**Health and care:**

**Template data protection impact assessment (DPIA)**

**Background**

A [data protection impact assessment (DPIA)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) will help you to identify and mitigate potential data protection risks to an acceptable level before using or sharing (processing) data that identifies individuals (personal data).

A DPIA will also help you meet a number of data protection legal requirements including:

* [Data protection by design](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/%22%20%5Cl%20%22%3A~%3Atext%3DExternal%20link-%2CWhat%20is%20data%20protection%20by%20design%3F%2Cand%20then%20throughout%20the%20lifecycle.) - privacy and data protection issues must be considered at the start, or in the design phase, of a new system, product or process, then continuously while it exists.

* [Accountability](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/) - your organisation is responsible for showing how it complies with data protection laws.

* [Transparency](https://ico.org.uk/for-organisations/accountability-framework/transparency/) - personal data must be used and shared in a transparent way.

* [Security](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/) - adequate measures need to be in place to protect data. This can range from policies and procedures to technical security measures such as encryption of data.

DPIAs are mandatory when there is a high risk to individuals, such as when using the health and care data of a large number of people. However, health and care organisations are strongly advised to complete a DPIA when using and sharing personal data in a new or substantially changed way.

A DPIA involves a risk assessment. If a high-level risk remains after applying mitigations, then you must consult with the Information Commissioner’s Office (ICO) for further advice before starting to collect, use or share the data.

A DPIA is a live document - you must update it if there are any changes to:

* the purpose - why you are proposing to use or share personal data
* the manner - how you will use or share the data
* who is involved - the organisations using and sharing personal data

This is a template DPIA for health and care organisations. We encourage organisations to adopt it. The template is written so that it is easy to use without needing expertise in data protection. It is the responsibility of the organisation which is deciding on why and how the data is being used and shared (known as the controller), to ensure that the DPIA is completed appropriately.

In the case of research, the sponsor is the controller. See Health Research Authority (HRA) guidance on [controllers](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-controllers-and-personal-data-health-and-care-research-context/) and research. HRA guidance on [DPIAs](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-privacy-impact-assessments/#:~:text=For%20personal%20data%20processed%20for%20the%20purpose%20of,of%20research%20are%20the%20responsibility%20of%20the%20sponsor.) sets out that sponsors should complete a DPIA for the broad range of health and care research they sponsor and ensure that individual research projects are designed in accordance with the DPIA. Individual DPIAs should only need to be completed for individual research projects that involve activities beyond the generic research DPIA. Where the study deviates from the established processes (for example, where it is intended that a project uses a new technology for the processing of personal data, or requires that safeguards set out in standing policies cannot be applied), the sponsor should consider whether a study specific DPIA is appropriate to address the level of risk, or whether updating existing DPIA(s) will be sufficient. Research sites should not complete DPIAs or request researchers to complete individual DPIAs for each research project, as they are not the controller.

Text in [square brackets and green highlight] is guidance only and should be removed for the final version.

Text in yellow highlight is sample wording and should be edited according to your local circumstances.

Table of contents

[Data protection impact assessment (DPIA) 4](#_Toc140216755)

[SECTION 1 – Screening questions 5](#_Toc140216756)

[SECTION 2 – Why do you need the data? 6](#_Toc140216757)

[SECTION 3 – What data do you want to use or share? 6](#_Toc140216758)

[SECTION 4 – Where will data flow? 10](#_Toc140216759)

[SECTION 5 – Is the intended use of the data lawful? 11](#_Toc140216760)

[SECTION 6 – How are you keeping the data secure? 13](#_Toc140216761)

[SECTION 7 – How long are you keeping the data and what will happen to it after that time? 16](#_Toc140216762)

[SECTION 8 – How are people’s rights and choices being met? 16](#_Toc140216763)

[SECTION 9 – Which organisations are involved? 20](#_Toc140216764)

[SECTION 10 – What data protections are there and what mitigations will you put in place? 22](#_Toc140216765)

[SECTION 11 – Review and sign-off 24](#_Toc140216766)

# Data protection impact assessment (DPIA)

|  |  |
| --- | --- |
| **Data protection impact assessment (DPIA) title:** | [add the name of the initiative, programme, project or process] |
| **DPIA reference number:** | [delete this row if not applicable] |
| **[Please provide any other reference numbers as needed]** |  |

## SECTION 1 – Screening questions

1. **Do you need to do a DPIA?**

[Consider whether you need to do a DPIA.

If a DPIA is needed, provide a short explanation of why. Reasons may include:

* you will be using and sharing data which needs more protections because it is sensitive (special category data). This includes identifiable health and care data
* you are implementing a new technology
* there are high risks to the processing (for example, data is being shared outside of the UK without adequate safeguards in place)
* large numbers of people will be affected, for example, converting thousands of paper records into digital format.

If you think there is a low risk to individuals, you do not need to complete a DPIA. However, if you feel there is a need to consider the risks further or document your reasons for not completing a DPIA, set that out here, complete questions [1a](#Page03_Section01a) and [1b](#Page03_Section01b) then [skip to sections 10](#Page25_Section10) and [11](#Page27_Section11) - the other sections do not need completing. Examples of where this may apply is where the processing is not high risk because the project involves a small dataset and the data is pseudonymised with the re-identification key held separately, or only staff names and email addresses are to be used.

Note that research sponsors are expected to complete a DPIA for the overall purpose of health and care research. Individual DPIAs for each research project are not required, unless the project will not fall within the arrangements set out in the generic research DPIA.]

* 1. **Summary of how data will be used and shared**

[For example, data is collected from our services, and aggregated. We will then share the aggregated data with Company A to gain improved insights to enable us to improve service provision.]

* 1. **Description of the data**

[Put an [x]  next to all that apply.]

|  |
| --- |
|[ ]  Personal data [individuals can be identified] |
|[ ]  Pseudonymised data [identifiers, for example name or NHS number, are replaced with a unique number or code (a pseudonym)] |
|[ ]  Anonymous data [not identifiable, for example trends or statistics] |

[Provide details of any pseudonymised data, including which organisation holds the key that allows the data to be re-identified. Describe the way the data has been anonymised and whether it is anonymised in the hands of those you will be sending it to. This should include detail of whether the data has been aggregated with small numbers suppressed. For example, if only two people in the area have a rare condition it could be possible to identify them so this data would need to be removed.

Where a DPIA is not required but you are documenting your decision and the risks, [skip to section 10](#Page25_Section10) and [11](#Page27_Section11) – the other sections do not need completing.]

## SECTION 2 – Why do you need the data?

1. **What are the purposes for using or sharing the data?**

[Give a high-level description of the purpose(s) for example, the purpose is to look at overall health of the people in our area to ensure we have the right services in the right places.

Multiple related purposes are acceptable for one DPIA, but where these are unrelated, a separate DPIA should be completed for each one.]

1. **What are the benefits of using or sharing the data?**

[Set out the benefits of using and sharing the data. This should cover the benefits to the individuals whose data is being used, the benefits to the organisation(s), the wider public, or other groups if applicable.

For example, installing a new telephony system will help deliver a better service to patients because they will be able to get through to the organisation faster and the organisation will also have an audit trail to ensure better management.]

## SECTION 3 – What data do you want to use or share?

1. **Can you use anonymous data for your purposes? If not, explain why.**

[Put an [x]  next to the one that applies.]

|  |
| --- |
|[ ]  Yes  |
|[ ]  No  |
|[ ]  Unsure [try to provide an explanation of what you think] |

[Anonymous data does not identify individuals, for example trends or statistics. You should use anonymous data whenever possible. This may not always be possible, for example if your intended use of data is to provide individual care.

For example, we intend to use analytical tools to identify which individuals in our local population are at high risk of diabetes so that their GP can offer them early intervention treatments.]

1. **Which types of personal data do you need to use and why?**

[Put an [x]  next to all that apply.]

|  |  |  |
| --- | --- | --- |
|[ ]  Forename |[ ]  Physical description, for example height |[ ]  Photograph / picture of people |
|[ ]  Surname |[ ]  Phone number | [ ] [ ] [ ]  | Location data e.g.* IP address
* Other [please state]
 |
|[ ]  Address |[ ]  Email address |[ ]  Audio recordings |
|[ ]  Postcode full |[ ]  GP details |[ ]  Video recordings |
|[ ]  Postcode partial | [ ]  | Legal representative name (personal representative) |[ ]  Other [please state] |
|[ ]  Date of birth |[ ]  NHS number |[ ]  None |
|[ ]  Age | [ ]  | National insurance number |  |  |
|[ ]  Gender | [ ]  | Other numerical identifier [please state] |  |  |

[State why you need this personal data and embed a description of the dataset if available.]

1. **Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Data that relates to criminal offences is also considered particularly sensitive. Which types of sensitive data do you need to use or share?**

[Put an [x]  next to all that apply.]

|  |  |
| --- | --- |
| **Type of data**  | **Reason why this is needed (leave blank if not applicable)** |
|[ ]  Information relating to an individual’s physical or mental health or condition, for example information from health and care records  | [be specific where possible, for example diagnostic data, care plans, medication details, test results, vitals readings are needed in order to…] |
|[ ]  Biometric information in order to uniquely identify an individual, for example facial recognition  |  |
|[ ]  Genetic data, for example details about a DNA sample taken as part of a genetic clinical service |  |
|[ ]  Information relating to an individual’s sexual life or sexual orientation |  |
| [ ]  | Racial or ethnic origin |  |
| [ ]  | Political opinions |  |
| [ ]  | Religious or philosophical beliefs |  |
|[ ]  Trade union membership |  |
|[ ]  Information relating to criminal or suspected criminal offences |  |
|[ ]  None of the above |  |

[Embed a description of the dataset if available, unless special category data is covered in your embedded description in response to [question 5](#Page06_Section03_Question05)]

1. **Who are the individuals that can be identified from the data?**

[Put an [x]  next to all that apply.]

|  |
| --- |
|[ ]  Patients or service users |
|[ ]  Carers |
|[ ]  Staff |
|[ ]  Wider workforce |
|[ ]  Visitors |
|[ ]  Members of the public |
|[ ]  Other [please state] |

1. **Where will your data come from?**

[This may be directly from the individuals or from a third party, such as another health and care organisation. Note this should be a brief summary - full details of the data flows are covered in [section 4](#Page10_Section04).]

1. **Will you be linking any data together?**

[Put an [x]  next to the one that applies.]

|  |
| --- |
|[ ]  Yes [provide an explanation below and then [go to question 9a](#Page08_Section03_Question09a)] |
|[ ]  No [skip to [question 10](#Page10_Section04_Question10)] |
|[ ]  Unsure [try to provide an explanation of what you think then [go to question 9a](#Page08_Section03_Question09a)] |

[For example, combining data received from a local authority with data from NHS organisations. If so, provide details of why this is necessary, for example local authority data needs to be linked with data from local NHS organisations so that we can understand admissions to care homes from different organisations.]

* 1. **Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?**

[Put an [x]  next to the one that applies.]

|  |
| --- |
|[ ]  Yes [provide details below] |
|[ ]  No |
|[ ]  Unsure [try to provide details below] |

[Standalone datasets may not be identifiable when all identifiers, such as NHS number, are replaced with a code. However, if you link the dataset with other data, it could become identifiable data. For example, if once linked, you could look up which code is associated with which NHS number. You will need to factor this in when you complete [section 5](#Page12_Section05).]

##

## SECTION 4 – Where will data flow?

1. **Describe the flows of data.**

[You can use this table - some examples have been provided. Alternatively, you can use a data flow map or a written description of the data flow. A simple example of a map could be: patient - inputs blood pressure reading into app X - reading uploaded into patient’s hospital record.]

|  |  |  |  |
| --- | --- | --- | --- |
| **Data flow name** | **Going from** | **Going to** | **Data description** |
| Admission data | Hospital | Local authority | Demographic data of patients admitted to hospital from local authority commissioned care homes |
| Diabetic data | Ambulance Trust | Hospital | Demographic data of patients with diabetes requiring an ambulance |

1. **Confirm that your organisation’s information asset register (IAR), record of processing activities (ROPA) or your combined information assets and flows register (IAFR) has been updated with the flows described above.**

[Put an [x]  next to the one that applies.]

|  |
| --- |
|[ ]  Yes |
|[ ]  No |
|[ ]  Unsure [add as a risk in [section 10](#Page25_Section10) with an action to find out]  |

[Your organisation is required to keep a record of the types of data processing it undertakes and any information assets it holds. The template [Information Asset and Flows Register (IAFR)](https://transform.england.nhs.uk/information-governance/guidance/universal-ig-templates-faqs/) allows you to record both of these in one register. Alternatively, you can record them separately, with types of data processing recorded in a ROPA and information assets recorded in an IAR.]

1. **Will any data be shared outside of the UK?**

[Put an [x]  next to the one that applies.]

|  |
| --- |
|[ ]  Yes [[go to question 12a](#Page10_Section04_Question12a)] |
|[ ]  No [[skip to question 13](#Page12_Section05_Question13)] |
|[ ]  Unsure [add as a risk in [section 10](#Page25_Section10) with an action to find out then [skip to question 13](#Page12_Section05_Question13)] |

* 1. **If yes, give details, including any safeguards or measures put in place to protect the data whilst outside of the UK.**

[An example of a safeguard is an up to date international data transfer agreement ([IDTA](https://ico.org.uk/media/for-organisations/documents/4019536/idta.docx)). This should be included in your contract with the overseas organisation. For countries without [UK adequacy in place](https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers), further checks on the organisation must be made before providing them access to data to ensure the data will be handled appropriately.]

## SECTION 5 – Is the intended use of the data lawful?

[You should consider seeking advice to help you complete this section if you are not an IG professional.]

1. **Under Article 6 of the UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?**

[The list below contains the most likely conditions applicable to health and care services. Put an [x]  next to the one that applies. If a different lawful basis applies for a different party, clearly indicate which lawful basis applies to which party by adding in brackets after the selected lawful basis which party it applies to e.g.

[x]  e) **We need it to perform a public task** (GP practice)]

|  |
| --- |
|[ ]  (a) **We have** [**consent**](https://transform.england.nhs.uk/information-governance/guidance/consent-and-confidential-patient-information/) [this must be freely given, specific, informed and unambiguous. It is not appropriate to rely on consent for individual care or research, even if you have obtained consent for other reasons, but is likely to be needed for the use of cookies on a website] |
|[ ]  (b) **We have a contractual obligation** [between a person and a service, such as a service user and privately funded care home] |
|[ ]  (c) **We have a legal obligation** [the law requires us to do this, for example where NHS England or the courts use their powers to require the data. See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.] |
|[ ]  (e) **We need it to perform a public task** [a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake particular activities. See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care. This is mostly likely to be relevant for the provision of NHS and social care services regulated by the CQC. See [HRA guidance on legal basis](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/legal-basis-processing-data/) for processing data for research] |
|[ ]  (f) **We have a legitimate interest** [for example, a private care provider making attempts to resolve an outstanding debt for one of its service users. This cannot be relied on by public bodies in the performance of their tasks.] |
|[ ]  **Other** [please state] |

1. **If you have indicated in question 6 that you are using special category data, what is your lawful basis under Article 9 of the UK GDPR?**

[The list below contains the most likely conditions applicable to health and care services. Put an [x]  next to the one that applies.]

|  |
| --- |
|[ ]  (b) **We need it to comply with our legal obligations for employment** [for example, to check a person’s eligibility to work in the NHS or a local authority. See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.] |
|[ ]  (f) **We need it for legal claims, to seek legal advice or judicial acts** [the information is required to exercise, enforce or defend a legal right or claim, for example a person bringing litigation against a health or care organisation.] |
|[ ]  (g) **We need to comply with our legal obligations to provide information where there is a** [**substantial public interest**](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/)**, as set out in** [**this list**](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/) [for example, safeguarding of children and individuals at risk.] |
|[ ]  (h) **We need it to comply with our legal obligations to provide or manage health or social care services** [providing health and care to a person, or ensuring health and care systems function to enable care to be provided. See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.] |
|[ ]  (i) **We need it to comply with our legal obligations for public health** [using and sharing information is necessary to deal with threats to public health, or to take action in response to a public health emergency (such as a vaccination programme). See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.] |
|[ ]  (j) **We need it for archiving, research and statistics where this is in the public interest** [for example, health and care research, with relevant safeguards in place for the use of the participant’s health and care information. See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care. See [HRA guidance on legal basis](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/legal-basis-processing-data/) for processing data for research. Processing must be in the public interest to rely on this lawful basis.] |
|[ ]  **Other** [please state] |
|[ ]  **Not applicable** [the use of special category data is not proposed] |

1. **What is your legal basis for using and sharing this health and care data under the common law duty of confidentiality?**

[The common law duty of confidentiality says that health and care information about a person cannot be disclosed without that person’s consent. Implied consent can be used when sharing relevant information with those who are directly involved in providing care to an individual. Explicit consent is normally required for purposes beyond individual care unless one of the other conditions set out below applies, for example you have section 251 support.]

[Put an [x]  next to the one that applies.]

|  |  |
| --- | --- |
| [ ]  | [**Implied consent**](https://transform.england.nhs.uk/information-governance/guidance/consent-and-confidential-patient-information/) [for individual care or local clinical or care audits. [Skip to question 16](#Page15_Section06_Question16)] |
| [ ]  | [**Explicit consent**](https://transform.england.nhs.uk/information-governance/guidance/consent-and-confidential-patient-information/) [a very clear and specific statement of consent. [Go to question 15a](#Page14_Section05_Question15a)] |
| [ ]  | **Section 251 support** [this means you have support from the Secretary of State for Health and Care or the HRA following an application to the [Confidentiality Advisory Group](https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/guidance-cag-applicants/) (CAG). CAG must be satisfied that it isn’t possible or practical to seek consent. [Go to question 15a](#Page14_Section05_Question15a)] |
| [ ]  | **Legal requirement** [this includes where NHS England has directed an organisation to share the data using its legal powers. State the legal requirement in the further information section. [Go to question 15a](#Page14_Section05_Question15a)] |
| [ ]  | **Overriding public interest** [for example to prevent or detect a serious crime or to prevent serious harm to another person. The justification to disclose must be balanced against the public interest in maintaining public confidence in health and care services. Routine use of this is extremely rare in health and care, as it usually applies to individual cases where decisions are made to share data. [Go to question 15a](#Page14_Section05_Question15a)] |
| [ ]  | **Not applicable** [you are not proposing to use identifiable health and care data. [Skip to question 16](#Page15_Section06_Question16)] |

* 1. **Please provide further information or evidence.**

[Provide evidence as follows depending on your selection in [question 15](#Page13_Section05_Question15)]

* A record of the explicit consent is stored in ….
* The CAG reference number is…

[for research the DPIA should cover multiple projects, so signpost to the sponsor’s list of research projects with relevant CAG reference numbers]

* The legal requirement is…

[for example directed by NHS England under the Health and Social Care Act 2012]

* The overriding public interest justification we are relying upon is…

## SECTION 6 – How are you keeping the data secure?

1. **Are you collecting information?**

[Put an [x]  next to the one that applies.]

|  |  |
| --- | --- |
| [ ]  | Yes [[go to question 16a](#Page15_Section06_Question16a)] |
| [ ]  | No [[skip to question 17](#Page15_Section06_Question17)] |

* 1. **How is the data being collected?**

[You should describe the method for the collection, for example it is collected by a team going through records and extracting relevant information.]

1. **Are you storing information?**

[Put an [x]  next to the one that applies.]

|  |  |
| --- | --- |
| [ ]  | Yes [[go to question 17a](#Page15_Section06_Question17a)] |
| [ ]  | No [[skip to question 18](#Page15_Section06_Question18)] |

* 1. **How will information be stored?**

[Put an [ ]  next to all that apply.]

|  |  |
| --- | --- |
| **Storage location** | **Details (leave blank if not applicable)** |
| [ ]  | Physical storage, for example filing cabinets, archive rooms etc | [provide details including whether the facility is operated by your organisation or a third party] |
| [ ]  | Local organisation servers | [provide details] |
| [ ]  | Cloud storage | [provide details including whether the facility is operated by your organisation or a third party] |
| [ ]  | Other | [please state] |

1. **Are you transferring information?**

[Put an [x]  next to the one that applies.]

|  |  |
| --- | --- |
| [ ]  | Yes [[go to question 18a](#Page15_Section06_Question18a)] |
| [ ]  | No [[skip to question 19](#Page16_Section06_Question19)] |

* 1. **How will information be transferred?**

[For example, will the information be physically moved as required, sent electronically by email, or uploaded into a shared system. Provide details of security measures to ensure the transfer is secure, for example using secure email (such as NHSmail).]

1. **How will you ensure that information is safe and secure?**

[You need to have measures in place to ensure that the data is safe and it won’t be used, either on purpose or accidentally, in ways that are unlawful. The measures needed will be dependent upon, and proportionate to, the data which is being used.]

 [Put an [x]  next to all that apply.]

|  |  |
| --- | --- |
| **Security measure** | **Details (leave blank if not applicable)** |
| [ ]  | Encryption | [specify the level of encryption, such as AES 256] |
| [ ]  | Password protection |  |
| [ ]  | Role based access controls (RBAC) | [where users only have access to the data held digitally which is needed for their role (this includes setting folder permissions)] |
| [ ]  | Restricted physical access | [where access to personal data is restricted to a small number of people, such as access cards or keys to a restricted area] |
| [ ]  | Business continuity plans |  |
| [ ]  | Security policies | [embed these] |
| [ ]  | Other | [please state] |

1. **How will you ensure the information will not be used for any other purposes beyond those set out in** [**question 2**](#Page07_Section02_Question02)**?**

Specify the measures below which will be used to limit the purposes the data is used for.

[Put an [x]  next to all that apply and provide details.]

|  |  |
| --- | --- |
| **Security measure** | **Details (leave blank if not applicable)** |
| [ ]  | Contract | [a legally binding contract] |
| [ ]  | Data processing agreement | [this sets out the arrangements between a controller and processor and is legally binding] |
| [ ]  | Data sharing agreement | [this sets out the arrangements for sharing data between the organisations involved – it may or may not be legally binding depending on the content] |
| [ ]  | [Data sharing and processing agreement (DSPA)](https://transform.england.nhs.uk/information-governance/guidance/universal-ig-templates-faqs/) | [where appropriately completed, this is a legally binding agreement that sets out the arrangements for processing and/or sharing data, and/or joint controller arrangements] |
| [ ]  | Audit | [provide details, for example there will be an audit trail of those who access health and care records, which is reviewed monthly] |
| [ ]  | Staff training |  |
| [ ]  | Other  | [please state] |

## SECTION 7 – How long are you keeping the data and what will happen to it after that time?

1. **How long are you planning to use the data for?**

We intend to start using the data on [add date] and will finish using the data on [add the contract/project/programme end date or indicate if it is ongoing.]

1. **How long do you intend to keep the data?**

[The time you keep the data for may differ from the period of time you intend to use the data, for example adult health records need to be kept for a minimum of 8 years from the time they were last used. The [Records Management Code of Practice](https://transform.england.nhs.uk/information-governance/guidance/records-management-code/) sets out the retention period for health and care records. Appendix 2 of the Code also includes guidance about setting a retention period for a record not covered in the retention table of the Code.]

1. **What will happen to the data at the end of this period?**

[Put an [x]  next to all that apply.]

|  |  |
| --- | --- |
| **Action** | **Details (leave blank if not applicable)** |
| [ ]  | Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction) | [provide details of who will do this] |
| [ ]  | Permanent preservation by transferring the data to a Place of Deposit run by the National Archives | [provide details of who will do this] |
| [ ]  | Transfer to another organisation | [provide details] |
| [ ]  | Extension to retention period  | [with approved justification] |
| [ ]  | It will be anonymised and kept | [provide details of how this will be done and by who] |
| [ ]  | The controller(s) will manage as it is held by them |  |
| [ ]  | Other | [please state. For research, explain the exemptions applicable to research. Explain the safeguards as set out in [HRA guidance on safeguards](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/safeguards/)] |

[The [Records Management Code of Practice](https://transform.england.nhs.uk/information-governance/guidance/records-management-code/) provides detail about what happens once a retention period has been reached.]

## SECTION 8 – How are people’s rights and choices being met?

1. **How will you comply with the following individual rights (where they apply)?**

[For joint controllers, indicate anything you have agreed, such as designating one controller as a point of contact for patients and service users (data subjects).

These rights will not always apply so you should review each one to see if it applies. In particular, some rights do not apply when data is being used for research purposes. The HRA has published guidance on [research exemptions](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/data-subject-rights-and-research-exemptions/).]

|  |  |
| --- | --- |
| **Individual right** | **How you will comply (or state *not applicable* if the right does not apply)** |
| **The right to be informed** The right to be informed about the collection and use of personal data. |  | We have assessed how we should inform individuals about the use of data for [state initiative/project/programme]. We consider the communications methods below meet this obligation because [add reasons to justify your decision][Put an [x]  next to all that apply.] |
| [ ]  | Privacy notice(s) for all relevant organisations [provide a link or describe where it will be displayed and embed a copy] |
| [ ]  | Information leaflets |
| [ ]  | Posters |
| [ ]  | Letters |
| [ ]  | Emails |
| [ ]  | Texts |
| [ ]  | Social media campaign |
| [ ]  | DPIA published (best practice rather than requirement) |
| [ ]  | Other [please state] |
| [ ]  | Not applicable  |
| **The right of access**The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request.  |  |
| **The right to rectification**The right to have inaccurate personal data rectified or completed if it is incomplete. |  |
| **The right to erasure** The right to have personal data erased, if applicable. [This will not apply if you have selected legal obligation, public task or legal claims in [question 13](#Page12_Section05_Question13), or if you have selected health and care services, public health or archiving, research or statistical purposes in [question 14](#Page12_Section05_Question14).] |  |
| **The right to restrict processing** The right to limit how their data is used, if applicable.[For example, that it can be held by the organisation, but restrictions placed on how it is used. This is unlikely to apply to health and care organisations.] |  |
| **The right to data portability** The right to obtain and re-use their personal data, if applicable.[This only applies where you are processing under UK GDPR consent, or for the performance of a contract; and you are carrying out the processing by automated means, therefore excluding paper files.] |  |
| **The right to object**The right to object to the use and sharing of personal data, if applicable.[This applies where you are carrying out a task in the public interest or for your legitimate interests, but there are exceptions. It is unlikely that an objection would be upheld where the data is processed for individual care, but each request must be considered on a case-by-case basis. However, it is important to note that there are other routes in which an individual can raise an objection to processing.] |  |

1. **Will the national data opt-out need to be applied?**

[Put an [x]  next to the one that applies.]

|  |  |
| --- | --- |
| [ ]  | Yes [provide details of how this is applied] |
| [ ]  | No [provide details of why this is not applicable] |
| [ ]  | Unsure [add as a risk in [section 10](#Page25_Section10) with an action to find out] |

[The [national data opt-out](https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out) applies to the use of confidential patient information for purposes beyond individual care, for planning and research. It will only apply if your answer to [question 15](#Page13_Section05_Question15) is section 251 support, although there are some [exceptions](https://digital.nhs.uk/services/national-data-opt-out/programmes-to-which-the-national-data-opt-out-should-not-be-applied) in which it would not apply to programmes with section 251 support.]

1. **Will any decisions be made in a purely automated way without any human involvement (automated decision making)?**

[Put an [x]  next to the one that applies.]

|  |  |
| --- | --- |
| [ ]  | Yes [[go to question 26a](#Page21_Section08_Question26a)] |
| [ ]  | No [[skip to question 27](#Page22_Section08_Question27)] |
| [ ]  | Unsure [add as a risk in [section 10](#Page25_Section10) with an action to find out] |

[An example of where automated decision making may be used is staff rostering.]

* 1. **Where the effect of the automated decision on the individual is substantial, how will you uphold an individual’s right not to be subjected to a decision solely made by automated means)?**

[For example, you provide people with an option to ask for a human review of the decision. If the effect on people is not legally significant, for example it will only have a minor impact upon them, state this here to confirm this right is not applicable.]

* 1. **Are you using any special category data as part of automated decision making?**

|  |  |
| --- | --- |
| [ ]  | Yes [we are not currently aware of any examples in health and care. If this is the case contact england.igpolicyteam@nhs.net for advice.] |
| [ ]  | No |

1. **Detail any stakeholder consultation that has taken place (if applicable).**

[For example, if your processing will have a significant impact on partner organisations or the public, you may have approached them for their views and incorporated them into the design of your data use. Include any consultation with the Information Commissioner’s Office (ICO) if applicable. For research, you should include information about the sponsors policies and procedures for [public involvement in research](https://www.hra.nhs.uk/planning-and-improving-research/best-practice/public-involvement/), and additional specific involvement relating to use of confidential patient information without consent under section 251 support.]

## SECTION 9 – Which organisations are involved?

1. **List the organisation(s) that will decide why and how the data is being used and shared (controllers).**

[The organisation(s) listed here will be making the decisions for example:

* to collect the data in the first place
* what data is being collected
* what it is being used for
* who it is being collected from

The organisation(s) will also be likely to have a direct relationship with those the data is being collected from, for example patients, service users or employees.

There may be more than one organisation listed here. They may be controllers for their own data, for example care homes would usually only be controller for their own residents’ information even if they were all using the same software supplier to manage their care records. In some instances, organisations may be joint controllers. For example, this may apply where organisations are using the data for the same purpose, where you share a dataset with another organisation, or where you have designed a new collection with another organisation. An example of where there may be joint controllers in some instances is shared care records, where multiple health and care organisations are contributing data for the same purpose.

In the case of research, the sponsor is the controller. See HRA guidance on [controllers](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-controllers-and-personal-data-health-and-care-research-context/) and research]

1. **List the organisation(s) that are being instructed to use or share the data (processors).**

[The organisation(s) listed here will be under instruction from those listed in [question 28](#Page23_Section09_Question28), for example they are likely to be told:

* what data to collect
* who to collect data from
* how the collection is legal
* the purpose for the collection
* who to share the data with
* how long to keep the data

Where processors are not being used, state not applicable.

For research, explain the sponsor’s policies and procedures for managing the use of data by research sites]

1. **List any organisations that have been subcontracted by your processor to handle data**

[Your processor listed in [question 29](#Page23_Section09_Question29) can only sub-contract an activity to another organisation with your authorisation. The organisation which has been sub-contracted is known as a sub-processor.

Where sub-processors are not being used, state not applicable.]

1. **Explain the relationship between the organisations set out in** [**questions 28**](#Page23_Section09_Question28)**,** [**29**](#Page23_Section09_Question29) **and** [**30**](#Page23_Section09_Question30) **and what activities they do**

[Describe here how it has been agreed that the organisations (controllers, processors and sub-processors) will work together. For example:

* Controller A has instructed Processor B to provide an IT system. Processor B sub-contracts the IT service desk function to sub-processor C; or
* Controllers A, B and C are controllers of their own data, which is shared between them. They all use processor D’s app

Where no other organisations are used, state not applicable.]

1. **What due diligence measures and checks have been carried out on any processors used?**

[Put an [x]  next to all that apply. Where multiple processors are used, indicate which option applies to which processor]

|  |  |
| --- | --- |
| **Due diligence measures** | **Details (leave blank if not applicable)** |
| [ ]  | **Data Security and Protection Toolkit (DSPT) compliance** | [applicable to all organisations that have access to NHS data and systems. Use the [organisation search](https://www.dsptoolkit.nhs.uk/OrganisationSearch) to check the latest DSPT score for any organisation required to complete DSPT] |
| [ ]  | **Registered with the Information Commissioner’s Office (ICO)** | [any organisation using and sharing data should be [registered](https://ico.org.uk/ESDWebPages/SearchHelp) - add the registration number] |
| [ ]  | **Digital Technology Assessment Criteria (DTAC) assessment** | [you should ask the processor for this - [see question 29](#Page23_Section09_Question29)] |
| [ ]  | **Stated accreditations** | [for example, [ISO accreditation]](https://www.iafcertsearch.org/) |
| [ ]  | **Cyber Essentials or any other cyber security certification** | [you can [check](https://www.ncsc.gov.uk/cyberessentials/search) the National Cyber Security Centre’s list of organisations that have this]­ |
| [ ]  | **Other checks** | [please state] |

## SECTION 10 – What data protections are there and what mitigations will you put in place?

1. **Complete the** [**risk assessment table**](#Page26_Riskassessmenttable)**. Use the** [**risk scoring table**](#Page26_Riskscoringtable) **to decide on the risk score.**

[Some examples have been added below. These should be amended and added according to your local set up.

This should include:

* Confidentiality risks - for example unauthorised or accidental disclosure of or access to personal data.
* Integrity risks - for example unauthorised or accidental alteration of personal data. Consider also how you will ensure data is accurate and up to date.
* Availability risks - for example unauthorised or accidental loss of access to, or destruction of personal data.

You must consider risks at each stage, for example when data is being transferred, when it is stored and when it is no longer needed.

Consider whether there are any responses to questions in this DPIA that are either inconclusive or insufficient.]

**Risk assessment table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk ref no.** | **Description** | **Risk score\* (L x I)** | **Mitigations** | **Risk score\* with mitigations applied** |
| 01 | Power outage affecting Trust servers leading to loss of availability of data | 10 | Backup generators kick in if main system fails | 2 |
| 02 | Information is stored in unrestricted network areas leading to inappropriate access to data | 8 | Ensure project team have dedicated network space with access restricted to team members | 2 |
| 03 | Data is not up to date | 12 | Controller A will send out daily notifications of updates | 4 |
| 04 |  |  |  |  |
| 05 |  |  |  |  |

**\*****Risk scoring table**

|  |  |
| --- | --- |
|  | **Impact (I)** |
| **Negligible (1)** | **Low** **(2)** | **Moderate (3)** | **Significant (4)** | **Catastrophic (5)** |
| **Likelihood (L)** | **Rare (1)** | **1** | **2** | **3** | **4** | **5** |
| **Unlikely (2)** | **2** | **4** | **6** | **8** | **10** |
| **Possible (3)** | **3** | **6** | **9** | **12** | **15** |
| **Likely (4)** | **4** | **8** | **12** | **16** | **20** |
| **Almost certain (5)** | **5** | **10** | **15** | **20** | **25** |

1. **Detail any actions needed to mitigate any risks, who has approved the action, who owns the action, when it is due and whether it is complete.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk ref no.** | **Action needed** | **Action approver** | **Action owner** | **Due date** | **Status e.g. outstanding/complete** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## SECTION 11 – Review and sign-off

[Ensure the relevant staff review or sign off the DPIA according to your governance structure. For example, this may be a more senior member of staff for higher risk processing. Add additional entries for multiple reviewers / approvers.]

|  |
| --- |
| **Reviewer sign-off** |
| Reviewer name: |  |
| Reviewer job title:  | [For example, Senior Information Risk Owner, Caldicott Guardian, Information Governance Lead, Information Asset Owner, IT lead, Data Protection Officer] |
| Reviewer contact details: |  |
| Date of review: |  |
| Comments: |  |
| Date for next review: |  |

|  |
| --- |
| **Approver sign-off** |
| Approver name: |  |
| Approver job title:  |  |
| Approver contact details: |  |
| Date of approval: |  |
| Comments: |  |