**Health and care:**

**Template data sharing and processing agreement (DSPA)**

**Background**

This is a template agreement (“Agreement”) that sets out the terms for data use and sharing and may be used in the following circumstances:

* Controller (an organisation which decides on why and how data is used or shared) to Controller data sharing. There is however, no legal obligation to enter into a written agreement to govern information sharing between a Controller and other Controller(s). Consider carefully whether it is beneficial to enter into this Agreement in such circumstances. For example, it will likely be appropriate to enter into this Agreement where you are setting up a new service that will share data in a new way. It is unlikely to be appropriate to enter into this Agreement for one off or ad hoc specialist referrals between health and care organisations.
* Controller to Processor (an organisation which has been instructed to use or share data).
* Joint Controller Arrangement (where two or more organisations jointly decide on why and how to use and share data).

It may be used for a combination of the above circumstances, for example where Joint Controllers instruct a Processor to set up a system the Joint Controllers will manage. The Agreement recognises that there may be circumstances where there are Processors who are not signatories to this Agreement. This may arise where organisations which are Processors instructed by Controllers or Joint Controllers who already have or will only enter into separate contractual terms containing relevant data processing terms, and will not be parties to this Agreement.

This Agreement should not be used for health and care research involving NHS organisations, as there is a [separate suite of template agreements](https://www.myresearchproject.org.uk/help/hlptemplatesfor.aspx) for UK-wide use that have been negotiated and agreed for commercial and non-commercial research.

The first part of the Agreement requires the Controller(s) to add in details of the specifics of the particular Processing (including sharing) taking place. The second part consists of the general terms and conditions which parties to the agreement agree to meet. These general clauses are standard, and should not usually require amendment.

It is the responsibility of the Controller(s) to complete the Agreement and ensure that this is done appropriately. This template agreement has been prepared to be compliant with data protection legislative requirements and is intended to be legally binding in itself. It can therefore be used as a standalone agreement or in conjunction with a contract, service level agreement or similar. The Controllers should, however, ensure that the Agreement is appropriate for their circumstances, seeking legal advice where necessary.

Where Sub-Processors (organisations which have been sub-contracted by a Processor with the Controller’s authorisation to fulfil a processing activity) are appointed outside of the Parties to the Agreement, the Processor appointing the Sub-Processor is responsible for ensuring they enter into a separate legally binding agreement, compliant with the data protection legislation with those Sub-Processors that ensures that that same obligations imposed by these Agreements are imposed on the Sub-Processors.

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 the Parties’ local circumstances.

**Table of Contents**

[DATA SHARING AND PROCESSING AGREEMENT 5](#_Toc140220140)

[Part 1 6](#_Toc140220141)

[1. Set out what this Agreement will cover. 6](#_Toc140220142)

[2. Summary of how data will be used and shared. 6](#_Toc140220143)

[3. Data Protection Impact Assessment (DPIA) 6](#_Toc140220144)

[4. Confirm the level of identifiability of the data for each party. 7](#_Toc140220145)

[a. If using pseudonymised data, provide further details. 7](#_Toc140220146)

[b. If using anonymised data, provide further details. 7](#_Toc140220147)

[5. What are the purposes for using or sharing the data? 7](#_Toc140220148)

[6. What are the benefits of using or sharing the data? 7](#_Toc140220149)

[7. For this agreement, which types of personal data do the Parties need to use and why? 8](#_Toc140220150)

[8. Which types of sensitive (including special category) data do the Parties need to use or share? 8](#_Toc140220151)

[9. Who are the individuals that can be identified from the data? 9](#_Toc140220152)

[10. Describe the flows of data. 10](#_Toc140220153)

[11. Under Article 6 of UK General Data Protection Regulation (UK GDPR), what is the lawful basis for processing personal data? 10](#_Toc140220154)

[12. Under Article 9 of UK General Data Protection Regulation (UK GDPR), what is the lawful basis for processing special category data? 11](#_Toc140220155)

[13. What is the legal basis for sharing or using health and care data under the common law duty of confidentiality? 12](#_Toc140220156)

[14. How will the Parties ensure that information is safe and secure? 13](#_Toc140220157)

[15. For this Agreement, how long are the Parties planning to use the data for? 14](#_Toc140220158)

[16. For this Agreement, how long do the Parties intend to keep the data? 14](#_Toc140220159)

[17. What will happen to the data at the end of this Agreement? 14](#_Toc140220160)

[18. How will the Parties comply with the following data subject rights (where they apply)? 15](#_Toc140220161)

[19. Will the national data opt-out need to be applied? Which organisation is responsible for managing this process? 17](#_Toc140220162)

[20. List the organisation(s) that will decide why and how the data is being used and shared (Controllers). 18](#_Toc140220163)

[21. List the organisation(s) that are being instructed to use or share the data (Processors). 18](#_Toc140220164)

[22. List any organisations that have been subcontracted by your Processor to handle data (Sub-Processors). 19](#_Toc140220165)

[23. How will the Parties ensure data accuracy and that updates to the data are communicated where necessary? 19](#_Toc140220166)

[24. Describe how data breaches will be managed. 19](#_Toc140220167)

[25. Set out any terms agreed by the Parties regarding liability. 19](#_Toc140220168)

[26. If applicable, provide details of any agreed variation of terms from Part 2 of this agreement. 20](#_Toc140220169)

[28. Detail any processing that has not been captured above. 20](#_Toc140220170)

[29. Set out the review period for this agreement. 20](#_Toc140220171)

[30. Reviewers 20](#_Toc140220172)

[31. Signatories 20](#_Toc140220173)

[Part 1 Annex 1 – List of Controllers and Processors and their named points of contact 22](#_Toc140220174)

[Part 2 23](#_Toc140220175)

[1. BACKGROUND AND SCOPE 23](#_Toc140220176)

[2. DEFINITIONS AND INTERPRETATION 23](#_Toc140220177)

[3. DURATION AND CONSIDERATION 27](#_Toc140220178)

[4. GENERAL OBLIGATIONS 27](#_Toc140220179)

[5. CONTROLLER OBLIGATIONS 28](#_Toc140220180)

[6. ADDITIONAL ALL PARTY AND PROCESSOR SPECIFIC OBLIGATIONS 28](#_Toc140220181)

[7. PERSONAL DATA BREACHES 35](#_Toc140220182)

[8. DATA SECURITY ARRANGEMENTS 35](#_Toc140220183)

[9. LIABILITY 36](#_Toc140220184)

[10. VARIATION OF AGREEMENT 36](#_Toc140220185)

[11. FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION REGULATIONS 37](#_Toc140220186)

[12. GENERAL 37](#_Toc140220187)

[13. TRANSPARENCY 38](#_Toc140220188)

[14. DISPUTE RESOLUTION 38](#_Toc140220189)

[15. TERMINATION 39](#_Toc140220190)

# **DATA SHARING AND PROCESSING AGREEMENT**

Issued under UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018

**BETWEEN**

**The Controller(s) and Processor(s) (where applicable),**

**as set out below**

(Collectively the ‘Parties’.)

**In support of**

The Processing (including sharing) of personal data in the operation of services within the health and care system as set out in in Part 1.

# Part 1

**Scope of agreement**

This Agreement sets out the details relating to inter Party Data Processing Activities to which the Parties have agreed.

The Definitions in Part 2 of the Agreement shall also apply to this Part 1.

In the event of any inconsistency between Part 1 and Part 2 of this Agreement, the provisions of this Part 1 shall prevail.

1. **Set out what this Agreement will cover.**

[This information can be taken from the following question in the NHS England template Data Protection Impact Assessment (DPIA):

* + - DPIA Section 9, question 31 ­– Explain the relationship between the organisations]

[Put an  next to all that apply.]

|  |  |
| --- | --- |
|  | Controller to Controller data sharing |
|  | Joint Controller arrangement |
|  | Controller to Processor instruction |

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. This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 1 question 1a – Summary of how data will be used and shared.

Where the arrangements involve Controller to Processor instructions not set out elsewhere in this Agreement, these should be included or embedded here].

1. **Data Protection Impact Assessment (DPIA)**

[Embed, link or signpost to the DPIA for this Processing, or justify why it is not needed. Set out which Party or Parties are responsible for completing and updating the DPIA and any related responsibilities such as publishing it. The responsibility for completion and update of the DPIA will be as agreed between the Parties but any Processor should provide reasonable assistance to the Controller.]

1. **Confirm the level of identifiability of the data for each party.**

[You can embed a data flow map where it describes the identifiability of the data and which organisation it flows from and to. Alternatively, you can include a description. For example, identifiable data will flow from GPs into supplier X, who pseudonymises it. The pseudonymised data then flows to the Integrated Care Board (ICB), which does not hold the pseudonymisation key so the data it receives is considered anonymised in the hands of the recipient. The ICB publishes anonymised statistics on its website.]

* 1. **If using pseudonymised data, provide further details.**

[Provide details of pseudonymised data, including which organisation holds the encryption key (the key which allows the data to be re-identified). This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 1 question 1(b) – Description of the data]
  1. **If using anonymised data, provide further details.**

[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. This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 1 question 1(b) – Description of 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 research into asthma, or we intend to look at overall health of the people in our area to ensure we have the right services in the right places. This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 2 question 2 – What are the purposes for using or sharing the data?]

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. This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 2 question 3 – What are the benefits of using or sharing the data?]

1. **For this agreement, which types of personal data do the Parties need to use and why?**

[This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 3 question 5 – Which types of personal data do you need to use and why?]

[Put an  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. **Which types of sensitive (including special category) data do the Parties need to use or share?**

[This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 3 question 6 – 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?

Embed a description of the dataset if available, unless sensitive data is covered in your embedded description in response to question 7.]

[Put an  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 |  |

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

[This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 3 question 7 – Who are the individuals that can be identified from the data?]

[Put an  next to all that apply.]

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

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

[This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 4 question 10 – 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 A – 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. **Under Article 6 of UK General Data Protection Regulation (UK GDPR), what is the lawful basis for processing personal data?**

[This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 5 question 13 – Under 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  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.

(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.] |
|  | (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. **Under Article 9 of UK General Data Protection Regulation (UK GDPR), what is the lawful basis for processing special category data?**

[This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 5 question 14 – If you have indicated 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  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. However, this agreement should not be used for health and care research involving NHS organisations] |
|  | **Other** [please state] |
|  | **Not applicable** [the use of special category data is not proposed] |

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

[This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 5 question 15 – What is your legal basis for using and sharing 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  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] |
|  | [**Explicit consent**](https://transform.england.nhs.uk/information-governance/guidance/consent-and-confidential-patient-information/) [a very clear and specific statement of consent] |
|  | **Section 251 support** [this means you have support from the Secretary of State for Health and Care or the Health Research Authority 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.] |
|  | **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.] |
|  | **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, so is likely only to be used if the Agreement relates to formalising arrangements where safeguarding or law enforcement disclosures are envisaged.] |
|  | **Not applicable** [you are not proposing to use identifiable health and care data.] |

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

[Provide evidence as follows depending on your selection in question 13]

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

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

[This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 6, question 19 – How will you ensure that information is safe and secure?

The Parties 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  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. **For this Agreement, how long are the Parties planning to use the data for?**

[This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 7, question 21 – 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. **For this Agreement, how long do the Parties intend to keep the data?**

[Detail the retention period of the data for each party. This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 7, question 22 ­– How long do you intend to keep the data?

The length of time the Parties keep the data for may differ from the period of time they 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 Agreement?**

[Provide details of how the data will be returned, destroyed or other action taken upon termination of this agreement. Outline any specific responsibilities, such as where one party is responsible for deleting or archiving centrally held data. This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 7, question 23 ­– What will happen to the data at the end of this period?]

[Put an  next to all that apply.]

|  |  |  |
| --- | --- | --- |
| **Security measure** | | **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] |

[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.]

1. **How will the Parties comply with the following data subject rights (where they apply)?**

[For Joint Controllers, indicate anything you have agreed, such as designating one Controller as a point of contact for data subjects.

These rights will not always apply, so the Parties should review each one to see if it applies. This information can be taken from the following question in the NHS England template DPIA:

* + - DPIA Section 8, question 24 – How will you comply with the following individual rights (where they apply)?

|  |  |  |
| --- | --- | --- |
| **Individual right** | **How the Parties 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 the Parties’ decision]  [Put an  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 the Parties have selected legal obligation, public task or legal claims in [question 11](#Page10_Part1_Question11), or if you have selected health and care services, public health or archiving, research or statistical purposes in [question 12](#Page10_Part1_Question12).] |  | |
| **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 the Parties are Processing under UK GDPR consent, or for the performance of a contract; and the Parties 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 the Parties are carrying out a task in the public interest or for their 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? Which organisation is responsible for managing this process?**

[Put an  next to the one that applies.]

|  |  |
| --- | --- |
|  | Yes [provide details of how this is applied] |
|  | No [provide details of why this is not applicable] |

[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 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.

This information can be taken from the following question in the NHS England template DPIA:

* + - DPIA Section 8, question 25 ­– Will the national data opt-out need to be applied?]

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

[This information can be taken from the following question in the NHS England template DPIA:

* + - DPIA Section 9, question 28 ­– 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 is also 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 as part of a joint project 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.]

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

[List the Processors relevant to this agreement. You may wish to reference Annex 1 if the list is long. Explain the relationship between the Parties, indicating which Controller has instructed which Processor. This information can be taken from the following questions in the NHS England template DPIA:

* DPIA Section 9, question 29: List the organisation(s) that are being instructed to use or share the data (processors).
* DPIA Section 9, question 31: Explain the relationship between the organisations set out in questions 28, 29 and 30 and what activities they do

Where processors are not being used, state not applicable]

1. **List any organisations that have been subcontracted by your Processor to handle data (Sub-Processors).**

[Each Party should list any organisations that have been subcontracted by their Processors to handle data. A Processor listed in question 21 can only sub-contract an activity to another organisation with the authorisation of the Controller who has instructed them. The organisation which has been sub-contracted is known as a Sub-Processor. This information can be taken from the following question in the NHS England template DPIA:

* DPIA Section 9, question 30: List any organisations that have been subcontracted by your processor to handle data

Where Sub-Processors are not being used, state ‘not applicable’.]

1. **How will the Parties ensure data accuracy and that updates to the data are communicated where necessary?**

[This information may be found in your DPIA, under the risk assessment tables where you have identified a data integrity risk and actions against it under the following questions in the NHS England template DPIA:

* + - DPIA Section 10, question 33 ­– Complete the risk assessment table. Use the \*risk scoring table to decide on the risk score.
    - DPIA Section 10, question 34 – 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.

Otherwise, this will be as agreed between the Parties.

1. **Describe how data breaches will be managed.**

[Set out here how each Party should be notified of a data breach. For example, by emailing a specific mailbox such as for the Data Protection Officer, by calling an out of hours contact number, or completing a specific form on an online portal.]

1. **Set out any terms agreed by the Parties regarding liability.**

[Organisations should take legal advice on whether they would require indemnification from other Parties. For example, a health and care organisation as a Controller may consider it appropriate to obtain a level of indemnification against losses, damages, costs or expenses and other liabilities (including reasonable legal fees) arising as a result of a breach by a Processor.]

1. **If applicable, provide details of any agreed variation of terms from Part 2 of this agreement.**

[This will be as agreed between the Parties.]

1. **Set out the mechanism for issuing a variation to this agreement.**

[This will be as agreed between the Parties.]

1. **Detail any processing that has not been captured above.**

[This may be marked as not applicable in the majority of circumstances. You may wish to include any sub-processing contract or agreement, for example, where this has not already been included in question 10 Describe the flows of data.]

1. **Set out the review period for this agreement.**

[This is the time after which all parties will review the contents of the agreement to ensure that it is still fit for purpose.]

1. **Reviewers**

This Agreement has been reviewed by:

|  |  |  |
| --- | --- | --- |
| **Name** | **Role [e.g. Data Protection Officer, Senior Information Risk Owner, Information Asset Owner]** | **Organisation** |
|  |  |  |
|  |  |  |

[Add additional approval sections as required locally.]

1. **Signatories**

**Authorised signatory on behalf of the Controller**

[Add additional lines for multiple Controllers. Electronic signatures or clicking ‘Accept’ through data sharing management portals are acceptable.]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Role | Organisation | Signature | Date |
|  |  |  |  |  |
|  |  |  |  |  |

**Authorised signatory on behalf of the Processor**

[Add additional lines for multiple Processors. Electronic signatures or clicking ‘Accept’ through data sharing management portals are acceptable.]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Role | Organisation | Signature | Date |
|  |  |  |  |  |
|  |  |  |  |  |

Part 1 Annex 1 – List of Controllers and Processors and their named points of contact

[add additional lines where necessary]

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Organisation | Contact |
|  |  |  |  |
|  |  |  |  |

# Part 2

## **BACKGROUND AND SCOPE**

* 1. This Part 2 of this Agreement sets out the general terms and conditions relating to inter-Party Data Processing Activities which the Parties agree to meet.
  2. Part 1 of the Agreement sets out the specific details of what each Party has agreed to in respect of any intended inter-Party Processing of Personal Data.
  3. The Parties agree that no Party will access or otherwise Process Personal Data that solely relates to any other Party’s individual Processing purpose, which is outside of the scope of the Processing set out in Part 1 of the Agreement.
  4. To the extent that any other agreement between the Parties in relation to these Data Processing activities contains any provisions which govern the Processing of Personal Data by the Parties, the Parties agree and acknowledge that the provisions of this Agreement shall prevail in the event of any conflict or inconsistency.
  5. Data Protection Legislation requires that *“[w]here two or more controllers jointly determine the purposes and the means of Processing they shall be joint controllers.”* It also requires that Joint Controllers determine their respective responsibilities for compliance *“…in a transparent manner…by means of an arrangement between them…”* This Agreement meets the requirement of having an arrangement. All Parties shall meet the additional transparency requirements under clause 13.

**IT IS AGREED** as follows:

## **DEFINITIONS AND INTERPRETATION**

* 1. The following definitions shall apply in this Agreement:

**Commencement Date** means between any two Parties or more the date from which the last of those Parties have signed this Agreement in respect of any Data Processing Activities (or such other date as those Parties may agree);

**Controller** means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

**Data Guidance** means any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding information governance, confidentiality, privacy or compliance with the Data Protection Legislation (whether specifically mentioned in this Agreement or not) to the extent published and publicly available or their existence or contents have been notified to the Parties by NHS England and/or any relevant Regulatory, Advisory or Supervisory Body. This includes but is not limited to guidance issued by the National Data Guardian for Health and Care, the Department of Health and Social Care, NHS England, the Health Research Authority, Public Health England (now the UK Health Security Agency) and the Information Commissioner;

**Data Loss Event** means any event that results, or may result, in unauthorised Processing of Personal Data held by the Parties under this Agreement or the loss of Personal Data that the Parties have responsibility for under this Agreement including without limitation actual or potential loss, destruction, corruption or inaccessibility of Personal Data, including any Personal Data Breach;

**Data Processing Activities** means the data Processing activities described in Part 1 of this Agreement;

**Data Protection Impact Assessment (DPIA)** means an assessment by the Controller(s) of the impact of the envisaged Processing on the protection of Personal Data;

**Data Protection Legislation** means UK Data Protection legislation currently comprising (i) the DPA 2018 (ii) the UK GDPR, the Law Enforcement Directive and any applicable national Laws implementing them as amended from time to time (iii) all applicable Law concerning privacy, confidentiality or the Processing of personal data including but not limited to the Human Rights Act 1998, the Common Law Duty of Confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations 2003;

**Data Protection Officer (DPO)** shall be the individual designated as such by Controllers and Processors where required by the Data Protection Legislation;

**Data Subject** means an identified or identifiable natural person whose Personal Data is being Processed;

**DPA 2018** means the Data Protection Act 2018;

**EU** means the European Union;

**Information Commissioner** means the Information Commissioner's Office ([ICO](http://www.ico.org.uk)) which is the independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals and any other relevant data protection or supervisory authority recognised pursuant to the Data Protection Legislation;

**International Data Transfer Agreement (IDTA)** means the documents approved for the restricted transfer of Personal Data to countries not covered by UK adequacy regulations. The documents can be found on the [Information Commissioner’s website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/);

**Joint Controller** means where two or more Controllers jointly determine the purposes and means of Processing;

**Law** means any law or subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, by-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the Parties are bound to comply;

**LED** means the Law Enforcement Directive (Directive (EU) 2016/680);

**Party or Parties** shall mean any and all signatories to this agreement, including Controllers and Processors and signatories acting as Sub-Processors;

**Personal Data** means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**Personal Data Breach** shall take the meaning given in the Data Protection Legislation, and shall also include events that would have been regarded as Personal Data Breach but which relate to information about deceased individuals where a duty of confidentiality is still owed;

**Processor** means a natural or legal person, public authority, agency or other body which Processes personal data on behalf of a Controller or (where a Party to this Agreement this shall include Processors acting as Sub-Processors, provided that the relevant Processing is described Part 1 of this Agreement). A Controller may instruct a Processor who is not a Party to this Agreement, provided such contractual provisions as are required by the Data Protection Legislation are in place with such a Processor;

**Processing** and cognate terms mean 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;

**Protective Measures** means appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data; ensuring confidentiality, integrity, availability and resilience of systems and services; ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident; and regularly assessing and evaluating the effectiveness of such measures;

**Regulatory or Supervisory Body** means any statutory or other body having authority to issue guidance, standards or recommendations with which the Parties and/or their staff must comply or have regard to, including:

(i) The Care Quality Commission (CQC);

(ii) NHS England;

(iii) the Department of Health and Social Care;

(iv) the National Institute for Health and Care Excellence;

(v) Healthwatch England and Local Healthwatch;

(vi) UK Health Security Agency;

(vi) The General Medical Council

(vii) The General Dental Council

(viii) The Nursing and Midwifery Council

(ix) the General Pharmaceutical Council;

(x) the Healthcare Safety Investigation Branch; or

(xi) the Information Commissioner.

**Respective Responsibilities** means for each Controller who is a Joint Controller the responsibilities which must, in a transparent manner, be determined for compliance with the Data Protection Legislation

**Responsible Controller** means (i) in the event of a Personal Data Breach by a Processor, the Controller who instructed that Processor (ii) in the event of a Personal Data Breach by a Controller, that Controller (iii) where Joint Controllers have designated one party as the Responsible Controller in relation to the relevant Personal Data Breach under the Agreement, that designated Controller, (iv) where there is no agreement then each of the Joint Controllers shall be a Responsible Controller;

**Staff** means any and all persons employed or engaged from time to time in the provision of the Data Processing Activities whether employees, workers, consultants or agents of any Party or any subcontractor or agent of any Party;

**Subject Rights Request** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation including to access their Personal Data (including a “subject access request”);

**Sub-Processor** means any organisation appointed by a Processor to Process Personal Data on behalf of a Processor;

**UK GDPR** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018; and

**Working Day** means a day other than a Saturday, Sunday, or public or bank holiday in England.

* 1. The following rules of interpretation shall apply to this Agreement:

reference to any legislative provision shall be deemed to include any statutory instrument, by-law, regulation, rule, subordinate or delegated legislation or order and any rules and regulations which are made under it, and any subsequent re- enactment, amendment or replacement of the same;

* + 1. words in the singular shall include the plural and in the plural shall include the singular; and
    2. references to clauses and Annexes are to clauses and Annexes to this Agreement.

## **DURATION AND CONSIDERATION**

* 1. This Agreement shall commence on the Commencement Date and shall continue until termination or expiry for whatever reason.
  2. This Agreement is entered into in consideration of the mutual trust, convenience and benefit of all the Parties and in consideration of the benefits to the health and care system.

## **GENERAL OBLIGATIONS**

* 1. A Controller remains legally responsible for the Personal Data where it is being Processed by a Processor and therefore the Controller must take steps to ensure the information assets remain protected and that the liabilities and risk are appropriately managed, Personal Data is Processed lawfully, and the Agreement is legally enforceable.
  2. A Processor is nevertheless also legally responsible for the Personal Data to the extent required under Data Protection Legislation and in any relevant Personal Data Processing contract.
  3. Each Party shall ensure that it has in place Protective Measures in relation to the Personal Data Processed under this Agreement, which are appropriate to protect against a Data Loss Event having taken account of the:
     1. nature of the Personal Data to be protected;
     2. harm that might result from a Data Loss Event;
     3. state of technological development; and
     4. cost of implementing any measures;

Processors who are Party to this Agreement are subject to additional requirements under clause 6.7.2. Where a Controller instructs a Processor who will Process Personal Data in relation to this Agreement and such Processor is not a Party to this Agreement, the instructing Controller shall ensure that contractual provisions complying with the Data Protection Legislation are in place with such Processor.

* 1. Each Party shall ensure that its staff involved in the Processing of Data under this Agreement have undergone adequate training in the use, care, protection and handling of Personal Data that enables them and the Processor to comply with their responsibilities under the Data Protection Legislation and this Agreement. Processors are subject to additional requirements under clause 6.7.3.
  2. All Parties shall in good faith cooperate fully during any handover arising from the cessation of any part of the Data Processing Activities. Processors are subject to additional requirements under clause 6.7.7.
  3. All Parties shall be under a duty to notify any potentially impacted Parties where they become aware of or reasonably suspect a Data Loss Event; orbecome aware of or reasonably suspect that it has in any way caused, or might reasonably be considered to be likely to cause, a breach of Data Protection Legislation by another Party. Processors are subject to additional requirements under clause 6.8.

## **CONTROLLER OBLIGATIONS**

* 1. Each Controller shall at all times ensure Personal Data is Processed fairly, lawfully and transparently in accordance with Data Protection Legislation.
  2. Each Controller warrants that any instructions it issues to a Processor in respect of the Personal Data are lawful.

## **ADDITIONAL ALL PARTY AND PROCESSOR SPECIFIC OBLIGATIONS**

* 1. The following obligations within this clause 6 shall apply where at least one Processor has been identified in Part 1 of this Agreement. Where the Processor is not a Party to this Agreement, the Controllers who instruct them must ensure that any contracts with such Processors provide equivalent protection to the clauses set out in clause 6 of this Agreement. Where indicated, the obligations shall apply to any Party to this Agreement not just Processors.
  2. The Parties acknowledge that for the purposes of the Data Protection Legislation in relation to the Data Processing Activities, the Controller(s) and the Processor(s) are as set out in Part 1 of this Agreement. A Processor must Process the Processor Data only to the extent necessary to perform the Data Processing Activities and only in accordance with the written instructions set out in Part 1 of this Agreement.
  3. A Processor must use the Personal Data shared solely for the purposes as instructed and shall not Process the Personal Data for any other purposes.
  4. Each Party agrees to treat the data (including Personal Data) received by them under the terms of this Agreement as confidential and shall safeguard it accordingly.
  5. All Parties must provide all reasonable assistance to one another and in particular to any Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing under this Agreement. Such assistance may include:
     1. a systematic description of the envisaged Processing operations and the purpose of the Processing;
     2. an assessment of the necessity and proportionality of the Processing operations in relation to the Data Processing Activities;
     3. an assessment of the risks to the rights and freedoms of Data Subjects; and
     4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
  6. Any Party requested, but in particular any Processor who is a Party to this Agreement, shall provide all reasonable assistance to a Controller if the outcome of the Data Protection Impact Assessment leads the Controller to consult the Information Commissioner concerning any proposed arrangements.
  7. A Processor must (and must be required in any contractual documentation where such Processor is not a Party to this Agreement), in relation to any Personal Data Processed in connection with its obligations under this Agreement:
     1. Process that Personal Data only in accordance with the documented instructions of a Controller, unless the Processor is required to do otherwise by Law. If it is so required, the Processor must promptly notify the Controller before Processing the Personal Data unless such notification is prohibited by Law;
     2. ensure that it has in place Protective Measures, which have been reviewed and approved by the Controller as appropriate to protect against a Data Loss Event having taken account of the:
        1. nature of the Personal Data to be protected;
        2. harm that might result from a Data Loss Event;
        3. state of technological development; and
        4. cost of implementing any measures;
     3. ensure:
        1. when delivering the Data Processing Activities, the Processor Staff only Process Personal Data in accordance with this Agreement;
        2. it takes all reasonable steps to ensure the reliability and integrity of any Processor Staff who have access to the Personal Data and ensure that they:
           1. are aware of and comply with the Processor’s duties under this clause;
           2. are subject to appropriate confidentiality undertakings with the Processor and any Sub-Processor that are in writing and are legally enforceable;
           3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
           4. have undergone adequate training in the use, care, protection and handling of Personal Data that enables them and the Processor to comply with their responsibilities under the Data Protection Legislation and this Agreement. The Processor shall provide the Controller with evidence of completion and maintenance of that training within three Working Days of request by the Controller.
     4. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to that Controller on termination of the Data Processing Activities and certify to the Controller that it has done so within five Working Days of any such instructions being issued, unless the Processor is required by Law to retain the Personal Data;
     5. if the Processor is required by any Law or Regulatory or Supervisory Body to retain any Processor Data that it would otherwise be required to destroy under this clause 6, notify the Controller in writing of that retention giving details of the Processor Data that it must retain and the reasons for its retention;
     6. notify the Controller immediately if it considers that carrying out any of the Controller’s instructions would infringe Data Protection Legislation. This obligation extends to breaches concerning the systems on which the data shared under this Agreement are held, even if the data shared under this Agreement is not directly affected;
     7. cooperate fully with the Controller during any handover arising from the cessation of any part of the Data Processing Activities, and if the Controller directs the Processor to migrate Processor Data to the Controller or to another nominated organisation, provide all reasonable assistance with ensuring safe migration including ensuring the integrity of Personal Data and the nomination of a named point of contact for the Controller (as set out in Annex 1 of Part 1 of this Agreement).
  8. Subject to clause 6.10, a Processor must notify the relevant Controller immediately if it:
     1. receives a Subject Rights Request (or purported Subject Rights Request);
     2. receives a request to rectify, block or erase any Personal Data;
     3. receives any other request, complaint or communication relating to obligations under Data Protection Legislation owed by the Processor or Controller;
     4. receives any communication from the Information Commissioner or any other Regulatory or Supervisory Body (including any communication concerned with the systems on which Personal Data is Processed under this Agreement);
     5. receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;
     6. becomes aware of or reasonably suspects a Data Loss Event; or
     7. becomes aware of or reasonably suspects that it has in any way caused the Controller to breach Data Protection Legislation.
  9. The notification under clause 6.8 shall be given by emailing any relevant request and any subsequent communications to the Controller’s Data Protection Officer immediately, and in no longer than one Working Day of receipt by the Processor.
  10. A Processor shall not respond substantively to the communications listed at clause 6.8 save that it may respond to a Regulatory or Supervisory Body following prior consultation with the Controller.
  11. A Processor’s obligation to notify under clause 6.8 includes the provision of further information to the Controller in phases, as details become available.
  12. A Processor must provide their instructing Controller with all reasonable assistance in relation to either Party's obligations under the Data Protection Legislation and any complaint, communication or request made under clause 6.8 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
      1. the Controller with full details and copies of the complaint, communication or request;
      2. the Controller with any Personal Data it holds in relation to a Data Subject;
      3. such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Subject Rights Request within the relevant timescales set out in the Data Protection Legislation;
      4. such assistance as is reasonably requested by the Controller to enable the Controller to comply with other rights granted to individuals by the Data Protection Legislation including the right of rectification, the right to erasure, the right to object to Processing, the right to restrict Processing, the right to data portability and the right not to be subject to an automated individual decision (including profiling);
      5. assistance as requested by the Controller following any Personal Data Loss Event;
      6. assistance as requested by the Controller in relation to informing a Data Subject about any Data Loss Event, including communication with the Data Subject;
      7. assistance as requested by the Controller with respect to any request from the Information Commissioner, or any consultation by the Controller with the Information Commissioner.
      8. A Processor shall designate a Data Protection Officer if required by the Data Protection Legislation, and shall communicate to the Controller the name and contact details of any Data Protection Officer.
  13. A Processor must allow for reasonable audits of its delivery of the Data Processing Activities by the Controller or the Controller’s designated auditor at no additional cost to the Controller.
  14. For the avoidance of doubt:
      1. a Processor must not novate this Agreement nor assign, delegate, subcontract, transfer, charge or otherwise dispose of all or any of its rights or obligations or duties under this Agreement without the prior written approval of the instructing Controller. The approval of any sub-processing or subcontracting arrangement may include approval of the terms of the proposed subcontract;
      2. subcontracting any part of this Agreement will not relieve a Processor of any of its obligations or duties under this Agreement. A Processor will be responsible for the performance of and will be liable to the Controller for the acts and/or omissions of all Sub-Processors as though they were their own;
      3. any positive obligation or duty on the part of the Processor under this Agreement includes an obligation or duty to ensure that all subcontractors and Sub-Processors comply with that positive obligation or duty. Any negative duty or obligation on the part of the Processor under this Agreement includes an obligation or duty to ensure that all subcontractors and Sub-Processors comply with that negative obligation or duty.
  15. Without prejudice to clause 6.16, before allowing any Sub-Processor to Process any Personal Data related to this Agreement, a Processor must:
      1. notify the relevant Controller in writing of the intended Sub-Processor and Processing;
      2. obtain the written consent of the relevant Controller;
      3. carry out appropriate due diligence of the Sub-Processor and ensure this is documented;
      4. enter into a binding written agreement with the Sub-Processor which includes equivalent terms to those set out in this Agreement; and
      5. provide the relevant Controller with such information regarding the Sub-Processor as the Controller may reasonably require.
  16. The Parties agree to take account of any guidance issued by the Information Commissioner. A Controller may (or where there is more than one Controller they may by agreement) on not less than 30 Working Days’ notice to the Processor amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner.
  17. A Controller may (or where there is more than one Controller they may by agreement), at any time on not less than 30 Working Days’ notice, revise this Agreement by adding to it any applicable Controller to Processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).
  18. A Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Agreement, the Data Protection Legislation and Data Guidance. A Processor must create and maintain a record of all categories of data Processing activities carried out under this Agreement, which must be made available to the instructing Controller within two Working Days of a written request, containing:
      1. the categories of Processing carried out under this Agreement;
      2. details of categories of Data Subjects;
      3. where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;
      4. a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data Processed under this Agreement; and
      5. a log recording the Processing of Personal Data in connection with this Agreement comprising, as a minimum, details of the Personal Data concerned, how the Personal Data was Processed, where the Personal Data was Processed and the identity of any individual carrying out the Processing.
  19. A Processor warrants and undertakes that it will deliver the Data Processing Activities in accordance with the Data Protection Legislation and this Agreement and in particular that it has in place Protective Measures that are sufficient to ensure that the delivery of the Data Processing Activities complies with the Data Protection Legislation and ensures that the rights of Data Subjects are protected.
  20. A Processor must assist the Controller in ensuring compliance with the obligations set out at Article 32 to 36 of the UK GDPR and equivalent provisions implemented into Law, taking into account the nature of Processing and the information available to the Processor.
  21. A Processor must assist the Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the UK GDPR (security of Processing, obligations with regards to Personal Data Breaches and conducting Data Protection Impact Assessments) and equivalent provisions implemented into Law, taking into account the nature of Processing and the information available to the Processor.
  22. A Processor must take prompt and proper remedial action regarding any Data Loss Event.
  23. A Processor must assist the Controller by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controllers’ obligation to respond to requests for exercising rights granted to individuals by Data Protection Legislation.
  24. A Processor must promptly (and in any event within a maximum of four (4) Working Days) comply with any request of the Controller or the Information Commissioner to provide a copy of any or all Personal Data which is under the Processor's custody or control, in the format and on a media reasonably specified by the Controller or the Information Commissioner.
  25. A Processor must not transfer Personal Data outside the UK except to countries covered by adequacy regulations, unless the prior written consent of their instructing Controller has been obtained and the following conditions are fulfilled:
      1. appropriate safeguards in relation to the transfer are in place as determined by the instructing Controller;
      2. the Data Subject has enforceable rights and effective legal remedies;
      3. the Party transferring the data complies with its obligations under Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the relevant Controller in meeting its obligations); and
      4. the Processor, where one has been appointed, complies with any reasonable instructions notified to it in advance by the relevant Controller with respect to the Processing of the Personal Data.

## **PERSONAL DATA BREACHES**

* 1. A Responsible Controller will notify the other Controllers who are Parties to this Agreement of a Data Breach if, acting reasonably, they consider that the interests of those Controllers may be affected by any Personal Data Breach for which it is the Responsible Controller. In the case of Joint Controllers, each of the Joint Controllers shall notify the other Joint Controllers of any Personal Data Breach of which it becomes aware.
  2. A Responsible Controller will determine whether to notify Personal Data Breaches to the Information Commissioner.
  3. A Responsible Controller will determine whether and how to notify Personal Data Breaches to the Data Subjects.
  4. The Responsible Controller will monitor Personal Data Breach responses to ensure compliance with statutory timescale and any other requirements arising by Law or under this Agreement.

## **DATA SECURITY ARRANGEMENTS**

* 1. All Parties shall:
     1. have in place appropriate technical and organisational security measures designed to protect Personal Data against accidental events or unlawful or malicious actions that compromise the availability, integrity and confidentiality of the Personal Data, and ensure that such measures are appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and have regard to the nature of the Personal Data which is to be protected;
     2. ensure that all Personal Data Processed by any Party and its staff are subject to the technical and organisational security measures the Party implements and maintains, pursuant to clause 8.1.1 above;
     3. have procedures in place to monitor access to the Personal Data and to identify unauthorised and unlawful access and use of Personal Data;
     4. where health and care data is accessed by a Party, that Party must complete and publish an annual information governance assessment in accordance with, and comply with the mandatory requirements of, the NHS Data Security and Protection Toolkit, as applicable to the Data Processing Activities and the Party’s organisation type. Where health and care data is not accessed, any Party accessing other Personal Data must maintain annual governance assessments to any agreed equivalent standard; and
  2. A Processor shall:
     1. immediately report any untoward incidents, near misses or activities that suggest non-compliance with this Agreement to the Controller and cooperate with the Controller to carry out a risk assessment, root cause analysis and identify any corrective action required. A Processor will cooperate with the Controller in implementing any required corrective action agreed between the Parties. (N.B. It is the Controller’s responsibility to ensure that any incidents are reported in accordance with the Department of Health and Social Care policy and procedures and for informing the relevant Data Subjects as appropriate.)

## **LIABILITY**

* 1. The Parties shall not do or omit to do anything that will put any other Party in breach of the Data Protection Legislation or the Data Guidance.
  2. The rights and remedies provided under Part 1 of this Agreement are in addition to, and not exclusive of, any rights or remedies provided by Law or in equity.
  3. A waiver of any right or remedy under Part 1 of this Agreement or by Law or in equity is only effective if given in writing and signed on behalf of the Party giving it and any such waiver so given shall not be deemed a waiver of any similar or subsequent breach or default.
  4. A failure or delay by a Party in exercising any right or remedy provided under Part 1 of this Agreement or by Law or in equity shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this Agreement or by Law or in equity shall prevent or restrict the further exercise of that or any other right or remedy.

## **VARIATION OF AGREEMENT**

* 1. Any proposed changes to this Agreement, including the addition or removal of parties, the purposes of the information sharing, the nature or type of information shared or manner in which the information is to be Processed must be notified promptly to the Information Compliance/Governance leads so that the impact of the proposed changes can be assessed.
  2. No variation of this Agreement shall be effective unless it is in writing and signed by all Parties to this Agreement.

## **FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION REGULATIONS**

* 1. Where a Controller is a public authority, the Parties acknowledge that such a Controller is subject to the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).
  2. A Controller as set out in clause 11.1 will be statutorily required, subject to any applicable exemptions, to disclose information about the Data Processing Activities provided under this Agreement or the Agreement itself in response to a specific request under FOIA or EIR. In which case:
     1. A Processor shall provide its instructing Controller with all reasonable assistance and co-operation to enable the Controller to comply with its obligations under FOIA or EIR; and
     2. A Controller as set out in clause 11.1 Controller shall consult any Party it reasonably considers relevant or who may have a legitimate interest in respect of any commercial, confidential or other issues in relation to the Agreement relevant to the issue of whether the information is exempt from disclosure or not; however the final decision about disclosure of information or application of exemptions shall rest solely with the Controller which has received the request.

## **GENERAL**

* 1. A Processor, where appointed, shall not assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any or all of its rights and obligations under this Agreement without the prior written consent of their instructing Controller.
  2. This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.
  3. It is an offence under the Data Protection Legislation for any Party to knowingly or recklessly re-identify any data that is de-identified without the consent of the Controller that has provided the information.

## **TRANSPARENCY**

* 1. All Parties agree that the Controllers shall:
     1. ensure publication of a summary of the Data Processing Activities, provided in a concise, transparent, intelligible and easily accessible form;
     2. ensure Data Subjects are appropriately instructed on how they can exercise their rights under Data Protection Legislation, including where they must contact another Party; and
     3. to reference other Parties’ transparency materials published under 13.1.1.

## **DISPUTE RESOLUTION**

* 1. Parties shall aim to resolve all disputes, differences and questions by means of cooperation and consultation.
  2. If any dispute arises, the Parties in dispute must first attempt to settle it with a written offer of negotiation by any of the Parties to the other Parties. During the following 15 Business Days Period each of the Parties in dispute must negotiate and be represented:
     1. for the first 10 Business Days, by a senior person who where practicable has not had any direct day-to-day involvement in the matter and has authority to settle the Dispute; and
     2. for the last 5 Business Days, by their chief executive, director, or equivalent senior individual who has authority to settle the dispute.
  3. Where practicable, no Party in dispute should be represented by the same individual for the different stages described in 14.2.1 and 14.2.2 above.
  4. If the Parties in dispute are unable to settle the Dispute by negotiation, they must, within 5 Business Days after the end of the Negotiation Period, submit the Dispute to mediation by the Centre for Effective Dispute Resolution (CEDR) or other independent body or organisation agreed between the Parties which will follow the mediation Process of CEDR or other independent body or organisation as agreed.
  5. This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the Law of England.
  6. Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims), provided that nothing in this clause shall prevent a Party from enforcing any judgement obtained in the court of England and Wales in any other court with jurisdiction over the other Party.

## **TERMINATION**

* 1. These arrangements may be terminated in respect of a Party by that Party giving reasonable notice to the other Parties. Termination by one Party shall not terminate the Agreement in respect of the other Parties.
  2. The Parties may terminate this Agreement by mutual agreement.
  3. Without affecting any other right or remedy available to it, a Controller may immediately terminate this Agreement by notice in writing to a Processor if the Processor commits a material breach of any provision of this Agreement, or the Processor repeatedly breaches any of the provisions of this Agreement.