UK Health Security Agency

UKHSA Data Application Form

Use this form if you are making a new application to access protected UKHSA data.

UKHSA generates, curates and integrates high quality data on infectious diseases and other external public health threats. Access to this data can be acquired subject to the approval of a data application. All applications are rigorously reviewed using an objective, standards-based assessment to ensure:

a) all processing will be fair, lawful, and transparent

b) all processing will be for a specific, explicit, and legitimate purpose(s) and the data will not be processed in a manner that is incompatible with those purposes

c) such purpose(s) for processing the data provides direct and tangible benefits to individuals or the health system, and is expected to deliver a positive social outcome

d) the data requested are necessary and proportionate to fulfilling the purpose(s)

e) all processing will be conducted within safe settings to protect the data from unlawful or unauthorised processing, access, loss, destruction or damage; and

f) compliance with good standards of ethical and research integrity, including public involvement, FAIR data, and Open Science principles

Completing the Data Application Form

The UKHSA data application form is a ‘smart form’ presented in Adobe. It has been configured to use conditional logic to hide and show questions, so that the content of the form is personalised to the circumstances of your project. Based on your responses, the form will highlight the instructions and questions that are specific to your project.

If you do not have an Adobe Reader, you can download it for free.

Before completing the form, you are asked to:

- familiarise yourself with the pre-application guidelines, including Approval Standards
- complete Step 1, by responding to two filter questions on page 3

Submitting your application

The requirements for submitting a valid application are set out in the Approval Standards and Guidelines.

Please complete all relevant fields in the application form and provide all required supporting evidence.

Valid applications must be submitted electronically to odr@phe.gov.uk. It is advised that all evidence is consolidated in a single zip folder, with each document appropriately labelled.

UKHSA will only use the information provided in your application to determine the acceptability and feasibility of your data request. Therefore, you must demonstrate all relevant and prevailing Approval Standards have been met within the application.

Incomplete applications and missing evidence will delay the approval process.

Should your request be rejected, you may amend and resubmit your application.

Processing your data

UKHSA will use the personal information you provide in this form and any supporting evidence to consider your application. Further information on how we collect, hold, and process your information can be found at: https://www.gov.uk/guidance/processing-your-personal-data-for-secondary-purposes.

Step 1. Filter questions

1: Project type

Indicate the type of project you intend to conduct by ticking the relevant box. Select one only.

If one of these broad definitions does not describe your project, select 'other' and provide an alternative description.

- ☐ Research
- ☐ Service Evaluation
- ☐ Clinical Audit
- ☐ Surveillance, emergency planning and response
- ☐ Other

If other, please specify

2: Project type

Select the level of identifiability of the data you are requesting access to.

In circumstance where the application includes the need for both de-personalised and personally identifiable data select, 'Personally identifiable'.

✔	De-personalised	☐	Personally identifiable

3. Prior engagement with UKHSA

Do you have any contacts in UKHSA with whom you have discussed the value or feasibility of this project? If so, provide details.

Step 2: Application form

Section A: Primary applicant

A1: Project Lead/Principal Investigator details

Provide details of the individual who is leading on the project and has overall responsibility for its day-to-day management, outputs, and dissemination of results. This individual will typically be the main point of contact for any formal correspondence. Where the management of this application has been delegated, stipulate the primary point of contact in section A3.

A1.1: Title	
A1.2: First name	
A1.3: Surname	
A1.4: Role / job title	
A1.5: Email address	
A1.6: Work telephone / mobile	

A2: Applicant organisation

Provide the identity and contact details of the substantive organisation of the Project Lead. Include the registered address or if different, the business address any formal correspondence, including contracts, should be addressed.

A2.1: Organisation name	
A2.2: Organisation department	
A2.3: Registered address	Address Line 1
	Address Line 2
	City
	Postcode
A2.4: Organisation type	Other
	If other, please specify

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

Provide the name and contact details of the person designated to serve as the primary contact for this application. Leave blank if this if the person identified in A1.

A3.1: Primary contact name	Main contact name
A3.2: Primary contact email address	Main contact email

A4: Organisational and technical safeguard to process the data

Unless exempt, demonstrate that your organisation has complied with its responsibility under the Data Protection (Charges and Information) Regulations 2018 to share specified information and pay a fee to the Information Commissioner's Office (ICO).

A4.1: Indicate if the Organisation named in A2.1 is exempt under the Data Protection (Charges and Information) Regulations 2018

A4.2: ICO Fee Payers Registration Number	
A4.3: Registered organisation name	
A4.4: Registration expiration date	

Demonstrate that your organisation has in place appropriate organisational, physical, and technical measures in place that protect the availability, usability, consistency, integrity, and security of the data requested.

UKHSA accepts two types of security assurance as evidence:

- a valid Data Security and Protection Toolkit to 'Standard Met' or 'Standard Exceeded'
- a current ISO 27001:2013 certificate issued by an UKAS accredited certification body

A4.5: Organisational and technical assurance (provide one of the following)

☐ Data Security and Protection Toolkit. If selected complete questions A4.6a-c

☑ ISO27001:2013 certificate. If selected complete questions A4.7a-c

DSP toolkit	ISO 27001:2013 certification
A4.6a: ODS code	A4.7a: Certificate number
A4.6b: Latest standard attained	A4.7b: Initial registration date
A4.6c: Version assessed against	A4.7c: Current expiry date

A4.8: Territory of processing of Primary Applicant, where other describe.

If other, please specify

Section B: Co-applicant(s)

In circumstances where the there is a clear and documented agreement between the respective applicants to act as joint data controllers, UKHSA supports collaborative applications, from two or more organisations that intend to operate joint working practices in the management and delivery of the project,

Should the application be favourably reviewed, each named co-applicant will be jointly responsible for the processing controlled within the Data Sharing Contract. It is expected that the Sponsor ensures that there are appropriate policies to effectively govern the activities of the joint working.

B1.1. Is this application is being made by two or more co-applicants?

The contribution of co-applicants should be acknowledged in the 'Co-applicant' form - found in Appendix 1. This form records comparable information on each co-applicant to the information recorded on the primary applicant in section A.

This form should be repeated for each additional co-applicant, and included with the application.

Section C: Project sponsor and funding

C1: 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. Should the application be favourably reviewed, a data sharing contract will be executed with the Sponsor.

Provide details of the Sponsor.

C1.1: Tick if sponsor's name and address is the same as given in A2.1 ☐

C1.2: Sponsor's name

C1.3: Sponsor's address

Address Line 1

Address Line 2

City

Postcode

C2: Funding arrangements

Services attributable to the release of the data for a specific project may be charged. Adequate funding must be in place before an application is submitted. Should your project have more than one funder, document in section I: 'Additional Information.'

C2.1. Tick if the funder's name and address is the same as given in A2.1 ☐

C2.2: Funder name

C2.3: Funder address

Address Line 1

Address Line 2

City

Postcode

United Kingdom

C2.4: Reference(s) assigned by the funder

If you have multiple references please separate them with a comma

Section D: Project

Provide an overview of the conduct of the project, as well as the broader anticipated impact(s) and beneficiaries of your project.

Should your application be successful. the responses provided to questions D2 (lay summary) will be published alongside high level details of your organisation and the data requested in a data uses register to support transparency around the uses of UKHSA data.

D1: Overview

D1.1: EOI reference(s)

D1.2: Project title

D2: Lay summary

Provide a description of the project in plain English (using non-technical language and avoiding jargon, unexplained acronyms and/or abbreviations). All editorial requirements set out in the Approval Standards and Guidelines.

In addition to the lay summary, all applications must be accompanied by a detailed scientific protocol. See the Approval Standards and Guidelines for further information on protocol requirements.

D2.1: Describe the overall aim(s) and objectives of the project.

D2.2: Explain the rationale for why this project is needed, including citing evidence which supports the need for this work.

D2.3: Explain the methods you will use in your project, such as how you will obtain the data, how you will analyse it and how you will draw conclusions. Where the project involves data linkage, the instruction of data processors, profiling and/or automated decision making, this must be described.

D2.4: Describe the anticipated benefit(s) and/or impact(s) of conducting this project to public health or the public good; including all direct/indirect beneficiaries.

D2.5: Specify any intended outputs that will communicate the findings from this project with the beneficiaries identified in D2.4 or other relevant audiences. If you are not intending to publish your outputs, UKHSA may ask you to explain why.

- ☐ Peer reviewed scientific journals
- ☐ Conference presentation
- ☐ Submission to regulatory authority
- ☐ Software products/web tools (open access or restricted)
- ☐ Internal report (publication not intended)
- ☐ Website
- ☐ Press release
- ☐ Other

Where 'other' provide further details of intended outputs in the box below:

D2.6: Provide the URL of any websites that will highlight the conduct of the project or the outputs listed in D2.5. If the project does not operate a website, leave blank.

D3: Patient and/or professional contact

Provide details of any instance where UKHSA data, or data UKHSA data will be linked to, will be used to contact the data subject or a public health/health professional about the data subject. Where a contact exercise will be delivered, you must share all copies of materials that will be used to contact individuals (such as draft letters, emails, or phone scripts).

D3.1: Will this project process UKHSA data to contact members of the public, patients, or service users? If yes, provide details of how the data will be used and accompany your application with copies of the contact materials (such as draft letters or emails).

Yes

D3.2: Will this project process UKHSA data to contact public health or other health care professionals about members the public, patients, or service users? If yes, provide details of how the data will be used and accompany your application with copies of the contact materials (such as draft letters or emails).

D4: Data management and information systems

D4.1: Provide a technical description of how the data will be processed through its lifecycle, up to and including destruction. This must include a description of any the systems, processes and other business operations that will be used when the data is in transit, is stored (including persistent storage) or destroyed. You must also clearly document any transfers of data between co-applicants and/or data processors acting under instruction.

In addition to the technical summary, all applications must be accompanied by a logical data flow diagram to visualise the information flows within the proposed systems, any processes and interaction points between any external and internal parties. See the Approval Standards and Guidelines for further information.

D5: Project timeline

Provide details of the anticipated project timeline. You are advised to take into account the complete data lifecycle, including requirements for retention and archiving, up to and including the deletion of the data.

D5.1: Start date

D5.2: Project duration (months)

Section E: Summary of data requirements

Provide an overview of the data that is necessary and proportionate for the conduct of the project. In addition to the information below, it is a mandatory requirement that all applications must be accompanied by a detailed data specification. See the Approval Standards for further information.

E1: Data specification summary

E1.1 Level of identifiability

✔	**De-personalised**: the data 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 published results (e.g. ethnicity, sex, month and year of birth, admission dates, geographies or other personal characteristics).
	Personally identifiable: the data request includes direct identifiers (e.g. name, address, NHS number, date of birth), free text or is coded (pseudonymised), but would be directly identifiable in the hands of the data recipient (such a cipher that links the study specific number or code back to the real world identifiers, like a medical record number for a hospital). To process personally identifiable data, the applicant(s) must demonstrate processing would be lawful, fair, and transparent.

E1.2: What UKHSA dataset(s) and coverage period(s) do you require access to?

E1.3: What data items/fields do you require?

Provide us with an accompanying file such as an excel document that lists the variables you require and a justification for each variable.

E1.4: State whether your project requires an extract once or whether it relies on periodic updates of the extract. Where the project requires periodic updates, provide details of the frequency needed and why this is necessary to fulfil the Purpose(s). If UKHSA is satisfied with your reasons for updates of data, we may not require you to re-apply each time, however we reserve the right to ask you to do so.

The feasibility of the proposed periodic updates must be agreed with the UKHSA system owner prior to submission of the application.

E2: Other data processed for this project

E2.1: Will any other personally identifiable or de-personalised data not controlled by UKHSA be processed for this project?

If yes, provide the dataset name, level of identifiability of the data, the legal basis for processing (where applicable), and the data controller.

Section F: Integrity and accountability

All projects must be conducted within an ethical framework.

Provide details of any material ethical issues that that may arise in the conduct of the project or from its outputs; identify how such issues will be mitigated to ensure high standards of ethical practice are upheld throughout the project life course. This should include issues arising from but not limited to:

- managing any adverse effect on the data subject's personal, social, or economic well-being, including how the project will safeguard the rights, safety, dignity and well-being of the data subject.
- managing departures from usual care or introducing variation between groups of individuals
- managing diminished and/or Gillick competency
- data management practices to prevent breaches to confidentiality
- data management practices to uphold privacy and compliance with data protection
- ensuring that the project yields appropriate results through its design, and the valid and reliable assessment of findings
- ensuring that all findings are transparent and accessible, so knowledge is shared and developed
- real or perceived conflicts of interest that could compromise the project, including commercial interests and restrictions on the freedom of the Applicant(s). All commercial interests in the delivery of the project must be declared

F1.1: Describe any material ethical issues and mitigations that will be deployed , which have been identified in the design or conduct of the project, including pertaining to any planned outputs.

F1.2: Has the project been discussed or are there plans to discuss the project with those likely to be involved, including potential participants or those who may represent their views? If so, describe who and in what circumstance?

F2: Independent ethical oversight

Where personally identifiable data is requested for the conduct of research on a population sampled because of their current or historic relationship with the NHS, applicants must evidence NHS REC Favourable Opinion has been obtained. For other populations, details of ethical oversight by the Sponsor should be supplied.

Where the data requested is de-personalised, you are asked to evidence the Sponsor has reviewed the application and appropriately considered all ethical implications.

F2.1: Type(s) of ethical approval obtained	
F2.2: Ethics committee name	
F2.3: Ethics committee reference(s)	

F3: Research databases and access procedures

Organisations responsible for the management of research databases may apply for review of their governance and sub-licensing arrangements to enable the sub-licensing of UKHSA data to third parties.

For such arrangements to be considered, applicants must accompany their application with evidence that describes: (1) the data management plan for the research database, (2) the access policy and assessment process (including risk assessment), (3) the contractual controls that will be used, including a copy of the sub-licence and (4) how they intend to demonstrate the uses of the data to the public (such as a data uses register).

F3.1: Will the data requested be curated for a research database?	

F3.2: Describe the proposed management of the research database

Section G: Lawful processing

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). This duty extends beyond death and is distinct from obligations under data protection legislation.

However this duty is not absolute and confidential information or confidential patient information (collectively referred to as personally identifiable data in this form) may be lawfully disclosed when there are valid grounds to set this duty aside and project purpose cannot be met with either open data or de-personalised data.

If your application includes the processing of personally identifiable data, you must include evidence of how the duty of confidentiality has been set aside and demonstrate to the UKHSA:

- the organisation(s), including UKHSA, 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 UKHSA, 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

G1.1: Select the applicable exemption to the common law duty of confidentiality. Select 'other' if more than one exemption applies:

Your response to G1.1 will prompt additional questions about the selected exemption or prompt you to include within your application specific supporting evidence.

Direct care

To demonstrate processing will be legal, ethical, and strictly for direct care purposes, provide the name of your organisation's Caldicott Guardian and accompany your application with a signed letter that demonstrates their support for this project. The letter must be in line with the Approval Standards and the time parameters set.

G1.2: Caldicott Guardian name

G1.3: I understand I must accompany my application with evidence of Caldicott Guardian approval for a direct care activity that involves the processing of data on my patients

Explicit informed consent

Where the individual has capacity and has provided their explicit, informed consent to the processing described in this application, you must accompany your application with blank copies of the consent form (including version history) and any participant information sheets.

G1.4: I understand I must accompany my application with evidence of explicit informed consent

Statutory exemption

G1.5: Select the statutory exemption applicable to the processing of personally identifiable data for this project

G1.6: Describe the processing operations in scope of exemption, including but not limited to the affected population, purpose, restrictions, and retention of the data.

Regulation 2, 3 or 5, Health Services (Control of Patient Information) Regulations

Where Regulation 2, 3 or 5, Health Services (Control of Patient Information) Regulations 2002 is selected as a 'statutory exemption', you must also provide details of the approval granted by the Secretary of State or Confidentiality Advisory Group (CAG). Your application must be accompanied by 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.

G1.6: CAG/UKHSA reference:

G1.7: Date of next renewal:

G2: Legal gateway (data protection)

If you are requesting to process personally identifiable data, you must demonstrate the applicant(s) has a lawful basis to do under Article 6 and Article 9 (UK GDPR). This is in addition to a common law exemption. The ICO webtool might help you determine which condition is right for your project.

G2.1: Article 6 lawful basis for processing personal data

- ☐ 1(a): Consent
- ☐ 1(b): Contract
- ☐ 1(c): Compliance with a legal obligation
- ☐ 1(d): Vital interests
- ☐ 1(e): Public task
- ☐ 1(f): Legitimate interests

G2.2: Article 9 condition for processing special category personal data

- ☐ 2(a): Explicit consent
- ☐ 2(b): Obligations/rights of the controller / data subject
- ☐ 2(c): Vital interests
- ☐ 2(d): Legitimate activities with safeguards
- ☐ 2(e): Made public by the data subject
- ☐ 2(f): Legal claims
- ☐ 2(g): Substantial public interest
- ☐ 2(h): Preventative or occupational medicine
- ☐ 2(i): Public interest in the area of public health
- ☐ 2(j): Public interest, scientific or historical research

G2.3: Provide justification for the selection of the lawful basis and condition(s) in questions G2.1 and G2.2, drawing on any evidence material to the decision making (such as a legitimate interest test or the relevant task, function or power which is clearly set out in law).

G3: Transparency

In addition to demonstrating lawful processing, applicants wishing to process personally identifiable data must demonstrate that they comply with transparency and accountability principles of UK GDPR. You must include a project-specific privacy notice which adheres to the Approval Standards and clearly articulates the role of UKHSA as a source of data, or as responsible for any other processing operations.

G3.1: Describe how the project-specific privacy notice is/will be made available to the data subject(s), including (a) the mode(s) of communication used/to be used and where the notice will be made available electronically, (b) the URL of the published notice.

Section H: Data processor(s) acting under instruction

All fields in this section are mandatory if a third party (a person, public authority, agency or other body) will act on the documented instructions of the controller to process the data and 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’ can be found in the UK GDPR Article 4(8).

For each processor (or their respective sub-processor(s)), a fully executed data processing agreement must accompany your application. The data processing agreement must comply with the obligations prescribed in Article 28 – 36 of UK GDPR.

You must ensure that the logical data flow diagram details any processing operations between the data controller and the processor(s) acting under instruction.

H1.1: Are you engaging one or more data processors to process the data requested?

Data Processor 1

H1.2: Data processor name

H1.3: Registered address

Address Line 1

Address Line 2

City

Postcode

United Kingdom

H1.4: State the written instruction provided by the Applicant(s) to Data Processor 1 for the processing of UKHSA data.

H2: Data Processing Agreement

You must fully execute a data processing agreement (a type of contract) with each Data Processor. This contract must bind the data processor to the data controller in respect of its processing activities, as specified in the application.

H3: Organisational and technical assurances of the data processor

H3.1: ICO Fee Payers Registration Number

H3.2: Registered organisation name

H3.3: Registration expiration date

H3.4: Organisational and technical assurance (provide one of the following)

Demonstrate that the data processor has appropriate technical and organisational measures to protect the confidentiality, integrity and availability of the data requested (including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage).

UKHSA accepts two types of security assurance as evidence:

- a valid Data Security and Protection Toolkit to 'Standard Met' or 'Standard Exceeded'
- a current ISO 27001:2013 certificate issued by an UKAS accredited certification body

☑ Data Security and Protection Toolkit (DSP Toolkit), complete G3.5a-c

☐ ISO 27001:2013 certification, complete G3.6a-c

DSP toolkit	ISO 27001:2013 certification
H3.5a: ODS code	H3.6a: Certificate number
H3.5b: Latest standard attained	H3.6b: Initial registration date
H3.5c: Version assessed against	H3.6c: Current expiry date

H3.7: Territory of processing, where other describe:

If other, please specify

H4: Other Data Processor(s)

Where more than one data processor is to be instructed to process the data (entirely or in part), you must complete a 'Data Processor' form (Appendix 2) for each distinct entity.

Section I: Any additional information

This section allows you the opportunity to share any other relevant information with UKHSA in support of your application.

Section J: Supporting documents

Your application will not be complete unless all the relevant supporting evidence are submitted together.

Please ensure you submit all the relevant documents that you want the UKHSA to consider when assessing your application.

For each document, identify the document name and version.

Document name	Version

Declaration

By completing the declaration below, I, the primary applicant 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 Approval Standards and associated Guidelines, and where applicable, sought assistance from the subject specific experts in the development of my application
- I have consolidated all accompanying evidence as prompted by this form or the Approval Standards and Guidelines
- I understand that any changes to this application while it is in review will require this application to be withdrawn and resubmitted

Signed:

Date:

Save Application

Evidence checklist

Mandatory requirements

- [x] Scientific protocol
- [x] Data specification
- [x] Logical data flow diagram

Qualified requirements

- [ ] Any contact exercise materials
- [ ] Attach a letter of support for the project from your Caldicott Guardian
- [ ] Attach a blank copy of the consent form(s) and participant information materials
- [ ] Attach co-applicant form(s)
- [ ] Attach all supporting evidence of a statutory exemption to common law*
- [ ] Attach REC approval materials
- [ ] Attach a copy of your organisation's ISO 27001:2013 certificate
- [ ] Attach a copy of the data processor's ISO 27001:2013 certificate
- [ ] Attach a copy of the project-specific privacy notice
- [ ] Attach the executed data processing agreement(s) with the data processor(s)
- [ ] Attach evidence detailing governance arrangement of proposed research database

*Please note, this checklist assumes that the project relies upon one common law basis to process personally identifiable data. If the project relies on a mixed model (for example consent and a statutory exemption) contact UKHSA to confirm you understand all qualified requirements before submission.