of your response.

If your application is referred for Tier 2 review, it will be passed to a small group of panel members (comprised of public representatives and NHSS Caldicott Guardians) for their opinion. This group may also approve your application (with or without conditions), seek further information or clarification from you, or refer your application for review by the Full Committee. If your application is approved at this stage, you will be issued with an approval letter. It is the normal expectation that the application process will be concluded within 90 working days of submission, not including any time elapsed whilst awaiting a response from you.

If your application is referred for review by the Full Committee, it will be reviewed at the next meeting of the Full Committee. You or a suitable nominee will be invited to attend the meeting. You will be informed of the outcome shortly after the meeting. In this scenario, your application will take longer to conclude, and your eDRIS coordinator will discuss likely timescales with you.

# Definitions Used

**‘A Proposal’**

This is the study, project, audit or other piece of work which is the subject of an application for scrutiny. The entirety of what the applicant proposes in their application form.

The panel has a wide remit to consider applications for use of NHSS data for a variety of purposes. These purposes include use of data for medical research, medical education, healthcare audit, healthcare planning and improvement. For these reasons neither the word ‘study’ or ‘project’ is wholly appropriate to describe the proposed uses of data for which applicants seek the panel’s approval, and so the word ‘proposal’ is used to describe all such work which the panel is asked to consider.

**‘Datasets and data sources’**

These are the Information assets which your proposal seeks to access and use.

You should consider this definition to be wide in scope and include any source of information which you propose to access and use. The data may be highly structured or less structured in nature, already existing or to be newly collected or gathered. Examples may include national datasets, local datasets, national or local extracts from systems, national or local registries or networks, patient records, or new information to be gathered from patients, families or other cohorts. A list of commonly used existing datasets is given in **Table 1** of [Appendix A](#_Appendix_A:_).

**‘Identifiable or potentially identifiable data’**

This is information which does or could be used to identify an individual or individuals. A list of common personal identifying variables is given in **Table 2** of [Appendix A](#_Appendix_A_–).

You should consider this definition to be wide in scope and encompass both data and variables which do identify individuals (e.g. name) as well as data and variables which, even after controls such as anonymisation have been applied, could potentially be used to identify individuals depending on context. Examples include postcode, linkage of dates of admission or discharge to hospital, a specific date, an unusual diagnosis in a defined geographic area, gender or ethnicity or *combinations* of these variables could identify a single individual. The more variables, the more likely the combination of these variables will identify an individual.

**‘Safe Haven’**

A Safe Haven is a physical and technical environment designed to allow secure access and facilitate the safe processing of data.

Several Scottish Government-accredited Safe Haven environments exist in Scotland; these are listed in **Table 3** of [Appendix A](#_Appendix_A_–). Their use for secure access and processing of data represents a significant privacy control and provides additional assurance. Wherever possible the HSC-PBPP encourages the use of these Safe Havens for the access to and analysis of data.

**Definitions of ‘Personal’, ‘Pseudonymised’ and ‘Anonymised Data’**

Where possible, patient identifiers should be removed and the data should be anonymised or pseudonymised.

Personal data relates to any information relating to an identified or identifiable living person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Please note that combinations of variables can make a person more identifiable than any single variable alone, even if direct identifiers have been removed.

Pseudonymisation of data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data. If the identifiers can be replaced so that the data can be linked back to the individual, then the data is only pseudonymised and still counts as personal data under data protection law. Most data obtained from NHSS would be classed as pseudonymised, as the identifiers for the patients within the proposal are usually held by someone, even if they are not accessed by the applicant and their team.

Anonymisation refers to the process of removing personal identifiers (directly and indirectly) that may lead to an individual being identified from that information, or combined together with other information. If personal data can be truly anonymised, then the anonymised data is not subject to data protection law. If there is no way in which the data can be linked back to an individual, by anyone, it can be classed as anonymised. Once a dataset is anonymised, this cannot be reversed.

The Data Protection Act 2018, section 171 states that ‘It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.’

Information about a deceased person does not constitute personal data but it is still subject to the Common Law Duty of Confidentiality.

# Information Governance Training

Although there are a number of Information Governance (IG) courses available in different NHS boards and Trusts throughout the UK, there are few courses that are available to all applicants, and many do not sufficiently cover the IG requirements for the handling of large amounts of health data. HSC-PBPP does not have the capacity to assess all available IG courses, so has limited the approved ones to those that are widely available and of sufficient depth. The HSC-PBPP-approved IG training courses are listed in **Table 4** of [Appendix A](#_Appendix_A_–). HSC\_PBPP requests the IG training is updated every **three** years, regardless of the of the time-frame for which the course provider might say the training is valid. All those with access to the data **must** have valid IG training throughout the whole of the time for which approval is given and data is accessed. If your IG training will expire before your HSC-PBPP approval expires, your training **must** be renewed in sufficient time to continue to access the data.

Evidence of IG training is an important aspect of all applications, giving assurances that individuals are aware of the privacy, confidentiality, data protection and Caldicott implications of working with personal health data. IG training is typically mandatory in NHSS boards and if you have a contract or honorary contract with an NHSS board, you should have undertaken IG training.

**Please note that HSC-PBPP approval will not be given until all people in sections 1.1 – 1.5 have up to date HSC-PBPP-approved IG training.**

# UK-wide studies and other approval processes

HSC-PBPP only covers the use of data from NHSS and NHSCR in Scotland. For applications that require data from elsewhere in the UK, you will need to obtain the appropriate and relevant approvals.

The Health Research Authority (HRA) has stated that if an application for the use of data without consent has been made to HSC-PBPP in Scotland and the activity is also taking place in England/Wales, the Confidentiality Advisory Service in the HRA will take assurance from the HSC-PBPP and not re-review the study. This is not yet a fully reciprocal arrangement.

**Please note HSC-PBPP does not cover ethical review. If your proposal requires ethical review, this must be obtained separately.**

# Supporting Documents

Additional relevant information should be included in support of your application. This is indicated at specific points throughout the application form. The value of supporting evidence will be commensurate with the novelty, complexity, sensitivity, volume and level of risk associated with the proposal. Scrutiny of complex, sensitive or risky proposals will be assisted by providing necessary supporting information. Links to openly accessible web resources can be used instead of physical attachments.

Please list each of the individual pieces of supporting evidence you have submitted with your application form. Please list each supporting document or link with a name which clearly identifies its relevance to the application.

Examples of documents/files which might be submitted in support of an application include:

* Business case or protocol
* Diagram/s illustrating systems in use
* Previous application (of which this is an extension, renewal, re-application)
* Research/ethics approval or evidence to support its absence
* Examples of existing local NHS Board approval (e.g. data access/Caldicott)
* Caldicott Guardian approval from beyond Scotland
* Approval/permission to use data from non-NHSS data controllers
* Data Protection Impact Assessment
* Information Sharing Protocol / Data Sharing Agreement / Data Processor Contract (between relevant parties)
* Risk Assessment / Register / Log
* Information leaflet (participants / public)
* Participant consent / registration form
* Contact form / letter
* Relevant Information governance / information security policies and procedures
* Retention and disposal (records management) policies/procedures.

# Completing the Application Form

You should refer to the sections whilst filling out the corresponding parts of your application form. You can direct any questions or queries to your eDRIS application coordinator via phs.edris@phs.scot

Please do not add anything to or change any blue boxes.

Please do not reformat the form, remove options or change the footer.

Please answer all questions, as instructed, in the white boxes.

To fill in a tick box, double-click on it and change “default value” from “checked / unchecked” as required.

To “choose an item”, click on the text and choose an item from the drop-down menu that should appear.

**Application History and Version Control**

The application history and version control box is **for HSC-PBPP** use and is the audit trail of the approved versions of the application.

All applications for submission will be labelled as version 1.0. Any changes to that version prior to first approval will be version 1.1, 1.2 etc. and the approved version will be version 1.x.

The submission of the first amendment will be version 2.0 and any changes required will mean the approved version will be version 2.x and so on.

Applications should be submitted as both Word and pdf files, labelled as version 1.0. The pdf will be used for review purposes. Any updates of the application in response to clarifications should be done using the Word version, with the changes highlighted and version as 1.1.

When an application is approved, the approved Word version (v 1.x) will be returned to the applicant with the front page completed. This is the approved version that should be used for the any subsequent amendment request, which should be updated and submitted as version 2.0.

The PSD is the Project Specification Document and required for all applications for which eDRIS provide the data. Again, for the first submission to HSC-PBPP, this will be version 1.0 and the approved version will be V1.x.

For any amendment requests for the application that require a change in the PSD this will be the next version up (V2.0). If the amendment does not include a change in the PSD, this will remain at the previously approved version number.

**Pre-submission Checklist**

This is **for the eDRIS coordinator** to complete and should act as a prompt to the eDRIS coordinator to check with the applicant whether these things are in place. This must be completed before the application is sent for review. If this is not completed, the application will be returned to the coordinator.

**Supporting Documents**

Please list the supporting documents that are included with the application submission. Please ensure these are relevant and referenced within the application. Please indicate what type of document they are and give a short, clear filename, so that the reviewers know what to expect when they open the document.

# Section 1: Safe People Involved

### 1.1 Applicant

The applicant is the person filling out the application form and principal contact for the application. Typically, this is the person with operational or day-to-day responsibility for the proposal. If you are filling out the application form, this is you.

You should not complete the application form on behalf of another applicant as Section 7 of the form requires a declaration and undertakings on your behalf.

* + 1. Please provide your own full name.
    2. Please provide your title (for example *Mr, Mrs, Ms, Dr, Professor*).
    3. Please provide your position: this will be your current professional role or roles relevant to your application (for example ‘*Project Coordinator, Scottish Diabetes Research Network’*).
    4. Please give the full name of the organisation on whose behalf you are making the application, or within which you work in your professional capacity as the applicant.

This should include a parent organisation, and sub-division or department if appropriate (for example ‘NHS Tayside, Medical Directorate, ‘University of Edinburgh, Department of Informatics’, ‘Scottish Government, Director General of Health and Social Care’).

* + 1. Please provide your own work address where you can be contacted, including postcode.
    2. Please provide your own work email address. This should be an email address associated with your organisation or institution, and not a personal email address (such as hotmail or gmail).
    3. Please provide your professional organisation and registration number if applicable (e.g. General Medical Council (GMC) 1234567, General Dental Council (GDC)12345).
    4. Please select ‘Yes Standard’ if you have a standard NHS employee contract or ‘Yes honorary’ if you have an honorary NHS contract, or ‘None’ if you do not have an NHS contract.
    5. Please indicate whether this application is part of any academic qualification (post-graduate or under-graduate). If this is the case, please give details of the academic supervisor in section 1.2.

If the application is for a research qualification, the application will be classed as research and should reflect this throughout.

* + 1. Please state which HSC-PBPP-approved Information Governance (IG) training course that you have completed within the last three years. A list of accepted training courses is included in **Table 4** of [Appendix A](#_Appendix_A_–). Please provide the name of the course/s most recently undertaken (e.g. ‘MRC Research, GDPR and Confidentiality: What you really need to know - *online module’*), and the date you completed the training. The eDRIS coordinator will ask to see the certificates as evidence of IG training. The HSC-PBPP requires IG training to be renewed every 3 years.

### 1.2 Academic Supervisor

If this application is being undertaken by the applicant as part of an academic qualification, please complete Section 1.2 to provide details of the main academic supervisor. If the application is for a research qualification, the application will be classed as research and should reflect this throughout.

* + 1. Please provide the full name of the Academic Supervisor.
    2. Please provide the title (for example Mr, Mrs, Ms, Dr, Professor) of the Academic Supervision
    3. Please provide the position of the Academic Supervisor; this will be their current professional role.
    4. Please give the full name of the organisation which the Academic Supervisor represents.
    5. Please provide the work address where the Academic Supervisor can be contacted. including postcode.
    6. Please provide the work email address of the Academic Supervisor. This should be an email address associated with their organisation or institution, and not a personal email address (such as hotmail or gmail).
    7. Please provide the professional registration number of the Academic Supervisor, if applicable: please indicate which type of professional registration (e.g. General Medical Council (GMC) 1234567, General Dental Council (GDC) 12345).
    8. Please select ‘Yes Standard’ if the Academic Supervisor has a standard NHS employee contract or ‘Yes, honorary’ if they have an honorary NHS contract, or ‘None’ if they do not have an NHS contract.
    9. Please state which HSC-PBPP-approved Information Governance (IG) training course that the supervisor has completed within the last three years. Even if the academic supervisor will not personally access the data, the training is required so they are aware of the standards to which the applicant must work. A list of accepted training courses is included in **Table 4** of [Appendix A](#_Appendix_A_–). Please provide the name of the course/s most recently undertaken (e.g. ‘MRC Research, GDPR and Confidentiality: What you really need to know - *online module’*), and the date you completed the training. The eDRIS coordinator will ask to see the certificates as evidence of IG training. The HSC-PBPP requires IG training to be renewed every 3 years.

### Clinical Lead

As you will be accessing health data, the HSC-PBPP requires someone to act as the Clinical Lead for this application, and who has had training in Information Governance even if they will not directly access the data themselves. Under data protection legislation, some legal bases for processing health data require it to be done with the oversight of a clinician or health professional, hence the requirement for clinical responsibility. The clinical lead is a senior clinician / Head of Department / Principal Investigator with overall clinical responsibility for the proposal. This will usually be a registered clinician or senior member of the team, whether directly involved with the processing of data or simply having clinical oversight of the proposal. If this is the Academic supervisor, then please state this in question 1.3.01 (e.g. ‘same as Academic Supervisor)and do not complete the remaining questions in section 1.3.

Please note, someone also completing an academic qualification cannot be the Clinical Lead.

* + 1. Please provide the full name of the clinical lead.
    2. Please provide the title (for example Mr, Mrs, Ms, Dr, Professor) of the clinical lead.
    3. Please provide the position of the clinical lead – this will be their current professional role or roles relevant to your application (for example ‘Medical Director, NHS Grampian’; ‘Director of Neonatal Epidemiology Unit, Glasgow University).
    4. Please give the full name of the organisation which the clinical lead represents. This should include a parent organisation, and sub-division or department if appropriate (e.g. ‘NHS Tayside, Medical Directorate’, ‘University of Edinburgh, Department of Informatics’, ‘Scottish Government, Director General of Health and Social Care’).
    5. Please provide the work address where the clinical sponsor/lead can be contacted, including postcode.
    6. Please provide the work email address of the clinical lead. This should be an email address associated with their organisation or institution, and not a personal email address (hotmail or gmail).
    7. Please provide the professional registration number of the Academic Supervisor, if applicable: please indicate which type of professional registration (e.g. General Medical Council (GMC) 1234567, General Dental Council (GDC) 12345).
    8. Please select ‘Yes Standard’ if the Clinical Lead has a standard NHS employee contract or ‘Yes, honorary’ if they have an honorary NHS contract, or ‘None’ if they do not have an NHS contract.
    9. Please state which HSC-PBPP-approved Information Governance (IG) training course that you have completed within the last three years. A list of accepted training courses is included in **Table 4** of [Appendix A](#_Appendix_A_–). Please provide the name of the course/s most recently undertaken (e.g. ‘MRC Research, GDPR and Confidentiality – what you really need to know - online module’), and the date you completed the training. The eDRIS coordinator will ask to see the certificates as evidence of IG training. The HSC-PBPP requires IG training to be renewed every 3 years.

### 1.4 Information/Data Custodian

The information or data custodian is the person with responsibility for safeguarding the confidentiality of data throughout the proposed work and should have training in Information Governance. An information custodian is a senior colleague with a key role in any proposal and is always required to be named in an application. If this is you (the Applicant) or the Clinical Lead or Academic Supervisor, then please state this in question 1.4.01 (e.g. for example ‘same as Applicant’, ‘same as Clinical Lead or Academic Supervisor’) and do not complete the remaining questions in section 1.4.

Please note, someone also completing an academic qualification cannot be the Information Custodian.

* + 1. Please provide the full name of the information/data custodian.
    2. Please provide the title (for example Mr, Mrs, Ms, Dr, Professor) of the information/data custodian.

1.4.03 Please provide the position of the information/data custodian: this will be their current professional role or roles relevant to your application (for example ‘Medical Director, NHS Grampian).

1.4.04 Please give the full name of the organisation which the information/data custodian represents. This should include a parent organisation, and sub-division or department if appropriate (for example ‘NHS Tayside, Medical Directorate’, ‘University of Edinburgh, Department of Informatics’, ‘Scottish Government, Director General of Health and Social Care’).

* + 1. Please provide the work address where the information/data custodian can be contacted, including postcode.
    2. Please provide the work email address of the information/data custodian. This should be an email address associated with their organisation or institution, and not a personal email address (hotmail or gmail).
    3. Please provide the professional registration number of the Academic Supervisor, if applicable: please indicate which type of professional registration (e.g. General Medical Council (GMC) 1234567, General Dental Council (GDC) 12345).
    4. Please select ‘Yes Standard’ if the information custodian you have a standard NHS employee contract, or ‘Yes, honorary’ if they have an honorary NHS contract, or ‘None’ if they do not have an NHS contract.
    5. Please state which HSC-PBPP-approved Information Governance (IG) training course that the information custodian has completed within the last three years. A list of accepted training courses is included in **Table 4** of [Appendix A](#_Appendix_A_–). Please provide the name of the course/s most recently undertaken (e.g. ‘MRC Research, GDPR and Confidentiality – what you really need to know - online module’), and the date you completed the training. The eDRIS coordinator will ask to see the certificates as evidence of IG training. The HSC-PBPP requires IG training to be renewed every 3 years.

### 1.5 Others with access to identifiable or potentially identifiable data, including pseudonymised data

Please provide details of all additional people who will have access to thepersonalidentifiable or potentially identifiable data. If someone is already in sections 1.1-1.4 they do not need to be included here. This will include those who are processing data on your behalf (for example in research safe havens or linkage agents) and these people also have to have IG training. The headings are as explained above.

Where the organisation and contact details are the same as for the applicant, please indicate this next to each name. The box can be copied for additional people to be added on to the form. Please do not use a separate list.

### 1.6 Others involved in proposal

Please include here the other people involved in the project but who will **not** have access to personal identifiable potentially identifiable or pseudonymised data, but who have a significant involvement in proposal design, content or outcomes. This might include colleagues who will be accessing aggregated tables, interpreting study findings, or providing strategic direction. For applications that will use the National Safe Haven, anyone not in section 1.5 that might need to see an interim output must be in section 1.6. Please provide the requested details for such people. The box can be copied for additional people to be added. Please do not use a separate list.

# Section 2: Safe Organisations & Bodies

### 2.1 Organisation or Body Leading Proposal

This is the organisation (e.g. *University of* *Aberdeen*) or body (e.g. *Scottish Infection Research Network*) that is putting forward the proposal requesting access to data for the purposes specified in the application. The applicant at section 1.1 is acting on this organisation’s behalf and is usually employed by this organisation. Where multiple organisations are collaborating to produce the proposal, the lead organisation should be the one which has a lead in the operational delivery of the proposal and will therefore be taking responsibility for matters relating to the access and processing of data.

2.1.01 Please provide the full name of the organisation or body.

2.1.02 Please indicate what type of organisation this is using the drop-down box.

2.1.02a If the organisation is commercial in nature please provide details of any commercial aspects of the organisation’s work. This should include details of industry sector, the organisation’s activities within this sector, and also any previous experience of working with NHSS data. Please attach any relevant supporting information.

2.1.03 Please indicate whether the organisation is wholly funding or paying the costs of conducting the proposal (by selecting ‘Wholly funding / partially funding / not funding).

**If the answer is wholly funding, you do not need to complete question 2.3.**

### 2.2 Main Contact for Lead Organisation

The organisation (e.g. *University of* *Aberdeen*) or body (e.g. *Scottish Infection Research Network*) is putting forward the proposal requesting access to data for the purposes specified in the application. The applicant at section 1.1 is acting on this organisation’s behalf.

Under the Data Protection Accountability principle, you and your organisation are responsible for complying with Data Protection law and the GDPR and you must be able to demonstrate your compliance. You and your organisation need to put in place appropriate technical and organisational measures to meet the requirements of accountability.

This main contact should be the agreed person within the leading organisation that is aware of the proposal and accepts the organisation’s obligations and roles in respect to any processing of data and compliance with data protection law. Note that this person should not be the Applicant, Clinical Lead, Data custodian or anyone from within the research team but someone who is able to assure the organisation’s role in the project. This role is to ensure organisational accountability for the data and therefore this role should not be filled by anyone involved in the study. If applicable and appropriate, this can be the same person as the Research Sponsor.

2.2.01 Please provide the full name of the Main contact.

2.2.02 Please provide the title (for example *Mr, Mrs, Ms, Dr, Professor*) of the main contact.

2.2.03 Please provide the position of main contact.

2.2.04 Please provide the work email address of the Main Contact. This should be an email address associated with their organisation or institution, and not a personal email address (hotmail or gmail).

### 2.3 Organisation or Body Funding Proposal

Please complete this question if the organisation or body providing the financial resource to fund the proposal is different to the organisation detailed in section 2.1. **You do not need to complete this section if the organisation mentioned in section 2.1.01 is wholly funding the proposal.** Examples of funding bodies include: Medical Research Council (MRC), Chief Scientist’s Office (CSO), Scottish Centre for Administrative Data Research (SCADR), National Institute for Health Research (NIHR).

If Research funding has been obtained for the proposal, it will be considered to be research and all other responses should be consistent with this.

2.3.01 Please provide the full name of the organisation or funding body. If this is an NHSS board, please provide the board name.

2.3.02 Please indicate what type of organisation this is from the drop-down menu.

2.3.02a If the organisation is commercial in nature, please provide details of any commercial aspects of the organisation’s work. This should include details of industry sector, the organisation’s activities within this sector, and also any previous experience of working with NHSScotland data. Please attach any relevant supporting information you wish to provide.

### 2.4 Research Sponsor

Under the UK Policy Framework for Health and Social Care, research projects require a Research Sponsor, who should be aware of all activity regarding the research study. If this box is completed the application is considered to be research and all other responses should be consistent with this.

In the Framework there is a section specific for Sponsors that says:

'9.10. The sponsor is the individual, organisation or partnership that takes on overall responsibility for proportionate, effective arrangements being in place to set up, run and report a research project. **All health and social care research has a sponsor**. The sponsor is normally expected to be the employer of the chief investigator in the case of non-commercial research or the funder in the case of commercial research (The employer or funder is not automatically the sponsor; they explicitly accept the responsibilities of being the sponsor). The sponsor has overall responsibility for the research project.

2.4.01 Please indicate if your proposal comes under this framework (Yes / No).

**If no, please go to question 2.5.**

**If yes, please go to question 2.4.02.**

2.4.02 Please provide the full name of the Research Sponsor.

2.4.03 Please provide the title (for example *Mr, Mrs, Ms, Dr, Professor*) of the Research Sponsor.

2.4.04 Please provide the position of Research Sponsor.

**2.4.05** Please provide the name of the organisation of Research Sponsor

2.4.06 Please provide the work email address of the Research Sponsor.

2.4.07 Please provide the Research Sponsor’s reference number associated with this proposal.

### 2.5 Other Relevant Organisations or Bodies

These are organisations or bodies which have a significant involvement or interest in proposal design, content or outcomes, or who host / employ the people mentioned in section 1. Please provide the requested details for such organisations or bodies. For applications where this is a large number of organisations, the required details can be appended separately, for example in a suitable extract from a study protocol.

# Section 3: Safe Proposal Overview

### 3.1 Proposal Essentials

This is a key section which must clearly outline the nature of the proposal, the ways in which it proposes to use NHSS-originated data and how this will result in benefit for the wider public. It places the proposal in context, and establishes if it has used peer review or lay involvement in the course of its design. Applicants should aim to provide absolute clarity when completing this section, and supporting evidence, specifically referenced, may be useful. You should use clear and concise language, which can be easily understood by colleagues and public partners without a background in epidemiology, health research, statistics or analysis.

3.1.01 Please specify the intended end date of the proposal.

**Please note that projects involving provision of data from the NHS Central Registry for follow up or flagging will be capped at 5 years.**

Similar to NHSCR, for long-term projects, renewal every 5 years may be required to ensure that suitable scrutiny of the project and its use of data is taking place.

This end date should be reflective of the entire duration of the proposal including time for analysis, dissemination and to prepare reports or manuscripts for submission to journals. If the outcome of the proposal will become ‘Business as usual’ for operational purposes, then this should be the intended ‘go live’ date.

To try to reduce the requests for time-extensions to proposals, please factor in how long it will take to obtain the data requested, either through data collection, or the likely time for the data to be extracted. Please check with your eDRIS coordinator, as these time-frames will differ according to the source(s) of the data and the complexity of the request.

**Once an end date is reached access to the data should stop and the data should be archived for a stated time-period (section 6). The end date should not include the archive time.**

3.1.02 Please indicate whether this proposal is a new proposal, or whether it seeks to extend, renew or alter an existing proposal.

3.1.02a If an extension, renewal or related to an existing proposal, please describe these specific changes and how they relate to any associated, currently ongoing application. Please give the reference number, full name and title of any relevant existing proposal. Please provide the existing proposal as a supporting document. Please only provide HSC-PBPP or PAC numbers and NOT XRB numbers for any previous application.

If the previous application is still ongoing, please explain how these will relate to each other; e.g. will the results from one inform the other application?

3.1.03 Please indicate whether this proposal will require regular updates of information.

3.1.03a If Yes, then please advise the frequency. This should be consistent with Q 5.3.02 and the trigger points for transfers of data.

3.1.04 Please indicate the substantive purpose of the proposal. This will be further outlined in your answers within Q 3.1.05 to Q 3.1.11. If the purpose of the proposal is not listed here, please select ‘Other’ and include information in the details box.

Please be clear about your purposes for processing. These need to be specified in any privacy notices or information for individuals. The purpose of the proposal should be consistent: e.g. if you say something is an audit and not research, then research should not be used as the legal basis for processing the data. If you are collecting data for an audit, this cannot automatically be stored for research or become a research database.

If you state in this question that your application is research, then you require a Research Sponsor and Q 2.4 must be completed. In addition, ethical review must be considered and the legal bases for processing data, under data protection law, must be for research.

3.1.05 Please indicate the sources of the data which the proposal seeks to access. This might include one or more of the sources listed, and you should select each that applies. These should be further outlined and justified in your answers in Q 3.1.06 to Q 3.1.11. If the sources of the data it is proposed to access are not listed here, please include these in the ‘other’ details box. These sources should also be consistent with the identity of the data controller for the different datasets requested in Q 4.2.

If you request NRS births or deaths, please tick these boxes even if it is for cohort generation and/or linkage or if you are getting the data from the copies of these data held within PHS.

If you tick NHS Central Registry, you **must** fill in section 4.4 and ensure that NHSCR are aware of the data request; they should have given you a reference number, which is required in section 4.4.

If you tick CHI Database, you **must** fill in section 4.6. Please note that the use of CHI database is **not** for the use of CHI for data linkage or matched controls, but for other information.

3.1.05a Please give details of any data that will be requested from other data controllers (e.g. Scottish Government, Local Authorities, other public sector administrative datasets). If other, please tick the box and state from where the data will be obtained. This is to give the reviewers an indication of the full scope of the data requested for the proposal.

3.1.05b Please give details of the requested data and provide evidence of the data controller approval, once it has been obtained.

3.1.06 Please provide a clear and concise **lay** outline of the proposal. You should use clear concise language which can be easily understood by the public. This is a stand-alone lay summary to inform the public of the use of their health data. This should include why it is required and how the outcomes will benefit the public. All abbreviations should be explained.

Your explanation should not extend beyond 250 words of text. If you are using extracts from study protocols or other relevant existing documentation, please ensure that it is relevant to the section.

Please note that the content of this section will be published on the HSC-PBPP website, to inform the public of the types of proposals that use NHSS data.

3.1.07 Please provide clear, specific aims and objectives or goals of the proposal. This can be done using bullet points. If this is a research proposal you may wish to consider using the PICO principle: Population / Participants, Interventions / Indicators, Comparator / Control and Outcome when responding to this question.

You should use clear concise language which can be easily understood by colleagues and public partners without a clinical background or extensive knowledge and expertise in epidemiology or health research. If you are using extracts from study protocols or other relevant existing documentation, please ensure that it is relevant to the section.

3.1.08 Please describe the envisaged benefits to the public and / or patients. This section must outline why the proposal, and the access to data it proposes, is necessary and to demonstrate a clear connection between this work, its expected outcomes and the benefit to patients or the wider public which will result thereafter. You should use clear, concise language which can be easily understood by colleagues and public partners without a clinical background or extensive knowledge and expertise in epidemiology or health research. If you are using extracts from study protocols or other relevant existing documentation, please ensure that it is relevant to the section and easily understood.

The public benefit of the use of NHSS data for this application must be clearly made. If there is no public benefit, then the application is likely to be referred to Tier 2 or not approved. The use of personal data from NHSS **must** provide a benefit to the public and / or patients.

3.1.09 Please provide a concise details of the proposal. It is essential that you use this section to paint a clear picture of the processing of data which you propose to undertake. Please use language that is understandable by colleagues and public partners without a clinical background or extensive knowledge and expertise in epidemiology or health research.

This should include background and the reasons for requesting the data and data sources, as well as details of sample size, cohort inclusion or exclusion criteria, ranges of data to be used, and incidences of proposed data access / extract / transfer and linkage / matching / anonymisation, etc. You should use clear, concise language which can be easily understood by colleagues and public partners without a clinical background or extensive knowledge and expertise in epidemiology or health research. Please justify the use of the datasets requested and how these will answer your aims and objectives. A number of prompt questions are provided to help you understand and provide the information required by the review panel. If you are using extracts from study protocols or other relevant existing documentation, please ensure that it is relevant to the section. Please do not include academic literature references in the application form. A separate protocol can be provided as a supporting document.

3.1.10 Please provide a clear and concise outline of any statistical methods that will be used in the project. This should be a brief, non-technical description of the statistical analysis, for people who may not have a background in statistics.

3.1.11 Please include a data flow diagram showing what data sources are being accessed and processed by which parties and at what point in the proposal methodology, from patient to outcomes, so that the roles and responsibilities for data controllers and/or processors are clear (e.g. including data controllers, processors and transfers). This illustration can also include key processes undertaken with respect to data, such as anonymisation or linkage. The flow diagram should also show from where the data will be accessed and stored at any point in the process and by whom.

Please ensure the flow diagram is large enough for the text to be read.

If the flow diagram is included in another supporting document, e.g. eDRIS PSD, please state where it can be found, but do not leave this question blank.

3.1.12 Please indicate whether the proposal has focuses on or includes people who might be considered vulnerable. A non-exhaustive list of vulnerable people is included in **Table 5** of [Appendix A](#_Appendix_A_–) of these guidance notes, but you should include any group or cohort which might reasonably be considered vulnerable in nature. This is part of the assessment of how safe is a proposal. Most applications are likely to include vulnerable people, unless they have been specifically excluded.

3.1.12a If the application is focused on or includes vulnerable people, please give further details of these people and why they may be thought to be vulnerable. It is good to acknowledge that vulnerable people might be present in the population for the data requested, even if they are not the focus of the proposal. If vulnerable people are the focus of the proposal, this should be taken into account in Q 4.2.01 about how patients are informed and aware of the use of their data.

3.1.13 Please indicate whether the proposal seeks to access sensitive data. Under GDPR, all health data is classed as special category personal data, some could be considered highly sensitive health data. In addition, some commonly requested variables are also classed as special category data but are not health data (e.g. ethnicity). A non-exhaustive list of special category data and potentially highly sensitive health data categories is included at **Table 6** of [Appendix A](#_Appendix_A_–) of these guidance notes, but you should include any data that, e.g. in combination, might reasonably be considered as sensitive in nature. Any other special category data that is non-health (e.g. ethnicity, religion) should be stated here. This is part of the assessment of how safe is a proposal.

3.1.13a If highly sensitive data, or non-health special category data are required, please provide details and justification of the variables requested.

3.1.14 Please indicate whether the proposal seeks to use information exclusively about deceased persons. This includes where the proposal seeks to access and use individual datasets which consist only of information relating to deceased persons. Please provide details of the relevant data sources. Please note that while deceased people are not subject to data protection law, they are still subject to the common law duty of confidentiality and laws that govern access to their health records. If someone is deceased, the manner of their death may be quite sensitive (e.g. drug overdose, suicide) which may cause some distress to the surviving family and friends. Therefore, the data requested may need to be handled carefully and as safely as if they were still alive.

3.1.15 Please describe how any members of the public, lay representatives or patient groups have been involved in the design or any other aspects of the proposal. This would include details of any public engagement or consultation activity which has been undertaken in the course of designing the proposal. Any supporting evidence resulting from consultation should be provided as supporting evidence.

3.1.15a Please include details as to how this public / lay input affected the design or any other aspect of your proposal, e.g. lay input into a questionnaire about their experience of having this condition, or what would be their research priorities.

3.1.15b Please provide details of your plans of how you will keep the public, lay representatives or patient groups informed about the ongoing use of health data for this application and its outcomes. E.g. this could include newsletters, emails public presentations, workshops.

3.1.16 Please describe any process under which your proposal has been reviewed by any other people, e.g. formal external scientific peer review for research funding, or internal review or review by a third party. Please give details of how this was undertaken, including bodies or organisations involved. If no formal external review has been done, please explain why not.

3.1.17 This question relates to whether a Data Protection Impact Assessment (DPIA) is required and has been carried out for this application or a bigger overarching proposal under which this proposal sits. If you are applying to HSC-PBPP, personal identifiable data and special category data, will be processed for your proposal, even if it is not done by you but on your behalf. Such processing should comply with the Caldicott Principles (**Table 1** [Appendix B](#_Appendix_B__The)) and Data Protection Principles (**Table 2** [Appendix B](#_Appendix_B__The)). In general, for processing of personal and special category data, the ICO suggest that a DPIA should be carried out as the proposal is designed, so that privacy issues are thought through as the proposal is developed. This is called Privacy by Design. In addition, carrying out a DPIA is good practice. The Information Commissioner’s Office (ICO) website has a lot of information about DPIAs, including screening questions as to whether a Data Protection Impact Assessment (DPIA) is a legal requirement for your proposal.

(<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>)

A DPIA is a recognised control for identifying and assessing risk where data is being processed, and may be mandatory for some proposals which are processing personal data. A DPIA should have commenced in the early stages of planning a project and before an application is submitted to the HSC-PBPP. The completed DPIA should be signed-off by your organisation’s Data Protection Officer or IG Lead or Information Asset Owner or Senior Information Risk Owner (SIRO) or other designated person. These might differ with each organisation, but the Data Protection Officer or Information Governance team for your organisation should be able to advise.

3.1.17a If a DPIA has not been carried out, have the ICO screening questions been carried out and accepted by your organisation?

3.1.17b If neither a DPIA nor the screening questions have been done, then you will need to explain and justify why not, and also how your application has been suitably assessed for the risks associated with the processing (by yourself or by others on your behalf) of personal health data.

If the proposal will access the requested data in an accredited Safe Haven (national or regional) and there is no overarching DPIA in place to cover the processing of the personal and special category data prior to the data being made available to the research team, please describe how the use of a Safe Haven mitigates the privacy risks inherent in processing such personal and special category data.

3.1.18 Please indicate if there is *any* commercial aspect or dimension to the proposal or its outcomes. This would include any involvement of commercial organisations at arm’s-length to the proposal, (e.g. outsourced processes, funding, spin-out company), access to data by a commercial company, use of data for a proposal that will be commercialised, or likely impact on commercial organisations, individually or collectively, that might result from the outcomes or methodology of the proposal. Any involvement of a commercial company, needs to be explained carefully as these companies will potentially make money out of the use of free health data.

If the commercial organisation is based outside the European Economic Area (EEA), then special consideration has to be made as GDPR does not allow personal data to be transferred outside the EEA.

3.1.18a Please justify the necessity of the commercial involvement, how it is necessary for the success of the proposal and what the company will gain from their involvement in this proposal. This information is helpful to the reviewers to determine the public benefit against the privacy risk of the use of patients’ health data for the purposes of the commercial company. More specific guidance for work that involves commercial applications is currently being updated and will be included in an appendix to these notes.

3.1.18b Please provide a list of the partners involved and an explanation of how partners in NHS Scotland have been involved in any discussions of the commercialisation and describe how NHSScotland will benefit from such use of patients’ health data? Please provide a formal agreement between the partners so that reviewers can be assured that suitable arrangements are in place for the commercialisation of the outcomes from the use of NHSS data.

3.1.18c Please describe how the commercialisation of any product or outcome and the intellectual property associated with that, will be handled and by whom? Will it be by the company, the applicant’s organisation.

### 3.2 Statutory and Regulatory Context

This section explores the statutes and regulations relevant to the proposal, and ensures that confidentiality, Data Protection and Caldicott obligations have been accounted for. It identifies key controls in place to help reduce risks to individual privacy.

**Personal data** are those which individually, or in combination, identifies an individual: e.g. name, address, postcode, date of birth, identifiable code number (e.g. National Insurance number, CHI number).

**Special category data** are **personal data that needs more protection because it is considered to be sensitive. A list of special category data is** provided in **Table 6** of [Appendix A](#_Appendix_A_–).

**If you are unsure whether to use consent as your legal basis, please read below.**

**Consent** to process personal data has legal definition under data protection legislation. This is not the same as consent to take part in a research study or for medical treatment, which may be required under different legislation. There are usually more appropriate legal bases for processing personal, health and social care data, apart from consent. However, if consent to process personal data is the legal basis used, all the relevant rights of the subjects must be upheld (see **Table 3**, [Appendix B](#_Appendix_B:_)) including the right to be erased (or forgotten). If this is not possible then, consent should not be used as a lawful basis for processing data.

In relation to consent, the ICO states: ‘*Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative. Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair. If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis. Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.’*

3.2.01 Please indicate if your proposal is substantively in response to, or calls upon, a statutory or regulatory requirement placed upon your organisation. This might include the exercise of a statutory power, or a regulatory requirement to carry out audit or monitoring under specific legislation. Please provide details of any statutory or regulatory basis to support the proposal.

3.2.01a If yes, please give details and cite the specific statues from the legislation involved.

3.2.02 If you are applying to HSC-PBPP, then someone must be processing personal and special category data, either yourself or someone else on your behalf. Therefore, you must provide the lawful bases for this data processing under current data protection legislation. To help, the most common appropriate lawful bases for health data are provided.

3.2.02a Please tick the appropriate lawful basis for processing personal data under GDPR article 6.1. The different legal bases are listed in **Table 4** of [Appendix B](#_Appendix_B__The), but the most appropriate for the use of health data are provided in the application form.

3.2.02b Please tick the appropriate lawful basis for processing special category data under GDPR article 9.2. The different legal bases are listed in **Table 5** of [Appendix B](#_Appendix_B__The), but the most appropriate for the purposes generally used for health data are given.

Under the Data Protection Act 2018, some legal bases for processing data under article 9.2 of GDPR also require a condition from Schedule 1. These are also provided in **Table 5** of [Appendix B.](#_Appendix_B__The) This also needs to be consistent with those in section 1: e.g. if the applicant is reliant on 9.2.i, then for condition 3, the work must be carried out under the responsibility of a clinician / health professional and this would be the applicant and/or clinical lead.

3.2.02c Please indicate the specific group of people who will process any personal and special category data, whether it will be you or done on your behalf.

3.2.03 Please provide any existing agreements (e.g. data processing agreements, information sharing agreements or contracts) which are in place which support your proposal. This can include any formal documented procedures or agreements which facilitate the exchange or sharing of information in ways or between parties or organisations relevant to your application. Such procedures can indicate both a basis for access, sharing or transfer of information, and also the existence of controls in place to ensure that risk is minimised where data is processed in this way. You should give details and also append any relevant supporting documentation, providing references to the relevant sections if appropriate.

3.2.04 Please indicate if you have sought regulatory approval in relation to your proposal from any organisations, within or outwith Scotland, whether received or pending. This would include e.g. approvals from such bodies such as the Confidentiality Advisory Group (CAG) of the Health Research Authority (HRA). You should provide names of organisations and / or specific roles as appropriate, and append any relevant documentation associated with these approvals.

### 3.3 Research Ethics Governance

If you declared in Q 2.4 that your project is not research and does not require a Research Sponsor, please go to Q 3.4.

For all research applications, the requirement for some form of ethical review, whether by NHS REC ethics or another ethical review body, needs to be considered. This section details the ethical opinion which you have obtained or sought for your proposal, or otherwise provides evidence as to why such approval is not appropriate. Where such approval is not in place, it is important that you demonstrate why this is the case and provide assurances if approval is pending. It is the responsibility of the applicant and the Research Sponsor to ensure that suitable ethical review has taken place. Please note that HSC-PBPP is not an ethical review body and does not give ethical opinion on any application, but wishes to ensure that this is in place, where appropriate.

If you need advice on whether NHS REC ethics approval is necessary, you should approach your local NHS ethics service in the first instance. Information about UK research ethics committees and ethical opinions can be found on the [Health Research Authority website.](http://www.hra.nhs.uk/) If NHS REC ethical review is not required, you still may require ethical review by another ethical body, such as the ethics committee in your University.

For applications that will use the National Safe Haven, they may come under the generic ethical approval obtained. The criteria for this are:

1. Data held / accessed in National Safe Haven
2. Research is in field of Health or Social care
3. There will be no contact with participants
4. Study has undergone external scientific peer review
5. Study will be carried out by UK-based research team

3.3.01 Please indicate whether you have sought NHS and / or University research and ethics approval (by selecting ‘Yes or ‘No’). If you answer ‘No’, please proceed directly to question 3.3.01b.

3.3.01a If you have answered ‘Yes’ to question 3.3.01, please provide details of the relevant research ethics committee, and status of the approval (whether approved or pending) and reference number. You should append relevant documentation in relation to the applications.

3.3.01b If you have answered ‘No’ to question 3.3.01, will your application be covered by the National Safe Haven generic ethical approval?

If you have answered ‘No’ to question 3.3.01b, please provide a full explanation of why research and ethics approval has not been sought or is not appropriate for your proposal. Where this has been indicated by relevant colleagues with research and ethics expertise, you should provide an explanation and details of the colleague or committee which has advised you. Wherever relevant supporting evidence for this decision is available, it should be appended.

### 3.4 Safe Havens

This section indicates if your proposal intends to use the services of a Scottish Government-accredited research Safe Haven. A list of recognised safe havens is included in **Table3** of [Appendix A](#_Appendix_A_–). Safe Havens provide a physical and technical environment designed to facilitate the safe processing of data; their use represents a significant control and provides additional assurance. The use of the national safe haven (see below) is normally expected where processing data from the national datasets or from PHS or NHS NSS. If you are proposing to access data exclusively through a recognised safe haven, then you will not need to complete sections 5.1 or 5.2 of the form. Please note that you may be asked to use a safe haven as a condition of your approval if the panel feel it is appropriate.

National Safe Haven: eDRIS, Public Health Scotland (PHS) and the University of Edinburgh host secure access points to the National Safe Haven at the Edinburgh BioQuarter. The National Safe Haven is a secure workspace environment where your data will be stored and can be accessed and analysed using statistical analysis software packages. Microsoft Office packages are also available for use. The National Safe Haven can also be accessed remotely by approved researchers from approved institutions.

3.4.01 Please indicate whether you intend to access data exclusively through any Scottish Government-accredited safe haven. This would be the case only where data (existing or newly created) is being accessed and processed exclusively within the confines of the safe haven environment, and would not be transferred beyond this environment, and is not being processed in any way before being placed in a safe haven.

3.4.02 If you are requesting access to data for which PHS or NHS NSS is the Data Controller, and you do not intend to do this through the National Safe Haven, please explain why. PHS or NHS NSS data are typically processed from within the National Safe Haven: if your proposal seeks to process PHS or NHS NSS data out-with this environment, you should provide a full explanation as to why this is the most appropriate way of processing the data. If you are not obtaining national data, this should be stated.

3.4.03 If you answered Yes to Q 3.4.01, please choose whether this is the National Safe Haven or a Regional Safe Haven from the drop-down menu.

If you are using the National Safe Haven, you do not need to complete sections 5.1 and 5.2 of the form.

3.4.03a If you are using a Regional Safe Haven, please specify which one.

3.4.04b If you are requesting access to national data for which PHS or NHS NSS is the Data Controller, and you do not intend to do this through the National Safe Haven, please explain why. PHS or NHS NSS data are typically processed from within the National Safe Haven: if your proposal seeks to process PHS or NHS NSS data out-with this environment, you should provide a full explanation as to why this is the most appropriate way of processing the data. If you are not obtaining national data, this should be stated.

If you are using a Regional Safe Haven, normally you do not need to complete sections 5.1 and 5.2 of the form. **However, if you require NHS Central Register (NHSCR) cancer flagging data and wish to access your data through a Regional Safe Haven, you will need to complete sections 5.1 and 5.2. This is a requirement of NHSCR.**

3.4.04 Please state how and from what location you will access the safe haven specified (e.g. remotely from on a university-provided laptop from a university office; e.g. using a safe setting from… (specify location).

3.4.05 Please indicate whether access to the NSH will be required by anyone working from home?

3.4.05a if yes, please state whether your organisation has a home working policy, and provide it as a supporting document. Please outline any mitigation measures that are in place to ensure that access to the safe haven will be secure.

# Section 4: Safe Data, Data Subjects and Methodology

### 4.1 New Data yet to be collected

This section should indicate which data sets are being newly collected for the purpose of this proposal. If no such collection of new data is proposed, please proceed to question 4.2. The emphasis here is on the *collection of new data*, as distinct from the creation of new dataset from existing data (for example by linkage or extracted from case notes) or data collected prior to the application.

For each source of new data, you should clearly identify which party (organisation or individuals referenced within the proposal) will be collecting the new data.

### 4.2 All Other Existing Datasets / sources

This section should indicate data sources or data sets that are already in existence, and are not being newly collected for the purposes of the proposal. This will include each existing local or national data set or source which your proposal seeks to access, and could include extracts from hospital systems, or research databases. It establishes that appropriate permission has been received for the data to be accessed and used in the manner proposed. Please note that contact should be established as early in the process as possible with NHS boards and data providers to discuss data provisioning requirements.

Please list each such data set or data source. Provide the name of the dataset or source, and the name of the current data controller of the data. If the data controller is not from NHSScotland, you should append documentation or details to illustrate your permission to use these data. If you will receive data indirectly (e.g. NRS Deaths from the copy held by PHS), the original data controller should be given (i.e. NRS in this example).

4.2.01 Include an explanation of how individuals who are the subject of the data were originally informed that their data would be used for your proposal specifically (e.g. participants were asked about the collection of their data from their medical records for this research), or more generally (e.g. privacy notices provided by the NHSScotland boards state that patient data may be used and shared for research). You should ensure that you include an **appropriate explanation for your participants** for each of the data sources which you have listed. If your application is focussed on participants who are particularly vulnerable, e.g. those with dementia, learning disabilities, live chaotic lives, you might need to think more about more appropriate routes for informing patients about the use of their data, than relying on generic data protection privacy notices provided by NHS Boards, or those on websites to which your participants may not have access.

Data Protection privacy notices and information to the participants need to be GDPR-compliant and transparent regarding how data will be used and by whom.

4.2.02 Please explain how the principle of data minimisation has been applied in this application. This is the principle within data protection law such that data are **sufficient, relevant and limited to what is necessary** in relation to the purposes for which they are processed (‘data minimisation’). Therefore, you can only ask for that data that you **need** to achieve your purposes. This means that you cannot ask for all available data and then work out what you require once you have it all.

This also applies to participants as well as variables. If you don’t know what data you will require to develop a larger project, a smaller pilot study might be appropriate. Under data minimisation principles, all variables should be clearly justified as to why they are necessary and required for the proposal, to indicate that these are the minimum dataset required to achieve the stated objectives of the application. Variables that are directly identifiable, or in combination with other variables could make individuals identifiable, should be particularly justified.

### 4.3 Data Variables

This section should provide a full, clear account of all the data variables included within your proposal. This can be provided as the eDRIS Project Specification Document (PSD) or in table 4.3. If you use a separate variables document, it must have the same information as that requested in the table. Please include all variables that are required, including those for ‘**processing only**’.

**Processing only** variables are those that will be used **only in processing of the data on your behalf** but will not be provided to you in the dataset for analysis. If you require such variables (e.g. CHI for data linkage, to provide a derived variable [e.g. postcode for deprivation scores, date of birth to calculate age at an event], prior to pseudonymisation or for matched control purposes), please tick the ‘processing only’ box. If your proposal will make direct use of the data (i.e. you will receive the variable in question), then the processing only box should remain unticked. Examples of your proposal making direct use of the data may include linked data extracts, IT front end of a database or results of case file audit. Please include any derived variables, for example those included in an output file.

Please list the dataset name or data source from which each variable will be obtained, and list each variable by name. Please indicate the time period over which the variable required extends. For data minimisation purposes, each variable should be justified briefly as to its necessity for your proposal.

**If you are requesting identifiable or potentially identifiable variables please ensure you justify your requirement for this level of data in each case so that the appropriateness, proportionality and risk associated with their disclosure can be carefully considered.**

### 4.4 NRS / NHSCR Data Sources

This section establishes if the proposal seeks to use data originating from National Records of Scotland (NRS), including the NHS Central Register (NHSCR), and if so, in what way. Please note that this **excludes** births, stillbirths and death registration data as a copies of these are held by PHS as part of a long standing agreement with NRS. These should be listed in Q 4.2, with NRS as the data controller.

Please note that if cancer flagging is requested, NHSCR will require an IT security review for section 5 by NRS **prior** to submission to HSC-PBPP.

**If such a review is required, and if the application is using a Regional Safe Haven, then sections 5.1 and 5.2 will have to be completed, regardless of whether Q 3.4.01 has been ticked. This is a requirement of the NHS Central Register.**

4.4.01 Please indicate if the proposal requires access to the NHS Central Registry (NHSCR) or any National Records of Scotland involvement, not mentioned in 4.2 (see note above).

**If no such data is required by the proposal, please choose ‘No’ and proceed to question 4.5.**

4.4.02 Please provide the NHSCR reference number for your project. This should also be provided on the pre-submission checklist. I**f you do not have a reference number and require NHSCR data, you will need to contact the NHSCR before submission of your HSC-PBPP form.**

Please indicate the nature of the access to the NHS Central Registry:

* the proposal requires access to the NHS Central Registry as a sampling frame for cohorts identified in the proposal.
* the proposal involves the flagging of individuals on the NHSCR for the purpose of long-term follow up.

4.4.03 If you require flagging, please select the specific purpose for which flagging of individuals against the NHSCR will be undertaken, selecting each relevant specific purpose listed. If Scottish Cancer Registrations is part of the selection these will be anonymised.

4.4.04 Please indicate if the proposal requires any further involvement of NRS, its data, infrastructure or staff, providing details where this is the case.

### 4.5 Making Contact with Individuals

This section outlines in detail any proposed contact with individuals, who are the data subjects and / or their families, those who will be approached to provide data from their patients (e.g. clinical staff, GPs) and how this will be controlled. It is considered best practice for contact with patients, patient’s relatives and families to be undertaken by clinical staff or other professionals already known to them. Proposed contact with individuals by those not already known to them should be supported by detailed evidence as to the reasons that contact in this way is appropriate.

If you wish to contact people (e.g. participants for research) via text or email, you need to ensure that your approach complies with the Privacy and Electronic Communications Regulations (PECR). The PECR sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications. These primarily apply to marketing emails, but recruitment for research could be classed as a form of marketing. For further information please see the link on the ICO’s website: <https://ico.org.uk/for-organisations/guide-to-pecr/> and / or contact your local Information Governance advisor / Data Protection Officer.

4.5.01 Please indicate if any direct contact with any group of individuals is proposed.

**If you answer ‘No’ to this question, please proceed to section 4.6.**

4.5.01a If you answer ‘Yes’ to this question, please use the section below to indicate which group will be contacted, what method of contact will be used, and who will make contact. Please include these details in respect of each group to be contacted.

4.5.02 Please provide an explanation of why contact is necessary within the context of the proposal methodology. You should attach as supporting evidence any relevant documentation detailing the methodology proposed for making contact, and in particular contact forms, information leaflets, letters or other communications being used when making contact with individuals.

### 4.6 Community Health Index (CHI) Database

This section details any proposed use of the information held within the Community Health Index (CHI) database. This includes the use of details such as current and previous address, current GP Practice, where accessed via the CHI database. This does not include the use of CHI numbers for data linkage, data matching or obtaining matched controls.

4.6.01 Please indicate whether you require access to the CHI database.

**If you answered No, please proceed directly to section 5.**

4.6.02 If you answered ‘Yes’ in 4.6.01, please provide details of how the use of the CHI number will be monitored and audited. This would include any controls which specifically govern access to, and use of, CHI data, outlined in the proposal. Examples might include additional controls around how and when CHI data is to be accessed, or regular checks on access to CHI data throughout the proposal.

4.6.03 Please provide details of the technical method which will be used to access the CHI number. You should explain how any extract or access to CHI will be facilitated technically such as electronic direct feed or provision of data from the CHI database by NHS NSS or NHSCR. Please make reference to anonymisation or other controls which will be used to minimise risks of re-identification associated with the use of the CHI number.

4.6.04 Please provide any further details regarding risks which have been identified as arising specifically from the use of the CHI number; these may have been identified in a DPIA or other information risk assessment, or have arisen from the proposal methodology.

# Section 5: Safe Data Processing and Security

### 5.1 Access

This section details in what way the proposal aims to provide access to data, and controls in place to minimise risks associated with this.

**If you have answered ‘Yes’ to Q 3.4.01**, **then you do not need to complete this section or section 5.2, and should proceed directly to section 5.3.**

**Should your application require NHSCR flagging, even if you intend to use a regional Safe Haven you will need to fill in sections 5.1 and 5.2 and NHSCR require your application to undergo an IT security review by NRS prior to submission to HSC-PBPP.**

This section requires specific details of the relevant policies and procedures in place to govern access to data as outlined in the proposal. General and repeated references to a whole policy (unless of a sufficiently narrow scope) should be avoided. This section requires to be repeated (on separate sheets if necessary) for each of the environments where data is to be accessed. Where the answers to each of the questions asked is identical for more than one environment (for example a network of physical or technical environments governed by the same policies and procedures and with identical controls in operation), then it is sufficient to state this at question 5.1.01.

5.1.01 Please provide details of the organisation and environment in which you seek to **access** data. If these details have been provided in previous sections, then you can provide a reference to the relevant section and question above. You may list multiple environments (for example a network of physical or technical environments) provided that these are governed by the same policies and procedures and with identical controls in operation. If you propose to use multiple environments not governed by the same policies and procedures, nor with identical controls in operation (e.g. NHS and University), then please complete the whole of section 5.2 for each environment.

5.1.02 Please provide details of the relevant security policy and procedures governing the proposed access to data within the physical and technical environment listed in question 5.1.01. These policy and procedures may reference any information security policies, and may exist within its own right, as part of a wider set of policies and procedures, or in more than one policy or procedure. Please make specific reference to the part, section, point or paragraph of the relevant supporting documents which act as evidence in response to the question.

5.1.03 Please confirm and provide details of the relevant policy and procedures that account for the implementation of robust password policy as a control to access of data. Please make specific reference to the part, section, point or paragraph of the relevant supporting documents which act as evidence in response to the question.

5.1.04 Please provide information on the processes for providing and removing access to the data to users and management of user accounts, including the removal of access to sensitive personal data. This question is to try to understand how the principle of least privilege (PoLP) is applied in this system, whereby users can only access the information and resources that are necessary to them. Please make specific reference to the part, section, point or paragraph of the relevant supporting documents which act as evidence in response to the question.

5.1.05 Please confirm whether access controls are associated with individual users accessing data, or whether shared user accounts or other access mechanisms are in use, and the controls in place to govern and manage the use of these. Please provide details of account management, including any specific reference to the part, section, point or paragraph of any relevant supporting documents which act as evidence in response to the question.

5.1.06 Please indicate whether access to data will be done by people working off-site and remotely from the data (Yes / No)

5.1.06a **If ‘No’ then go directly to question 5.1.07.**

If Yes, please clarify what device will be used to access the data externally and whether this is a personal device provided by the user, or provided by the organisation. If a personal device, please explain how this would comply with organisation IT security policies.

5.1.06b This question is to determine where the data will be held for remote working, whether it will remain in the host environment or whether it will be taken off-site too.

If the data remain on-site, the remote access technology in place to give the person access to the data must be outlined here. Please provide any supporting evidence that will give details of policies and procedures of how these data will be accessed securely.

If the data are taken off-site, the measures that are in place to maintain the security of the data (e.g. device encryption or data encryption) must be outlined here. What would happen if the device was lost? Or the data accidently deleted?

5.1.07 This question is for the use of any moveable device for any part of the application. At any point in the proposal, will moveable devices be used? This could include using iPads for patients to answer questions or provide specific in a clinic, the collection of patient information, e.g. during an interview, on a USB stick or laptop or separate recording device which would then be combined with a bigger database elsewhere. (Yes / No).

5.1.07a **If No, please go directly to Q 5.1.08.**

If yes, please provide details of any mobile device management solution that is in place to manage such devices, including whether the device can be remotely wiped clean of any data, in the event of any device being lost or stolen. Please provide details of the relevant policy or procedure in place to facilitate and monitor such device. Please provide any specific reference to the part, section, point or paragraph of any relevant supporting documents which act as evidence in response to the question.

5.1.08 Does your organisation have a clear desk and / or clear screen policy? This is to understand whether, at the end of a day, all papers that might contain any personal data will be cleared away, and whether, during the day, any screen is locked so that anything on screen cannot be accidently seen when it is unattended, even for a short space of time.

5.1.09 Please provide any further additional detail which provides assurances regarding the control of access to data which is proposed.

### 5.2 Storage & Use

This section details how the proposal aims to store and use data, and the controls in place to minimise risks associated with this storage and use.

**If you have answered ‘Yes’ to question 3.4.01** above (that your proposal seeks to store and use data exclusively through a recognised safe haven), t**hen you do not need to complete this section or section, and should proceed directly to section 5.3.**

The section requires specific details of relevant policies and procedures which are in place to govern storage and use of data as outlined in the proposal. General and repeated references to a whole policy (unless of a sufficiently narrow scope) should be avoided. This section requires to be repeated for each of the environments where data is to be stored or used. Where the answers to each of the questions asked is identical for more than one environment (for example a network of physical or technical environments governed by the same policies and procedures and with identical controls in operation), then it is sufficient to state this at question 5.2.01**.**

5.2.01 Please provide details of the organisation and environment in which the proposal seeks to store and use data. If these details have been provided in previous sections, you can reference the relevant section and question. You may list multiple environments (for example a network of physical or technical environments) provided that these are governed by the same policies and procedures and with identical controls in operation. If you propose to use multiple environments not governed by the same policies and procedures and with identical controls in operation, then you should complete the whole of section 5.2 for each environment.

5.2.01a If the data will be stored in a computing cloud please give information about who will host or provide that cloud storage and in what country the server is physically situated. If this the USA or somewhere outside the EEA, there may be further security information required as, under Data Protection Act UK 2018 / GDPR, personal data should not be sent outside the EEA,

Please also provide IT security i8nforamtion that covers such cloud storage and what access the provider will have to the data stored therein.

5.2.02 Please indicate to what cybersecurity standards your organisation works. This could be ISO 27001, or Cyber Essentials or some other recognised industry standard that needs to be outlined here. Please give details and attach any evidence of approval and duration of that approval.

5.2.03 Please provide details of the relevant policy or procedures governing the proposed storage and use of data within the physical and technical environment listed in question 5.2.01. This will make reference to information security, and may exist within its own right, as part of a wider policy or procedure, or in more than one policy or procedure. Please reference the specific part, section, point or paragraph of the supporting documents provided as evidence for this question.

5.2.04 Please outline the policy and procedures in place to cover the implementation of up-to-date controls for the detection and prevention of malware within the environment in which data will be stored. Please make specific reference to the part, section, point or paragraph of the relevant supporting documents provided as evidence for this question.

5.2.05 Please outline the policy and procedures in place to cover access control and auditing of users and / or system administrator activity within this environment. Please reference the specific part, section, point or paragraph of the supporting documents provided as evidence for this question.

5.2.06 Please outline the policy and procedures in place for the production and control of backup copies of the data, within the storage environment. Please reference the specific part, section, point or paragraph of the relevant supporting documents provided as evidence for this question.

5.2.07 Please outline the policy and procedures in place to ensure business continuity, contingency planning and system restoration in the event of a critical system failure. Please reference the specific part, section, point or paragraph of the relevant supporting documents provided as evidence for this question.

5.2.08 Please outline the policy and procedures in place to prohibit unauthorised copying of data within the storage environment. Please reference the specific part, section, point or paragraph of the relevant supporting documents provided as evidence for this question.

5.2.09 Please outline the policy and procedures in place to describe the physical and site controls of the storage environment. Please reference the specific part, section, point or paragraph of the relevant supporting documents provided as evidence for this question.

5.2.10 Please outline the policy and procedures in place that cover hardware repair, replacement or disposal, and the protection of data from inappropriate access during such processes. Please reference the specific part, section, point or paragraph of the relevant supporting documents provided as evidence for this question.

5.2.11 Please describe the systems, software and security used to store and use data. This is your opportunity to provide a clear picture of how data is being stored and used, over and above the specific questions identified above. Some examples of what information is required:

Is the host environment infrastructure actively vulnerability scanned and penetration tested? If so, is there a policy that covers this?

Is the data suitably encrypted, where possible?

Does the policy describe the organisations patch management policy? Are security updates installed within a suitable timeframe? This is applicable to both server environment hosting the data, as well as the device used to access the data.

Your answer should be proportionate to the complexity of the storage and use of data proposed: where this is straightforward, this question will require less detail, with more detail necessary where more complex storage and use is proposed. Please reference the specific part, section, point or paragraph of the relevant supporting documents provided as evidence for this question.

5.2.12 Please confirm whether the use of outsourced IT is proposed. The definition of outsourced IT should be considered to be very wide in scope, and could include any use of IT infrastructure or systems which are beyond the control of the organisation listed in section 2.1, and the originators of the data. You should mention by name organisations or bodies such as safe havens, third party suppliers or arms-length organisations processing data on your behalf.

### 5.3 Transfer

This section details with the procedures and controls in place for the transfer of data for this proposal. Transfer can include from person to person, system to system, between organisations or across divisions within the same organisation. It includes the movement, for example, of data from one storage media to another, whether for subsequent use, storage, or temporarily for transit. The section requires specific details of relevant policies and procedures in place for the proposed transfer of data. General and repeated references to a whole policy (unless of a sufficiently narrow scope) should be avoided.

5.3.01 Please provide details of the security policy or procedures governing the proposed transfer of data, such that it is protected from inappropriate or unauthorised access. Your answer should reflect the flow diagram for Q 3.1.11 and describe the transfer processes from the patient to its final destination including any intermediary stages. This may include controls as email encryption, secure file transfer protocols, device encryption, or physical controls. Please reference the specific part, section, point or paragraph of the relevant supporting documents provided as evidence in response to the questions.

5.3.02 Please describe any proposed time-intervals or triggers which will initiate the transfer of data.

5.3.03 Please indicate whether any personal (identifiable, pseudonymised or potentially identifiable) data will be transferred to or shared with any organisation within or beyond the UK (Yes/ No).

5.3.03a **If ‘No’, go directly to question 5.3.04.**

If ‘Yes’, please specify the organisation and country of destination to which you propose to transfer any personal data and provide details of the method of transfer, the proposed location and method of storage, and details of how the data will be handled and kept secure.

5.3.04 Please provide details of any required copying of data, other than that for initial transfers from source systems, and indicate why this is necessary, the method of copying, and the extent to which copied data will proliferate (multiple copies, dissemination etc.). Such processing should be detailed and justified in your answers to question 3.1.09.

# Section 6: Safe Outputs and Review

**6.1 Outputs and Dissemination**

This section details with the outputs from your analysis, how you propose to report your results and outcomes, and the controls in place to minimise any associated risks. Reporting and publication includes any dissemination or disclosure of any of the data and outputs from the proposal, to any person not already specifically identified in earlier questions, or who is not themselves one of the data subjects. This includes the dissemination or disclosure of any of the data sources or datasets, parts or components thereof detailed in the proposal, and of any results or outcomes, detailed, summarised, anonymised or otherwise, resulting from proposed processing of data. Dissemination or disclosure can take place in a variety of ways and through many mechanisms, including through electronic media, print media, or by word of mouth.

6.1.01 Please outline the procedure that will be used for disclosure control for the outcomes of the proposal. This is to ensure that tables and information from the findings does not include outputs from which any person could potentially be identified. Please pay particular attention to small groups, which should not consist of numbers less than 5. If you have groups containing <5 people, these should be combined so that the outputs contain groups >5.

6.1.02 Please indicate whether any of the outputs from the data will be published beyond those listed in section 1. Please note, if there is no dissemination this might raise some questions as to the public benefit of the proposal.

If ‘No’, please go to section 6.2

6.1.03 Please indicate how the results and outcomes from the proposal will be published or disseminated to stakeholders and interested parties, including patients and the general public.

**As the public do not read scientific literature or attend conferences, you will need to consider how the results or outcomes will be disseminated to the wider public and how this fits with the public benefits of the proposal, as outlined in Q 3.1.08.**

Outputs to the public could include: press releases, social media, progress reports on websites that the public might access, feedback to patient groups. The public are interested in the outcomes of research. If the public or patient groups have had some input into the proposal in some way, or the work focuses on a particular patient group whose data has been used, it is only polite that they are informed about the outcomes of the work.

6.1.04 Please describe the steps you will take to ensure the confidentiality of the data when disseminating or publishing your outcomes. This may include the application of disclosure control procedures, aggregation of data or other approaches.

6.1.05 Please detail any circumstances where a living or dead individual may be cited in the dissemination of outputs from your proposal.

6.1.06 Please confirm if you have sought any permission from data controller or other bodies to publish any findings or outputs. If you have then please provide details of who has and what they have given permission to publish and append any approval correspondence.

### 6.2 Retention and Disposal of data

This section details how the proposal will treat data being processed after it has been used for the purpose of the proposal outlined, including governance in place to determine how long it will be retained, and controls to manage its subsequent disposal. This section should show that you have considered these aspects of processing, and you will commit to appropriate retention and disposal of data. A comprehensive records management and / or retention policy will cover each of the aspects explored in this section; please reference the specific part, section, point or paragraph of the relevant supporting documents, provided as evidence in response to the questions.

Under data protection law, potentially identifiable or pseudonymised data should be retained for only a limited time. Once it is no longer needed, it should be fully anonymised or securely destroyed. This is known as the principle of storage limitation.

6.2.01 Please outline the policy and procedures in place governing the retention of information, data and / or records relating to this proposal.

6.2.02 Please state for how long you intend to retain or archive the identifiable, pseudonymised or potentially identifiable individual-level data in your proposal, including the time-period as an archive or back up copy. This is after all active processing has finished.

6.2.03 Please provide details of which organisation and where the data will be held for the specified retention period. If this is in different locations provide details for all.

6.2.04 Please provide reason(s) as to why the data should be held for this length of time relevant to your organisation. Provide evidence of any stipulations by appending documents or providing the URL to the relevant document.

6.2.05 Please provide details of how the data and output files will be disposed of at the end of the period specified above. You may refer to any relevant disposal or destruction policies used by your organisation. Please reference the relevant section from the policy or include a URL and indicate which section is relevant.

6.2.06 Please confirm what evidence will be obtained following that destruction, if appropriate. This may include certificates of IT hardware destruction or completion of a data destruction certificate.

### 6.3 Review

This section describes how the policies and procedures, and the controls described within them, described in sections 5.1-5.3 will be operated effectively over time, during both routine and adverse events.

6.3.01 Please provide details on the checks to monitor and audit the mechanisms for the safe guarding of the data. You can reference the relevant parts of policies and procedures listed in sections 5.1-5.3 and 6.1-6.2 above (e.g. dates of policy review or review intervals, statements about accountability for compliance, or details of regular testing and audit of systems or environments).

6.3.02 Please provide details of any aspect of the provision of physical or technical security of data, described in your answers to sections 5.1-5.3, where the resource implications of provision remain unresolved. This might include such examples as encryption of devices which you intend to have in place, but which is not yet fulfilled, IT training which you intend to complete but which is not yet undertaken, secure email accounts you propose to use which have not yet been created, etc. You should provide assurances as to how you intend to resolve these issues.

6.3.03 Please provide details of how you will report any breaches if inappropriate access to the data occurs. Details can be summarised from any security documents that may be relevant. Please ensure that this includes details of how you will notify the data controllers.

# Section 7: Declarations

Please read this section carefully. It requires to be read and understood by both the Applicant identified at section 1.1, the academic supervisor, if applicable and at section 1.2, the Information Custodian identified at section 1.4, the main contact for the organisation at section 2.2 and the Research Sponsor, if applicable at section 2.4.

For the Applicant: You should provide your full name and date the declaration. By doing so you are signifying that you commit to the declarations, undertakings and understandings contained within the declaration.

For the Academic supervisor: You should provide your full name and date the declaration. By doing so you are signifying that you commit to the declarations, undertakings and understandings contained within the declaration.

For the Information Custodian (where this is not the same person as the applicant or Academic Supervisor): You should provide your full name and date the declaration. By doing so you are signifying that you commit to the declarations, undertakings and understandings contained within the declaration.

For the Main Contact for the Organisation: You should provide your full name and date the declaration. By doing so you are signifying that you commit to the declarations, undertakings and understandings contained within the declaration on behalf of the lead organisation.

For the Research Sponsor: You should provide your full name and date the declaration. By doing so you are signifying that you commit to the declarations, undertakings and understandings contained within the declaration on behalf of the lead organisation.

# Contacts

You should contact your eDRIS application coordinator in the first instance with any questions or queries relating to any aspect of your proposal, or your application form ([phs.edris@phs.scot](mailto:phs.edris@phs.scot)

Full information about the HSC-PBPP (for applicants, members of the public, and participants in the panel process) is available from the [HSC-PBPP website](http://www.informationgovernance.scot.nhs.uk/pbpphsc).

# Appendix A: Reference lists for applicants

|  |  |
| --- | --- |
| **Table 1. Examples of Existing Datasets and Data Sources** | |
| [SMR 00 Outpatients](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=1) | [SMR 04 Mental Health](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=4) |
| [SMR 01 Inpatients and Day Cases](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=2) | [SMR 06 Cancer Registration](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?ID=5&SubID=104) |
| [SMR 02 Maternity](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=3) | [SMR 11/SBR Neonatal/Scottish Birth Records](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?ID=1&SubID=6) |
| [Scottish Drugs Misuse Database (SDMD)](http://www.isdscotland.org/Health-Topics/Drugs-and-Alcohol-Misuse/Drugs-Misuse/Scottish-Drug-Misuse-Database/) | [Birth Registrations](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=14) |
| [A&E: Accident & Emergency](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=10) | [Stillbirth Registrations](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=14) |
| [PIS Prescribing Information](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=11) | [Death Registrations](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=14) |
| [CHSP-PS](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=28) / [CHSP-S](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=29) / [SIRS](http://www.ndc.scot.nhs.uk/National-Datasets/data.asp?SubID=87): Child Health Surveillance and Immunisation | [SCI-DC](http://www.sci-diabetes.scot.nhs.uk/) |
| Public Health Scotland (PHS) maintains a [National Dataset Catalogue (NDC)](http://www.ndc.scot.nhs.uk/National-Datasets/index.asp) containing details of all health and health related datasets that are held by PHS. | |

|  |  |  |
| --- | --- | --- |
| **Table 2. Common Identifiable Variables** | | |
| Forename | Middle Name | Surname |
| CHI Number | Date of Birth | UK NHS Birth Registration Number |
| Gender | Postcode | Full dates of admission / discharge |

|  |
| --- |
| **Table 3. Recognised Safe Havens** |
| [National Safe Haven](http://www.isdscotland.org/Products-and-Services/eDRIS/Use-of-the-National-Safe-Haven/) (run by eDRIS) |
| [NHS Research Scotland South East (ACCORD)](http://www.accord.ed.ac.uk/) |
| [NHS Research Scotland North (DaSH)](http://www.abdn.ac.uk/iahs/facilities/grampian-data-safe-haven.php) |
| [NHS Research Scotland West](http://www.nhsresearchscotland.org.uk/214_West+.html) / [Robertson Centre @ Glasgow University](http://www.gla.ac.uk/researchinstitutes/healthwellbeing/research/robertsoncentreforbiostatistics/) |
| [NHS Research Scotland East (TASC/University of Dundee Health Informatics Centre)](https://www.dundee.ac.uk/hic/) |
| [National Records Scotland Scottish Longitudinal Study (SLS)](http://sls.lscs.ac.uk/) at Ladywell House |

|  |
| --- |
| **Table 4. Approved Information Governance Training** |
| MRC   * ‘[Research, GDPR and Confidentiality – what you really need to know’ online module](http://www.byglearning.co.uk/mrcrsc-lms/course/category.php?id=1)   A series of 10 bite-sized e-learning modules accompanied by supplementary resources and a quiz.  We ask that applicants go through all the modules and pass the quiz. Each module has a dotted box next to it. As each module is completed, a tick will appear automatically when the module has been completed. Please print out a screen shot of the ticked boxes showing that each module has been completed and send it to the Research Coordinator, together with the certificate showing that you have passed the quiz. |
| NHSScotland Information Governance eLearning:   * Information Governance in Action   (This would be accessed via your NHS organisational training, e.g. LearnPro   * **AND a higher level IG training is required (MRC course recommended).** |
| Scottish Government   * Data Protection e-Learning |
| Office for National Statistics (ONS)   * Safe Researcher Training   Please note that while the provider states that this training is valid for 5 years, the HSC-PBPP still requires IG training to be updated every three years. Therefore, other IG training (e.g. MRC course) will be required to cover the other two years. |
| **Approved Information Governance Training: courses no longer accessible** |
| University of Edinburgh SHIP Information Governance Training |
| NHS Health and Social Care Information Centre Online Information Governance Training |
| ADLS Safe Researcher training |
| Administrative Data Research Network (ADRN) SURE Training |

HSC\_PBPP requests the IG training is updated every **three** years. All those with access to data **must** have valid IG training throughout the whole of the time for which approval is given and data is accessed. If your IG training will expire before your HSC-PBPP approval expires, your training **must** be renewed.

|  |  |  |
| --- | --- | --- |
| **Table 5. Vulnerable Populations** | | |
| Adults with Incapacity | Mentally ill | Elderly |
| Children | Drugs / alcohol users | Children in care |
| Minority ethnic groups | Asylum seekers | Specific religious affiliation |

|  |  |  |
| --- | --- | --- |
| **Table 6. Special Category Data under Data Protection Act with GDPR (UK) 2018** | | |
| Race / Ethnicity | Physical and Mental health | Sexual orientation and sex life |
| Religion | Politics | Crime-related statistics |
| Trade Union Membership | Genetics | Biometrics |
| **Sensitive Data Categories for Health data** | | |
| Sexually transmitted diseases | Mental health | Pregnancy in age <16 years |
| Drugs and alcohol misuse | Suicide |  |

# Appendix B: The Caldicott Principles, Data Protection Principles and Law

|  |
| --- |
| **Table 1. Caldicott Principles** |
| 1. **Justify the purpose(s)**   Every single proposed use or transfer of patient identifiable information within or from an organization should be clearly defined and scrutinized, with continuing uses regularly reviewed, by an appropriate guardian. |
| 1. **Don't use patient identifiable information unless it is necessary**   Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s). |
| 1. **Use the minimum necessary patient-identifiable information**   Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out. |
| 1. **Access to patient identifiable information should be on a strict need-to-know basis**   Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes. |
| 1. **Everyone with access to patient identifiable information should be aware of their responsibilities**   Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality. |
| 1. **Understand and comply with the law**   Every use of patient identifiable information must be lawful. Someone in each organization handling patient information should be responsible for ensuring that the organization complies with legal requirements. |
| 1. **The duty to share information can be as important as the duty to protect patient confidentiality**   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies. |

|  |
| --- |
| **Table 2. Data Protection Principles** |
| **Personal data must be:** |
| 1. processed lawfully, fairly and in a transparent manner in relation to individuals **(lawfulness, fairness and transparency)**. |
| 1. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes **(purpose limitation)**. |
| 1. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **(data minimisation)**. |
| 1. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **(accuracy)**. |
| 1. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subjects **(storage limitation)**. |
| 1. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **(integrity and confidentiality)**. |
| The data controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 **(‘accountability principle’)**. |

|  |  |
| --- | --- |
| **Table 3: Data Protection law: Rights of the data subjects** | |
| Right to be informed | Right to Data portability |
| Right of access | Right to rectification |
| Right to erasure | Right to Object |
| Right to restrict processing | Rights related to automatic processing |

|  |
| --- |
| **Table 4: Data Protection law: Lawful basis for processing personal data (GDPR article 6.1)** |
| 1. **Consent:** the individual has given consent to the processing of his or her personal data for one or more specific purposes.   *For this to be lawful, the rights of the subject, including the right to erasure must be upheld.*  ***Please see guidance notes for Q 3.2 on consent under GDPR.*** |
| 1. **Contract:** the processing is necessary for the performance of a contract to which the data subject is party or in order take steps at the request of the data subject prior to entering into a contract. |
| 1. **Legal obligation:** processing is necessary for compliance with a legal obligation to which the data controller is subject.   ***This would be used in the case where the organisation has to process personal data to comply with other legislation. Please cite the specific legislation involved.*** |
| 1. **Vital interests:** the processing is necessary to protect the vital interests of the data subject.   ***This can only be used for the patient in front of you.*** |
| 1. **Public task:** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.   *This is the most common legal basis used by public organisations* |
| 1. **Legitimate interests:** the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child,   **NB: This shall not apply to processing carried out by public authorities in the performance of their tasks.** |

|  |  |  |
| --- | --- | --- |
| **Table 5: Data Protection law: Legal bases for processing special category data (Article 9.2)**  For some of these bases and an additional condition from DPA 2018 Schedule 1 Part 1 is required.  **Please see link:** [**https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/**](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/) | | |
| **GDPR article 9.2 legal basis** | **DPA Schedule 1 condition required** | **Conditions to be met** |
| 1. **Explicit consent**   The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.  *For this to be lawful, the rights of the subject, including the right to erasure must be upheld.* ***Please see guidance notes on consent under GDPR for Q 3.2.*** | No | None |
| 1. **Employment, social security and social protection**   Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the **field of employment and social security and social protection law** in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.  *This does not usually apply to the secondary use of health data.* | Condition 1 | This condition is met if—   1. the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject **in connection with employment, social security or social protection,** and 2. when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule). |
| 1. **Vital Interests**   Processing is necessary to protect the **vital interests of the data subject** or of another natural person where the data subject is physically or legally incapable of giving consent.  *Vital interests are intended to cover only interests that are essential for someone’s life. so this condition is very limited in its scope, and generally only applies to matters of life and death.*  *This condition only applies if the individual is physically or legally incapable of giving consent. This means you should ask for explicit consent if possible. If a data subject refuses consent, you cannot rely on vital interests as a fallback condition, unless they are not legally competent to make that decision.*  *This condition is likely to be most relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is unconscious or otherwise incapable of giving consent.* | No | None |
| 1. **Not-for-profit bodies**   Processing is carried out in the course of its legitimate activities with appropriate safeguards by **a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim** and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.  *Does not usually apply to the use of health data.* | No | None |
| 1. **Manifestly made public**   Processing relates to personal data which are manifestly made public by the data subject.  *Does not usually apply to the use of health data.* | No | None |
| 1. **Legal claims**   Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.  *Does not usually apply to the use of health data.* | No | None |
| 1. **Substantial Public interest with basis in law**   Processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.  *For substantial public interest to apply it must be related to one of the conditions 6-28.* | Schedule 1  One of conditions 6 – 28. | 1. Statutory and government purposes (laws) 2. Administration of justice and parliamentary purposes 3. Equality of opportunity or treatment 4. Racial and ethnic diversity at senior levels 5. Preventing or detecting unlawful acts 6. Protecting the public against dishonesty 7. Regulatory requirements 8. Journalism, academia, art and literature 9. Preventing fraud 10. Suspicion of terrorist financing or money laundering 11. Support for individuals with a particular disability or medical condition 12. Counselling 13. Safeguarding of children and individuals at risk 14. Safeguarding of economic well-being of certain individuals 15. Insurance 16. Occupational pensions 17. Political parties 18. Elected representatives responding to requests 19. Disclosure to elected representatives 20. Informing elected representatives about prisoners 21. Publication of legal judgments 22. Anti-doping in sport 23. Standards of behaviour in sport |
| 1. **Health or social care**   Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.  *This is commonly used for the provision of health care or its management.* | Condition 2 | This condition is met if the **processing is necessary for health or social care purposes**.  In this paragraph “health or social care purposes” means the purposes of:   1. preventive or occupational medicine, 2. the assessment of the working capacity of an employee, 3. medical diagnosis, 4. the provision of health care or treatment, 5. the provision of social care, or 6. the management of health care systems or services or social care systems or services.   See also the conditions and safeguards in Article 9(3) of the GDPR (obligations of secrecy) and section 11(1). |
| 1. **Public Health**   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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.  *This is commonly used for the use of data for public health or medicinal products.* | Condition 3 | This condition is met if the processing:   1. is necessary for reasons of public interest in the area of public health, and 2. is carried out:    1. by or under the responsibility of a health professional, or    2. by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law. |
| 1. **Archiving, historical or scientific research or statistics (with basis in law)**   Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.  *This is commonly used for research, archive or use of data for statistical purposes.* | Condition 4 | This condition is met if the processing:   1. is necessary for archiving purposes, scientific or historical research purposes or statistical purposes, 2. is carried out in accordance with Article 89(1) of the GDPR (as supplemented by section 19), and 3. is in the public interest. |