Public Health England

Protecting and improving the nation's health

ODR Approval Guidelines: completing the ODR data request form (Annex A)

The ODR data request form v5 is presented in Adobe and uses conditional logic to help you understand what information to submit in support of your application for ODR Approval. If you do not have an Adobe Reader, you can download it for free.

These guidelines should be read in conjunction with the ODR Approval Guidelines: applying for PHE data and its associated annexes.

Contents

Section A: Chief investigator, organisation information and primary point of contact

A1: Chief investigator (primary applicant information)

Provide details of the individual who is leading on the proposed project and has overall responsibility for the intellectual, administrative, and ethical aspects of a project (including day-to-day management and dissemination of results).

This individual will typically be the main point of contact for the ODR and will be named in the ODR data sharing contract. The chief investigator should hold a contract of employment or honorary contract at the organisation named in A2.1.

Where an application is made for education purposes, such as for the completion of a master's thesis, it is advised that the student's supervisor is named as a chief investigator and the student is named in A3.1.

All formal correspondence, including outcome letters and contracts will be addressed to the chief investigator.

A1.1	Title	Select from the drop down the title prefixing a chief investigator's name.
A1.2	First name	Provide the chief investigator's first name.
A1.3	Surname	Provide the chief investigator's surname.
A1.4	Role/job title	Provide the chief investigator's role or job title.
A1.5	Email address	Provide a corporate email address for the chief investigator.
A1.6	Work telephone/mobile	Provide a direct contact number for the chief investigator. Where applicable, include the extension code.

A2: Chief investigator's organisation

Provide details of the requesting organisation.

A2.1	Organisation name	Provide the organisation name. This must be the name of the legal entity which employs the chief investigator.

A2.2	Organisation department	Provide the chief investigator's department name.
A2.3	Registered address	Provide the official address of the organisation named in A2.1. This address may differ from the business address of the chief investigator, which would typically be used for correspondence.
A2.4	Organisation type	Select from the drop down the organisation type which best describes the organisation named in A2.1. The options provided are: • Academic institution • Commercial – it is recommended that this category should be selected by industry and commercial research organisations • CQC registered health and/or social care provider – it is recommended that this category should be selected by NHS organisations that deliver care to patients (such as NHS Trusts or GP practices) • CQC approved national contractor • Local Authority • Government agency (health and social care) • Government agency outside of health and social care • Independent sector – it is recommended that this category should be selected by charitable organisations and the royal colleges • Other Should these options not be descriptive of the organisation type, select 'other' and provide an alternative description.

A3: Point of contact for day-to-day correspondence about your application

Where the main point of contact for the application is not the chief investigator, provide the full name and contact details of the person designated to serve as the primary contact for the ODR to liaise with.

A3.1	Primary contact name	Provide the full name of the primary contact for the application.
A3.2	Primary contact email address	Provide a corporate email address for the primary point of contact named in A3.1.

Section B: Project sponsor

All research carried out within the NHS or social care, involving NHS patients, their tissue or data requires a research sponsor in accordance with the UK Policy Framework for Health and Social Care Research (2017).

The sponsor is the individual, company, institution or organisation that takes on legal responsibility for the initiation, management and/or financing of the research. On this basis, any contract issued by the ODR to support data sharing will be executed with the sponsor.

To learn more about the responsibilities placed on sponsors, refer to the Health Research Authority 'Roles and Responsibilities'.

B1.1	If the project's sponsor is the same as the organisation named in section A2.1, indicate this using the 'tick' function.	
B1.2	Sponsor's name	Provide the organisation name of the research sponsor. Due to the collaborative nature of research, it may be appropriate for sponsorship responsibilities to be managed in partnership with another, or a small number of other organisation(s). This arrangement is called co-sponsorship. If your project involves co-sponsorship, it is important to clearly document the organisation(s), their roles and responsibilities in (1) the scientific protocol (see **ODR Approval Guidelines: scientific protocol (Annex B)** for further information) and (2) Section K of this form.

		It is also strongly recommended that you seek advice from your information governance team, Data Protection Officer or legal counsel about the implications of co-sponsorship on your responsibilities and liabilities as a data controller. You can also seek advice from the ODR Pre-application Support Service (PaSS) about how co-sponsorship will affect: • the scope of your application • the mandatory and qualified evidence requirements for a valid application • the service charges associated with the request; and • the standard conditions of ODR approval (including the data sharing contract).
B1.3	Sponsor's address	Provide the business address of the sponsor.

Section C: Funding arrangements

The administrative, operational and technical services directly attributed to your project will be charged by the ODR at full economic cost. All fixed and variable charges are described in the **ODR Approval Guidelines: cost recovery.** The ODR reserves the right to, from time-to-time, update its service rate and specific charges.

Charges will be waived in a limited number of scenarios and advice should be sought to understand the scale of costs associated with your project prior to submission to ensure adequate funding arrangements are in place. It is strongly advised to not submit your application for ODR Approval if adequate funding is not immediately available.

Where funding has been secured from outside the applicant's organisation, indicate the name and address details of the organisation(s) providing funding. This information will be published in the Data Release Register should your application be successful.

Should your application be successful, the ODR will invoice the organisation named in section A2.1. Invoices will be sent following all conditions of approval being met (including contract execution and a purchase order being shared with ODR). Payment of all service charges must be made within 30 days of the invoice date,

unless an alternative deadline is explicitly expressed in the contract (ie in circumstances where there is a staggered payment schedule).

If your organisation has not sought access to data through ODR before, you are advised to contact the ODR to your organisation holds a customer credit account with PHE; if not, this will need to be set up. It is recommended that this process is commenced during pre-application to avoid delays.

Advice on the indicative costs of your project and suggestions about the tolerances you should build into a grant proposal can be obtained through the ODR Pre-application Support Service (PaSS). Actual costs will be confirmed at the end of the application process in the ODR conditional approval letter and formally agreed before work commences.

C1.1	If the project's funder is the same as the organisation named in section A2.1, indicate this using the 'tick' function.	
C1.2	Name of awarding institution	Provide the name of any organisations or persons who have financially supported this project.
C1.3	Address of awarding institution	Provide the business address of any organisations or persons named in C1.1.
C1.4	Reference(s) assigned by the awarding institution	List all references assigned by the organisations or person providing financial support as named above. If you have multiple references, separate them with a comma.

Section D: Project summary

The project summary provides the ODR with an overview of the project, as well as the broader anticipated impact(s) and beneficiaries of the project. The summary must:

- describe a medical purpose;
- provide a high-level and consistent overview of the accompanying scientific protocol;
- ensure this description aligns with the dataset(s) requested;
- present and justify the need to access PHE data; and
- be written in non-technical language (reading age 13-14 years) and in line with the editorial requirements outlined in the **ODR Approval Guidelines: lay summary (Annex E)**.

In addition to completing Section D, you must share with the ODR a scientific protocol which clearly states the purpose(s) for the processing of the data and is descriptive of the type and scale of data necessary to fulfil the purpose(s). This includes a detailed analytical and data management plan. See **ODR Approval Guidelines: scientific protocol (Annex B)** for recommendations on the minimum set of scientific, ethical, and administrative elements that should be addressed in the protocol.

Together, the summary and scientific protocol enable the ODR to determine:

- the data requested will only be processed for a specific, explicit and legitimate medical purpose(s);
- the processing will be lawful, fair and transparent;
- the scope of the mandatory and qualified application requirements you submit to the ODR are both suitable and consistent with **ODR Approval Guidelines: application requirements**;
- the data requested is the absolute minimum needed for the purpose(s) and will be accessed on a need-to-know basis; and
- the appropriate term for processing the data, so the data is not held for any longer than necessary.

Note that the summary provided in this form does not bypass the requirement for a clear, specific and unambiguous scientific protocol to accompany your application. Per **ODR Approval Guidelines: scientific protocol (Annex B),** the protocol must also be version-controlled and correspond with that submitted to other approval bodies, where applicable (eg for review by an NHS Research Ethics Committee).

Where non-substantial amendments have been made to the scientific protocol, it is recommended that the current and a tracked changed copy of the superseded version are shared with ODR, so that changes can clearly be identified.

D1: Overview

D1.1	ODR reference	Provide the reference assigned by the ODR for this project. Leave blank if you are yet to be assigned a reference number.
D1.2	Data sharing contract reference	Provide the reference number of any pre-existing data sharing contracts or data re-use agreements (executed pre-April 2015) that relate to this application. Leave blank if this is a new project.
D1.3	Project title	Specify the title that has been given to the project. This should be the same title that has been used on any associated requests or applications (eg the NHS Research Ethics Committee application for the same project) and should meaningfully describe the project. Any abbreviations should be spelled out in full.

D2: Lay summary

D2.1	Describe in plain English the overall project aims(s) and objectives (limit to 2-3 sentences)	For D2.1-D2.4, you must write your responses to these questions according to the editorial requirements found in **ODR Approval Guidelines: lay summary (Annex E)**. Applications will be deferred where these requirements are not met. If your application for PHE data is successful, the responses provided to questions D2.1-2.4 will be published in the PHE Data Release Register. You can read examples of published lay summaries by downloading the Register or in the **ODR Approval Guidelines: lay summary (Annex E)**.
D2.2	Describe in plain English the health problem to be addressed by the project, why this project is needed and how the existing evidence supports the need for this work (limit to 200-300 words)	
D2.3	Describe in plain English the project methods, explaining how PHE data will be processed. This should include information on (but not limited to) the type or source of the data	

	required for the study, data collection, sampling and analysis methods. Where the project involves data linkage or use of Data Processors, this must be described (limit to 200-300 words)	
D2.4	Describe in plain English the anticipated public health benefits and/or impact of conducting this project. This should include the potential beneficiaries, how your project may impact them, and how you will facilitate this (limit to 200-300 words)	

D3: Project type

D3.1	Indicate if the project is research, service evaluation, clinical audit or surveillance (usual public health practice). If these broad definitions to not describe your project, select 'other' and provide an alternative description.	Select from the tick boxes whether the project's end use can be best described as: • research • service evaluation • clinical audit; or • surveillance (usual public health practice). Should these options not be descriptive of the project, select 'other' and provide an alternative description. Where more than one option applies, the form will allow you to select multiple options. Brief definitions of each category are described in Table 1 below; however, the ODR understands that it can sometimes be difficult to decide which end use is appropriate.

		As the form uses conditional logic, it is important that if you are not clear on how to categorise your project that you seek advice through the ODR Pre-application Support Service (PaSS) to discuss the categories and how the selections will impact on the qualified application requirements detailed in **ODR Approval Guidelines: application requirements**. The ODR further recommends guidance produced by the Health Research Authority: • Defining Research Table

Table 1: Project type definitions

Research	For the purpose of the UK Policy Framework for Health and Social Care Research, "research is defined as the attempt to derive generalisable or transferable new knowledge to answer or refine relevant questions with scientifically sound methods". This excludes audits of practice and service evaluations.
Service evaluation	Service evaluations are designed to answer the question "What standard does this service achieve?". They measure how current service is achieving its intended aims, without reference to a standard.
Clinical audit	Clinical audits are designed and conducted to inform delivery of best care and judge if the quality of a service meets a defined standard. They are designed to answer: "Does this service reach a predetermined standard?".
Surveillance	Surveillance or usual practice in public health is designed to investigate the health issues in a population to improve population health and/or understand an outbreak or incident to help in disease control and prevention.
Other	Select if your project is not defined by one of the categories above and provide a definition of your project type.

D4: Patient and/or professional contact

D4.1	Does this project involve processing PHE data to contact:	Select from the drop down menu your response. Where 'yes' is indicated, describe all instances where the data will be processed during the course of the project to contact a

	• patients • service users • health care professionals If yes, provide details of how the data will be used and share copies of the materials (such as draft letters or emails)	data subject, relative of the data subject, their representative, or any health professionals. You must accompany your application with any copies of letter templates and other materials proposed to be used in the contact exercise.

D5: Project timeline

D5.1	Estimated project start date	Provide an overview of project start date and the planned duration of the project. All data sharing contracts issued by the ODR will stipulate a start and end date ('the term'). In determining the appropriate term, the ODR will take into consideration the information presented in your project timeline and scientific protocol. Requirements for retention (including publication plans) and archiving, such as those required by funding bodies, should be included as part of the project timeline. This should also be reflected in the scientific protocol. At the end of the contract term, the data you access through ODR approval must be destroyed, unless an amendment request is approved to extend the agreed term. Failure to comply with this contractual requirement may affect ODR's issuing its support to other requests from your organisation.
D5.2	Project duration (months)	

D6: Research databases and access procedures

The ODR welcomes applications to form new research databases or for PHE data to be curated as part of a pre-existing research database. Should the data be requested for this purpose, the ODR must review the governance, access policy and/or procedures and the sub-licensing agreement(s) that will be used to support the sharing of data with third parties.

Note that the default terms of the ODR data sharing contract expressly prohibit any sub-licensing or onward sharing of PHE data, except in circumstances where:

- the contract is specifically drafted to include permissive clauses following review of the information requested in D6.1; or
- the data is rendered anonymous to ISB1523: Anonymisation Standard for Publishing Health and Social Care Data.

If you intend to use PHE data as part of a research database and would like to release data to third parties that does not comply with the ISB standard, you must clearly state how the research database will operate, so this can be considered. If positively reviewed, permissive clauses will be embedded in the contract. Details of the requirements are set out below and in **ODR Approval Guidelines: application requirements.**

Due to the interest in the curation of data for research databases, the ODR will develop further detailed guidance during 2021.

Should you be instructing a Data Processor to process the data on your behalf, this must also be made clear and Section J must be completed.

D6.1	Will the data requested be curated for a research database? If yes, give details	Select your response from the drop down menu. Where 'yes', provide a summary of the arrangements and accompany your application any documentation (such as a standard operating procedure) that is descriptive of: • the data management plan of the research database • how the suitability of a request to access data through the research database will be determined and details of who will conduct this assessment

		• the scope of the risk assessment conducted for the onward sharing of the data, including template checklist or privacy impact assessment; and • the controls placed on the data to comply with data protection legislation and the Information Commissioner's Office (ICO) Data Sharing Code of Practice, including a copy of the sub-licence that will be put in place to use the data.

Section E: Data requirements

The data requirements section of this form provides the ODR with an overview of data that is relevant and necessary for the conduct of the project, its level of identifiability and its source. It also provides the ODR with:

- information regarding the linkage of PHE data to other datasets controlled by the organisation named in A2, its processor(s) or a national data intermediary, such as the Office for National Statistics or NHS Digital; and
- information about whether any non-PHE data that is or will come into the possession of the applicant for this project may have a material effect on the ODR's risk assessment and the safeguards necessary to minimise risks to individuals or potential adverse effects of sharing.

In addition to this information, all applications for ODR Approval must be accompanied by a detailed data specification in line with the requirements outlined in the **ODR Approval Guidelines: data specification (Annex C)**. This specification must be carefully drafted in accordance with the specific criteria detailed in Annex C to ensure that the application for ODR Approval demonstrates the data to be processed is:

- adequate – sufficient to properly fulfil your stated purpose (the aims, objectives and methodologies presented in your scientific protocol)
- relevant – has a rational link to that purpose
- limited to what is necessary – no more than you need for that purpose

The ODR continues to build a library of data specification workbooks that can be used to identify the data required. Contact ODR to identify if a workbook is available for the data required for your application.

It is advised that due regard is given to the content of Annex C when drafting the scientific protocol, so that there is a clear definition of the population or sample; and that the protocol unambiguously justifies the scope and scale of the data requested.

E1: Data specification summary

E1.1	Classification of the level of identifiability of data requested	Select using the tick boxes the appropriate classification of the level of identifiability of the data requested. The definitions are outlined below. • **De-personalised:** Data is considered de-personalised if it is stripped of direct

		identifiers but contains fields which could be used to indirectly identify an individual through combinations of information, either by the people handling the data or by those who see the published results (eg ethnicity, sex, month and year of birth, admission dates, geographies or other personal characteristics). De-personalised data may otherwise be referred to as: de-identified, pseudonymised, key-coded, masked, anonymised in context, effectively anonymised, non-disclosive, non-identifiable, de-identified data for limited access. PHE data that is classified as de-personalised is not considered to be rendered anonymous in line with the Information Standards Board (ISB) Anonymisation Standard for Publishing Health and Social Care Data and therefore is not suitable for release as Open Data. • **Personally identifiable:** Data is considered personally identifiable if it includes direct identifiers (eg name, address, NHS number, date of birth) or would be directly identifiable in the hands of the data recipient (such as by hospital number or a cohort-specific identifier). In a health context, this level of identifiability is also referred to as 'confidential information' or 'confidential patient information'. If your data request is for both personally identifiable data and de-personalised data (for example data related to a consented cohort recruited from a small number of GP practice and aggregated denominator data on all patients within the wider CCGs the practice belong to), select 'personally identifiable' as

		this will prompt additional questions to be flagged for completion. For more information on these classifications and the 'spectrum of identifiability', see Understanding Patient Data.
E1.2	List the dataset(s) requested from PHE in this application which are necessary for the conduct of your project (for example 'Health Care Acquired Infections' or 'National Cancer Registration and Analysis Service')	List the PHE data source(s) applicable to the request (ie the particular dataset(s) you are requesting). This should be a top level description of the dataset name or system the data is held in.
E1.3	Where PHE data will be linked to other data sources, provide an outline of how the linkage will be conducted. This should include all organisations that will be involved and their respective roles in the data linkage	Provide a summary of any data linkages required using PHE data (either by PHE, the organisation named in A2 or any other body) as part of this project. You must share with the ODR a diagram to illustrate the proposed data flows between each data controller and any Data Processors acting under instruction. Ensure the diagram illustrates: • incoming and outgoing data • organisations and/or people sending/receiving information • storage system for the 'Data at Rest' • methods of transfer Each organisational boundary must be clearly identified and where personally identifiable data is moving between organisations, the fields to be shared must be listed (eg NHS number, DOB and StudyID). This should not be limited to linkages with PHE data, so that the ODR has a complete understanding of the scope and scale of the data involved in the project. Details of upholding national opt-out should be outlined at each stage.

		During 2021, the ODR will develop an example data flow diagram and make this available.

E2: Other (non-PHE) data processed for this project

For projects where you are currently processing or intend to process any other personally identifiable or de-personalised that does not fall under the custodianship of PHE, provide details of the data that is/will be processed.

This information enables the ODR to have a rounded and complete view of the scope and scale of the data you are, or will be, processing so that all risks associated with sharing PHE data can be identified and if necessary, appropriate actions can be put in place to mitigate such risk.

E2.1	Will any other personally identifiable or de-personalised data, which is not controlled by PHE, be processed for this project?	Select from the dropdown menu your response. Where 'yes', provide the dataset name, classification of the data (ie personally identifiable), the legal basis for processing (under common law and data protection), and the dataset period. Example 1: "We received personally identifiable Hospital Episode Statistics (Admitted Care) under explicit informed consent from NHS Digital. This includes all episodes from 2000-2020 that mention breast cancer (C50x). A copy of the consent form and PIS is included with my application. We will process under UK GDPR Article 6(1)(a) and 9(2)(J)." Example 2: "De-personalised data from the National Pupil Database (NPD) on all pupils aged under 10 and (2) for linkage to the NPD for the cohort of children with cancer requested in this application. We are seeking S251 support for the linkage to be conducted by NHS Digital as a trusted third-party linkage service. Both datasets will be for the school years 2018-2020. We will process the identifiable data under UK GDPR Article 6(1)(a) and 9(2)(J)."

Section F: Programme-level support

Access to certain PHE data is dependent on the positive review of the scientific value, integrity and feasibility of the proposed project by a programme-specific Research Advisory Committee (RAC) or Programme Lead.

Datasets requiring programme-level support include:

- NHS Abdominal Aortic Aneurysm (AAA) Screening Programme
- NHS Bowel Cancer Screening (BCSP) Programme
- NHS Breast Screening (BSP) Programme
- NHS Cervical Screening (CSP) Programme NHS Diabetic Eye Screening (DES) Programme
- NHS Fetal Anomaly Screening Programme (FASP)
- NHS Infectious Diseases in Pregnancy Screening (IDPS) Programme
- NHS Newborn And Infant Physical Examination (NIPE) Screening Programme
- NHS Newborn Blood Spot (NBS) Screening Programme
- NHS Newborn Hearing Screening Programme (NHSP)
- NHS Sickle Cell and Thalassaemia (SCT) Screening Programme
- Sloane Project (Audit of Non-invasive Carcinomas and Atypical Hyperplasias)
- NHS BSP & ABS Audit of Screen Detected Breast Cancer

You must approach the relevant RAC or Programme Lead for approval before completing an ODR application. A copy of the letter of support from the Research Advisory Committee or Programme Lead must accompany your application.

Contact details for the NHS Screening Programme RACs and information on how to apply can be found in the NHS population screening data requests and research guidance.

F1.1	Has support been granted?	If yes, provide the name of the RAC or Programme Lead that has provided programme-level support.
F1.2	Programme-level reference	Indicate any reference(s) assigned to your project by the RAC or Programme Lead.
F1.3	Date of programme support	Indicate the date of approval of your project by the RAC or Programme Lead.
F1.4	Identify any contacts within the programme that your request has been discussed with	Provide the names of PHE staff you have worked with on the development of your project.

Section G: Lawful basis to process personally identifiable data

Where the project purpose(s) cannot be met with either open data or de-personalised data, it may be appropriate to request access to personally identifiable data.

To process all personally identifiable data, the ODR must be assured that the data will be processed lawfully, fairly and in a transparent manner throughout its lifecycle. To do this you must evidence to the ODR:

- a valid exception to the common law duty of confidentially; and
- that the data controller or joint data controller(s) comply with UK GDPR. More information about the requirements for this are set out under Section G1 and G2.

Whilst applications for data can be discussed with the ODR Pre-application Support Service (PaSS) prior to confirmation of relevant approvals being received, all approvals, including (where applicable) NHS REC favourable opinion and Section 251 of the NHS Health and Social Care Act 2006 (S251), must be sought and submitted as part of a consolidation and complete application before ODR will commence its formal review.

G1: Legal gateway (common law duty of confidentiality)

A duty of confidentiality arises when information is obtained in circumstances where it is reasonable for a person providing information to expect that it will be held in confidence by the recipient (such as the relationship between a patient and the health professionals who care for them).

The duty extends beyond death and is distinct from obligations under data protection legislation (see Section G2). However, this duty is not absolute and confidential information or confidential patient information (collectively referred to as personally identifiable data in this form) can be lawfully disclosed, to or from, PHE when there are grounds to set this duty aside.

If your application includes the processing of personally identifiable data, you must demonstrate how the duty of confidentiality has been set aside (see ‘valid exceptions below’) and demonstrate to the ODR:

- the organisation(s), including PHE, transferring personally identifiable data have a legal basis to share the data for the specific purpose(s) in the scientific protocol
- the organisation(s), including PHE, receiving the data have a legal basis to receive and process the data for the specific purpose(s) described in the scientific protocol; and
- the organisation(s) which will act upon or link personal data have a legal basis to do so.

Valid exceptions include:

- **Direct care:** the individual care of patients by one or more registered and regulated health or social care professionals and their team, with whom the individual has a legitimate relationship for their care. The types of processing and projects that would be acceptable under this exception are provided in G1.1. This exception must be supported by the organisation's Caldicott Guardian.
- **Informed consent:** the individual has capacity and has explicitly consented to the processing described. This means the individual knows and understands how their data is to be used and shared (there should be 'no surprises') and they should understand the implications of their decision.
- **Statutory exemption:** the disclosure is required by law, or the disclosure is permitted under a statutory process that sets aside the duty of confidentiality for a limited purpose, such as Section 251 of the National Health Service Act 2006 and its current regulations, the Health Service (Control of Patient Information) Regulations 2002.

Where more than one of these exceptions applies, provide evidence of each.

In addition, there may be other situations which mean sharing confidential information is necessary; to safeguard the individual, or because of significant public interest, or because of a contractual relationship with the individual. As the ODR is responsible for supporting access to data for direct care or secondary (medical) purposes only, the options cited on the form are limited to those relevant to the application process.

G1.1	Direct care - authorisation from your organisation's Caldicott Guardian	The Caldicott Review (2013) defined 'direct care' as a "clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals by one or more registered and regulated health or social care professionals and their team, with whom the individual has a legitimate relationship for their care". Note that research cannot be conducted under the auspices of 'direct care'. Where direct care is identified to be the valid exception to set aside the common law duty of confidentiality, the ODR expects that the

		organisation's Caldicott Guardian (who is responsible for safeguarding the confidentiality of patient information) is cited and agrees: • the processing of the data will be legal, ethical and strictly for direct care purposes; • the data will be accessed on a need to know basis; and • the applicant named in A1.1 is (a) a registered and regulated health or social care professionals and their team, with whom the individual has a legitimate relationship for their care and (b) appropriate to disclose data to. To demonstrate their agreement of the above, you must name the Caldicott Guardian and accompany your application with a signed letter from your Caldicott Guardian using your organisation's letterhead. This letter must be dated within three months of the application date and it must clearly reference the project title and that they are satisfied patient confidential data will be processed for direct care purposes only. The ODR will confirm that the Caldicott Guardian named in G1.1 is associated with the applicant's organisation and is recognised by the UK Caldicott Guardian Council.
G1.2	Informed consent	Where informed consent is identified to be the valid exception to set aside the common law duty of confidentiality, you must enclose blank copies of the consent form(s), associated participant information sheet(s) and any other supporting materials for the consent process for the duration of the project. Where there has been iterate versioning of any of these documents, each version should

		be submitted and a summary explaining the changes shared with ODR. All the consent materials relevant to the application must have received a favourable ethical opinion from an NHS Research Ethics Committee. For consent to be valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. In practice, this means individuals should know and understand how their information is to be used and shared (there should be 'no surprises') and they should understand the implications of their decision, so they can provide an unambiguous indication of agreement. The ODR will review the information shared to ensure that the consent is compatible with the proposed processing. There will always be situations where some individuals cannot give consent, for example, young children or adults who lack capacity. In many of these cases, particularly in the case of small children, a responsible adult, usually their parent or guardian (or other person authorised to carry out this role) who is legally entitled to speak on their behalf will be asked to give their consent. In such circumstances, the PHE Caldicott Guardian and ODR will take into consideration key considerations such as Foster competency and the age of consent. It should be noted that over time and as case law has developed, the standard of consent expected has been superseded by modern best practice. Therefore it must be recognised that consent is an ongoing process and the law is developed by decided cases, with the consequence that even if a particular consent statement is deemed adequate today, it may later be found to be insufficient due to

		changes in the fact of what is being done with the data, or in light of subsequent legal decisions. Consequently, applications with amended or additional data flows or substantive changes to the purposes of a study that could not have been foreseen by the data subject at the time of original consent will need to consider the duty of confidentiality. It is recommended that as part of these considerations, patient and public involvement advocates are engaged to strengthen your understanding of whether any processing would be within their 'reasonable expectation'. Where the lawful basis to process the data under UK GDPR is identified as consent (ie Article 6(1)(a) &/or Article 9(2)(a)), then the approach to consenting participants will also be reviewed in line with published detailed guidance from the ICO to ensure the obligations under Article 7 are met. Where the applicant is relying on consent as the basis in data protection legislation for processing and has met the requirements for consent for lawful processing under UK GDPR, it will be taken that the consent material also meets the standard required in respect of the duty of confidentiality.
G1.3	Statutory exemption under the Health Services (Control of Patient Information) Regulations 2002 – exemption obtained for this project	In England and Wales, Section 251 of the NHS Act 2006 (originally Section 60 of the Health and Social Care Act 2001) provides the statutory power to permit the use of patients' medical information without their consent. Where a statutory exemption under the Health Services (Control of Patient Information) 2002) regulations has been sought to set aside the common law duty of confidentiality, select from the drop

		down the specific exemption obtained for your project. A description of the Health Service (Control of Patient Information) Regulations 2, 3 and 5 are outlined below: • **Regulation 2** makes provisions relating to processing patient information by bodies who construct and maintain cancer registries for surveillance on diagnosis and treatment of neoplasia. • **Regulation 3** makes provision for the processing of patient information for the recognition, control and prevention of communicable disease and other risks to public health. Note that Regulation 3 is administered by PHE, not the Confidentiality Advisory Group (CAG). • **Regulation 5** can be used to permit processing for a range of medical purposes, broadly defined to include 'preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and adult social care services. In addition, you must share with the ODR copies of: • all section 251 approval letter(s); and • confirmation of extant section 251 support (eg presence on CAG register, the applicant's latest annual review submission). Where these documents alone do not provide ODR with sufficient detail about the scope of the exemption in regard to the population, data flows or permitted processing, the

		ODR may also request a copy of your IRAS application. Before applying for a statutory exemption under Regulation 2 or 5 to process personally identifiable data controlled by PHE, you must approach the ODR. The Confidentiality Advisory Group expects that its applicants can demonstrate that they have explored with the data controller(s) why gaining individuals consent is impossible or impracticable, and the use of de-personalised or open data would not achieve the project purpose(s). In circumstances where there is no reasonable alternative to the processing of personally identifiable data and the sharing of the data is considered justified, the ODR will write a letter of support to the Chief Investigator. In circumstances where this request is not pursued, this may create delays in both the CAG and ODR providing a final outcome. Involving patients or members of the public in research design is also longstanding good practice; so, the ODR strongly recommends public and patient involvement in the design of your project, including circumstances where you are proposing that personally identifiable data should be processed without informed consent. This approach will strengthen your application to the Confidentiality Advisory Group. Where a statutory exemption is obtained and ODR Approval is successful, the ODR will uphold the national opt-out unless evidence is provided that the Secretary of State has set aside this responsibility for the specific processing in your scientific protocol. For further details, read **ODR Approval Guidelines: applying the national data opt out (Annex G).**
G1.4.1	Reference	Provide the unique reference assigned by the Confidentiality Advisory Group or PHE

		to your statutory exemption under Regulation 2, 3 or 5 of the Health Services (Control of Patient Information) Regulations 2002.
G1.4.2	Date of next renewal	It is a requirement under the Health Services (Control of Patient Information) Regulations 2002, where statutory support is provided under Regulations 2, 3 or 5, that such support is subject to review at intervals not exceeding 12 months. This expectation is also captured in the standard conditions of support detailed at the back of the final approval letters from both the Confidentiality Advisory Group or PHE. The ODR will only support requests where there is clear evidence that such reviews have been fulfilled as instructed. Provide the date this review must be completed by, as indicated by the Confidentiality Advisory Group (Regulation 2 and 5) or PHE (Regulation 3 support only). A register of active Regulation 2 and 5 approvals is published and maintained by the Health Research Authority on behalf of the Confidentiality Advisory Group. Should you be unclear of whether you have met this expectation or need to check the date of your new annual review, you can do so by checking the Confidentiality Advisory Group register, which is updated monthly.
G1.4.3	I have attached all letters, including evidence of positive annual review, from the Secretary of State or Confidentiality Advisory Group documenting that an exemption to set aside the common law duty confidentiality has	Select the drop down to prompt the summary of evidence to update. You must accompany your application with all letters, including evidence of positive annual review, from the Secretary of State or Confidentiality Advisory Group documenting that an exemption to set aside the common law duty confidentiality has been granted and is extant.

	been granted and is extant. Where an exemption is in place for a contact exercise, alongside evidence of the exemption, all copies of materials (letters etc) to be used to contact individuals are also attached.	Where the statutory exemption is in place for a contact exercise, alongside evidence of the exemption, all copies of materials (letters etc) to be used to contact individuals are also attached.

G2: Legal gateway and transparency (data protection)

Article 5(1) of the UK General Data Protection Regulation (UK GDPR) requires that personal data shall be:

> "(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')"

If your application includes the processing of personally identifiable data, you must demonstrate:

- that there are valid grounds under the UK GDPR (known as a 'lawful basis') for the processing of personal data by the data controller(s). The six acceptable lawful bases are described in Article 6 and detailed in G2.1
- as personal data concerning health is special category personal data, the application must also demonstrate that one or more specific additional condition(s) for processing in Article 9 are met (see Section G2.2); and
- you must also demonstrate that you have made available to the data subject accessible privacy information (also called a privacy notice or transparency information) about how their data will be processed to comply with the Right to be Informed (Article 12) and allow them to exercise their right to the protection of personal data.

The specific obligations that must be met in regard to transparency are established under Articles 13 and 14 of UK GDPR (which differentiate between circumstances where personal data is directly obtained from the data subject and where it is obtained from a secondary source). This obligation of transparency is also echoed in the Caldicott Guardian Principle 8: Inform patients and service users about how their confidential information is used.

For more information about the expected content of a privacy notice read **ODR Approval Guidelines: privacy notice (Annex D)**.

In order to ensure compliance with the UK GDPR, it is important to work with your information governance team, Data Protection Officer or legal counsel to identify and record the lawful ground(s) you are relying on in order to justify the processing of personal data. This is also necessary to understand the extent of the obligations, as some data subject's rights are contingent upon the controller's reliance on particular grounds.

In detailing to the ODR, the legal basis under data protection legislation, you should consider:

- Have you been clear with an individual about how you will use their data? If yes, is this documented, including evidence of what an individual was told, and what lawful processing condition you intend to rely upon for processing their data in the future?
- Does your Privacy Notice (also known as a Privacy Policy or Information Notice) and any other data subject facing materials consistently reflect the legal basis and specific condition(s) identified to the ODR?
- Are you confident you can defend the decisions you have made to an individual or a regulator?
- Where relying on consent (ie Article 6(1)(a) &/or Art 9(2)(a)), does the quality of the consent model used meet UK GDPR requirements?
- Where relying on legitimate interest (ie Article 6(1)(f) &/or Article 9(2)(d)) has a legitimate interest assessment (LIA) been carried out?

The ICO have published guidance on how to comply with the legal requirements laid out in UK GDPR and have also published an interactive tool to help determine the legal basis and specific condition for processing special category personal data.

Should you not be clear about how to comply with your responsibilities under UK GDPR, the ODR strongly recommends that you seek advice from your organisation's information governance team, Data Protection Officer or legal counsel. The ODR is unable to offer legal advice.

G2.1	Article 6 lawful basis for processing personal data	The lawful grounds for processing are set out in Article 6 of the UK GDPR. Select from the list below. At least one of these must apply whenever you process personal data: (a) Consent: the individual has given explicit, informed consent for you to process their personal data for a specific purpose (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take

		specific steps before entering into a contract (c) Legal obligation: the processing is necessary for you to comply with the law (d) Vital interests: the processing is necessary to protect someone's life (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests You are strongly encouraged to work with your information governance department, Data Protection Officer or legal counsel to identify which legal basis you should use. Technical guidance on UK GDPR intended for Data Protection Officers, research managers, information governance or equivalent roles has been made available by the Health Research Authority to support the research community.
G2.2	Article 9 condition for processing special categories of personal data	Special category data is personal data that needs more protection because it is sensitive. It includes data that reveals a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation. In addition to the Article 6 lawful basis, at least one condition listed in UK GDPR Article

		9(2) must be met to process special categories of data. Select the condition(s) for processing. More than one condition can be selected where applicable: (a) Explicit consent (b) Obligations/rights of the controller/data subject (c) Vital interests (d) Legitimate activities (e) Made public by the data subject (f) Legal claims (g) Substantial public interest (h) Preventative or occupational medicine (i) Public interest in the area of public health (j) Archiving purposes in the public interest, scientific or historical research purposes You are strongly encouraged to work with your information governance department, Data Protection Officer or legal counsel to identify which conditions you should use. Technical guidance on UK GDPR intended for Data Protection Officers, research managers, information governance or equivalent roles has been made available by the Health Research Authority to support the research community.
G2.3	Privacy notice	The individual's right to be informed is set out under Articles 12, 13 and 14 of UK GDPR. If you are requesting personally identifiable data, you must demonstrate that you have in place a UK GDPR compliant privacy notice that informs the subjects of the processing of their personal data.

		Applications from health and social care providers to process personally identifiable, where 'direct care' is cited in G1, must evidence their corporate privacy notice. The ODR recommends that a hyperlink to the published notice is included in Section K. Applications to process personally identifiable data for purposes other than direct care must be project-specific and provide due reference to the role of PHE as a source of data. Detailed guidance to support you in meeting this legal responsibility is available from the ICO and summarised in **ODR Approval Guidelines: privacy notice (Annex D)**. During 2021, the ODR will develop an example wording that describes the role of PHE as a secondary source of data.

Section H: Ethics approval for research

If you are requesting data from PHE that relates to NHS patients' or their care, you must demonstrate that your project has NHS Research Ethics Committee (REC) Favourable Opinion from the Health Research Authority.

Applicants must demonstrate this approval by providing:

- the name of the research ethics committee,
- reference assigned by the committee and;
- your application must also be accompanied by copies of the approval letter(s) from the committee and/or acknowledgement of amendments to an existing approval, where either a substantial amendment has been sought or the committee has been informed of a non-substantial amendment.

Applications for NHS Research Ethics Committee review can be started using the Integrated Research Application System (IRAS).

If you are requesting data that does not relate to NHS patients' or their care, institutional REC approval is sufficient (ethical oversight and approval from your own organisation). Where applicable, evidence of this approval must also be sent with the details listed above (committee name, project reference, evidence of approval and/or acknowledgement of any amendments).

Applicants should note that the ODR will review the concordance of document versions submitted for REC approval, against those submitted to the ODR as part of their data request. Applications will be deferred where version control does not align. For more information on best practice in document management, read Section 9.5 of the UK Policy Framework for Health and Social Care Research (2017).

Whilst applications for data can be discussed with the ODR Pre-application Support Service (PaSS) prior to confirmation of relevant approvals being received, all approvals, including (where applicable) NHS REC favourable opinion and Section 251 of the NHS Health and Social Care Act 2006 (S251), must be sought and submitted as part of a consolidation and complete application before ODR will commence its formal review.

H1.1	Research Ethics Committee (REC) name	Provide the name of the REC who reviewed your application.
H1.2	Reference(s) assigned by the REC	Provide the REC reference(s) assigned to your project.
H1.3	I have attached all REC approval letter(s), including amendments	You must accompany your application with all the REC approval letters, including amendments.

Section I: Information governance, data management and security assurances of the applicant's organisation

For all requests to access personally identifiable or de-personalised data (see Section E1), the ODR will check that the organisation requesting the data has in place appropriate organisational and technical safeguards to process the data safely and securely.

I1: Information governance declaration

I1.1	I, the applicant, certify by ticking this box that the above organisational information governance requirements have been met	You must certify that the follow guarantees are in place to ensure that the data are safe from unforeseen, unintended or malevolent use: • I certify that the individual(s) who will process the data is a/are bona fide worker(s) at the applicant's organisation (Section A). • I certify that the individual(s) (including permanent, temporary and locums) who will process the data has/have been subject to personnel background checks and their employment contracts include compliance with organisational information governance standards. • I certify that information governance awareness and mandatory training procedures are in place and the individual(s) who will process the data is/are appropriately trained. • I certify that the data can be entrusted to the organisation, in the knowledge that the individual(s) processing the data will conscientiously discharge his/her/their obligations, including with regard to confidentiality of the data. Indicate, using the tick function that you can comply with the statements outlined above. Should you not be clear about how to comply with these responsibilities or are unable to

		provide such assurances, the ODR strongly recommends that you seek advice from your organisation's information governance team, Data Protection Officer or legal counsel.

I2: Territory of processing

I2.1	Territory of processing	Select from the drop down the region the data will be processed. Where the data will be processed in more than one region or outside of the EEA, select 'other' and specify. The territory of processing includes not only where the data will be accessed and worked upon, but also where it is stored and where those servers are physically located. For the avoidance of doubt, this includes the server locations for cloud hosting arrangements.

I3: Data protection registration (UK organisations only)

The Data Protection (Charges and Information) Regulations 2018 requires that every organisation in the UK that processes personal information to pay a fee to the ICO, unless they are exempt.

If your organisation is based in the UK, you must provide details of their organisation's registered name, registration number and the expiration date of the data protection register, as detailed on the Data Protection Public Register.

Details of each organisation registered on the Data Protection Public Register are publically available at www.ico.org.uk/esdwebpages/search. Should your organisation not appear on this Register, it is advised that you liaise with your information governance team or Data Protection Officer, so that this evidence can be provided to the ODR as part of your application.

If you are requesting to access personally identifiable data and citing that the lawful basis for the processing under Article 6 is Article 6(1)(e) Public Task, the ODR will also validate this is correct using the Register.

I3.1	Data Protection Public Registration number	Insert the unique registration number for the organisation named in Section A2 as recorded in the Data Protection Public Register. If your organisation is exempt from completing the register or situated outside of the UK, state 'Exempt' and leave your responses to I3.2 and I3.3 blank.
I3.2	Registered organisation name	Insert the official name of the organisation as recorded in the Data Protection Public Register.
I3.3	Registration expiration date	Insert the expiry date for the organisation's data protection public register record (a registration is usually valid for 12 months).

I4: Security assurance

A key principle of the **UK GDPR** is the '**security principle**' (UK GDPR Article 5(1)(f)). This principle requires that data is:

> "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')".

Article 32 of the UK GDPR provides more specifics on the security, stating:

> "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".

In this section you must demonstrate that you have in place suitable policies, procedures and practices that ensure the data are safe from unforeseen, unintended or malevolent use.

These include:

- technical measures, such as encryption, anti-virus, anti-malware and firewalls
- physical measures, such as ensuring servers are in a separate room with secure lockable doors using access codes or entry combination/cards

- organisational measures, such as appointing a Data Protection Officer, policies and staff training to recognise system threats, such as phishing emails, malware and unauthorised use; breach reporting procedures or restricting access to the data to a need-to-know basis

The ODR will review the assurances you provide to make sure that your organisation's information security measures provide sufficient guarantees equivalent to, or better than, the Department of Health and Social Care's data security and information governance requirements – as set out in the Data Security and Protection Toolkit.

I4.1	Security assurance	Select using the tick boxes one of the three security assurances that demonstrates that the organisation named in A2 have in place appropriate organisation, physical and technical measures to ensure the confidentiality, security integrity and availability of the data. you must certify to the ODR that the organisation named in A2 can provide sufficient guarantees that they will implement appropriate technical and organisational measures, and that you will continue ensure their compliance on an ongoing basis. A description of the possible choices is outlined below, alongside an explanation of the qualified application requirements that must be shared with the ODR to confirm these measures are valid: • **Data Security and Protection Toolkit (DSPT)** (previously called 'Information Governance Toolkit') is the gold standard and a requirement for all health and care services operating under an NHS contract from April 2018. Where the DSPT is indicated and the reference provided, the ODR will assess your organisation has in place 'Standard Met' or 'Standard Exceeded' for the most recent version of the toolkit. Where partial or non-compliance is revealed, the ODR will require you to update the toolkit record to address the

		shortcomings before we can progress or provide alternative evidence (either ISO27001:2013 certification or a project-specific SLSP). You can search for your organisation's DSP toolkit code and score on the toolkit website. • **ISO 27001:2013 certification** with alignment of policies, procedures and controls to ISO 27002:2013 and, if utilising third party services ISO 27017:2015, ISO 27018:2014 (where the third party has a multi-tenanted location). Where ISO certification is indicated, you must submit a copy of a valid ISO certificate as part of the application. The certificate must clearly indicate the name and address of the organisation identified in A2. • **A project-specific System Level Security Policy (SLSP)** - you must submit to the ODR a report that is descriptive of how your organisation will administer, secure, handle and use the requested data with due regard to the organisational, technical and physical controls employed to enforce your organisation's information governance, security policies and procedures. The SLSP must consider the complete lifecycle of the data, including deletion and due reference should be given to corporate policies. A template is available on request from the ODR that will assist in the formatting of an SLSP.

Section J: Data processor(s) acting under instruction

All fields in this section are mandatory where a third party (a person, public authority, agency or other body) will act on the documented instructions of the controller to process the data in circumstances where the data cannot be rendered anonymous to the ISB1523: Anonymisation Standard for Publishing Health and Social Care Data.

The formal definition of the 'Data Processor' and 'Processing' as set out in the UK GDPR Article 4:

Article 4(8) 'Data Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Article 4(2) 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

In circumstances where the data cannot be effectively rendered anonymous to the ISB1523 Anonymisation Standard, you must complete the information in Section J. Where there are multiple processors (or a processor has instructed a sub-processor), repeat the content of Section J for all parties. These assurances can be included in Section K: Any additional information.

For each processor or their respective sub-processor(s), a fully data processing agreement must also accompany your application. The data processing agreement must comply with the obligations prescribed in Articles 28 – 36 of UK GDPR and terms broadly mirror controls that will be placed on the applicant by PHE; specifically:

- there are documented instructions to process the data for a specific, time-limited purpose
- there is evidence of due diligence over the suitability of the processor in respect of the types of personal data being processed
- there are suitable confidentiality clauses in the agreement
- the processor has adequate information security in place
- the contract manages the downline use of sub-processors
- the contract puts in place measures for the processor to help the controller comply with data subject rights

- there are mechanisms to assist in cooperation with the controller and the relevant data protection authorities
- there are processes in place to deal with data incidents and data breach notifications; and
- there are processes in place to deal with destruction or return of personal data at the end of the agreement.

These expectations are set out in **ODR Approval Guidelines: data processors (Annex H)** and an example copy of the ODR contract is available on request**.**

You are strongly encouraged to consult with your organisation's information governance team, Data Protection Officer or legal counsel to make sure that all obligations set out in Articles 28-36 can be met and that all necessary due diligence has been conducted before formally procuring the services of the Data Processor.

J1.1	Are you instructing a Data Processor to process the PHE data on your behalf?	Select from the dropdown and if yes, complete J1.2 and J1.3.
J1.2	Data Processor name	Provide the name of the Data Processor that you will instruct to act on behalf of the organisation named in A2.
J1.3	Data Processor address	Provide the business address of the Data Processor named in J1.1.

J2: Information governance assurances - data processor declaration and data processing agreement

When instructing the Data Processor, you must execute a written data processing contract. The contract must bind the Data Processor to the controller in respect of its processing activities, as specified in your application.

In addition, you must certify to the ODR that the processor has provided you with sufficient guarantees that they will implement appropriate technical and organisational measures, and that you will continue ensure their compliance with these measures on an ongoing basis.

In J2.1, you are asked to declare the following:

- I certify that a data processing agreement has been executed that:
  – provides an explicit, written directive to the Data Processor to process the data for a specific, time-limited purpose(s) as presented to ODR in this application; and

– complies with and enforces the legal obligations under Articles 28 – 36.

- I certify that appropriate due diligence has been conducted to demonstrate that:
  – the Data Processor can provide "sufficient guarantees" (in particular, terms of its expert knowledge, resources and reliability) to implement appropriate technical and organisational measures; and
  – the Data Processor will conscientiously discharge their obligations, including confidentiality of the data and understands their direct obligations under the UK GDPR.
- I certify that the Data Processor's compliance will be reviewed on an ongoing basis, in order to satisfy the accountability principle.

A copy of the fully executed data processing agreement must accompany your application.

J2.1	I, the applicant, certify by ticking this box that the above responsibilities have been addressed and a copy of the executed data processing agreement accompanies this application	Indicate, using the tick function that you can comply with the declaration statements as outlined above.

J3: Confidentiality and data protection assurance(s) - data processor

Per the declaration in Section J2, you must show that the Data Processor(s) can provide "sufficient guarantees" to implement appropriate technical and organisational measures to ensure that the data are safe from unforeseen, unintended or malevolent use; and can uphold and protect the rights of the data subject. As part of your assessment of sufficient guarantees, you should have in place a number of due diligence activities.

These may include activities that assess:

- information securities policies and procedures
- cyber risk assessment and compliance
- incident reporting and if they have a history of breaches (notified or not);
- evidence of staff training and awareness of confidentiality and data protection
- procedures for vetting staff
- audits or investigated by the ICO
- contractual management of sub-processors

This list is not exhaustive. You are reminded that should your application for ODR Approval be successful, your organisation will be wholly liable for the conduct of the Data Processor acting under your instruction.

The ODR does not ask that all of this due diligence is presented to the ODR in your application, however, the ODR reserves the right to audit the ongoing due diligence in respect of the instruction of the processor and broader compliance with the terms of an ODR contract.

In this Section J3, you must evidence that:

- all processing will be conducted within the UK or EEA – this includes all cloud hosting arrangements (including backup servers)
- the Data Processor has information security measures in place which provide sufficient guarantees equivalent to, or better than, the DHSC (Department of Health and Social Care)'s data security and information governance requirements – as set out in the Data Security and Protection Toolkit; and
- the Data Processor is registered on the Data Protection Public Register.

J3.1	Territory of processing	Select from the drop down the region(s) the data will be processed by the Data Processor. Where the data will be processed in more than one region or outside of the EEA, select 'other' and specify as applicable. This includes not only where the data will be accessed and worked upon, but also where it is stored and where those servers are physically located. For the avoidance of doubt, this includes the server locations for cloud hosting arrangements.
J3.2	Data Protection Public Register Registration number	Provide the Data Processor's Data Protection Public Register registration number. If your Data Processor is exempt from completing the register or situated outside of the UK, state 'Exempt' and leave your responses to Sections J3.3 and I3.4 blank.
J3.3	Registered organisation name	Provide the name of Data Processor as recorded in the Data Protection Public Register.

		Where this name is substantially different to the response provided in J1.2 it is recommended that you provide an explanation as to why in Section K (eg the trading name and registered name are different for branding purposes). If the Data Processor has a number of records reported in the register and they are unsure which to report, the ICO recommends calling them on 0303 123 1113 to establish which record to rely on.
J3.4	Registration expiration date	Provide the expiry date for the organisation's Data Protection Public Register record (a registration is usually valid for 12 months).
J3.5	Security assurance	Select using the tick boxes one of the three security assurances that demonstrates that the Data Processor has in place appropriate organisation, physical and technical measures to ensure the confidentiality, security, integrity and availability of the data. Descriptions of the possible choices are outlined below, alongside an explanation of the qualified application requirements that must be shared with the ODR to confirm these measures are valid: • **Data Security and Protection Toolkit (DSPT)** (previously called 'Information Governance Toolkit') is the gold standard and a requirement for all health and care services operating under an NHS Contract from April 2018. Where the DSPT is indicated and the reference provided, the ODR will assess the Data Processor has in place 'Standard Met' or 'Standard Exceeded' for the most recent version of the toolkit at the time of review.

		Where partial or non-compliance is revealed, the ODR will require you to demonstrate alternative evidence (either ISO27001:2013 certification or a project-specific SLSP). You can search for the Data Processor's organisation's DSP toolkit code and score on the toolkit website. • **ISO 27001:2013 certification** with alignment of policies, procedures and controls to ISO 27002:2013 and, if utilising third party services ISO 27017:2015, ISO 27018:2014 (where the third party has a multi-tenanted location). You must submit a copy of a valid, in date certificate as part of the application. The certificate must clearly indicate the name and address of the Data Processor. • **A project-specific System Level Security Policy (SLSP)** - you must submit to the ODR a report on how the Data Processor will administer, secure, handle and use the requested data with the technical and physical controls employed to enforce organisation's information governance, security policies and procedures for the lifecycle of the data, including deletion. Due reference should be given to corporate policies. A template is available on request from the ODR that will assist in the formatting of an SLSP.

Section K: Any additional information

K1.1	Any additional information	Stipulate any other information relevant to this project you think the ODR should be aware of.

Section L: Declaration

The declaration statement outlined in Section L requires the chief investigator to acknowledge their responsibilities in applying for ODR Approval and that the information shared with ODR in the application is true, complete and accurate.

It states:

By submitting this application form to the ODR I, the chief investigator, certify:

- the information contained in this application form is true, correct and complete. I understand that any misrepresentations may invalidate my application or lead to a delay in access to data
- I have read the ODR Approval Guidelines, and where applicable, sought assistance from the ODR/subject specific experts in the development of my application
- I have consolidated all accompanying evidence as prompted by this form and the **ODR Approval Guidelines: application requirements**; and
- I understand that where PHE employees make intellectual, scientific and professional contributions to this project, their input will be acknowledged through co-authorship or by recognition as non-author contributor on all publications produced from the data.

In agreeing these statements, the date of declaration must be completed.

L1.1	Date of declaration	You must sign the declaration by adding the date of declaration. This should be within three calendar months of application submission. Should your application be found to be invalid, this declaration will need to be completed again.

Section M: Summary of evidence

The summary of evidence provides you with an indicative list of documents that will need to be submitted to the ODR based on the responses you have provided.

This Section M is populated automatically based on conditional logic that is built into the form's design. However, the ODR strongly recommends that you review the **ODR Approval Guidelines: application requirements** to ensure that you compile all the requisite mandatory or qualified application requirements before submitting your application for ODR Approval.

ODR Approval Guidelines – publication list

Applying for data
Application requirements
- Annex A: completing the ODR data request form
- Annex B: scientific protocol
- Annex C: data specification
- Annex D: privacy notice
- Annex E: lay summary
- Annex F: data linkage (pending publication)
- Annex G: applying the national data opt out
- Annex H: data processors

Cost recovery

Feedback

The ODR welcomes your feedback on the content and format of this document. Please contact ODR@phe.gov.uk.

About Public Health England

Public Health England exists to protect and improve the nation's health and wellbeing, and reduce health inequalities. We do this through world-leading science, research, knowledge and intelligence, advocacy, partnerships and the delivery of specialist public health services. We are an executive agency of the Department of Health and Social Care, and a distinct delivery organisation with operational autonomy. We provide government, local government, the NHS, Parliament, industry and the public with evidence-based professional, scientific and delivery expertise and support.

Public Health England
Wellington House
133-155 Waterloo Road
London SE1 8UG
Tel: 020 7654 8000

www.gov.uk/phe
Twitter: @PHE_uk
www.facebook.com/PublicHealthEngland

Version 2.0

Prepared by: Office for Data Release
For queries relating to this document, please contact: ODR@phe.gov.uk

Published February 2021
PHE gateway number: GW-1876

PHE supports the UN Sustainable Development Goals

SUSTAINABLE DEVELOPMENT GOALS