NHS
Yorkshire
Ambulance Service
NHS Trust

Information Sharing Policy

Document Author: Head of Risk & Assurance and Data Protection Officer (DPO)

Approved: February 2025

Document Reference	PO – Information Sharing Policy – February 2028
Version	V3.0
Responsible Director (title)	Director of Corporate Services and Company Secretary, Deputy Chief Executive
Document Author (title)	Head of Risk & Assurance and Data Protection Officer (DPO)
Approved by	Information Governance Working Group
Date Approved	February 2025
Review Date	February 2028
Equality Impact Assessed (EIA)	Yes
Document Publication	Internal and Public Website

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
0.1	January 2021	Head of Risk and Assurance	D	Initial version produced.
1.0	May 2021	Risk Team	A	Approved at TMG
1.1	February 2023	Head of Risk and Assurance	D	Full review completed – GDPR amended to UK GDPR
2.0	April 2023	Risk Team	A	Approved at TMG
2.1	January 2025	Head of Risk & Assurance and DPO	D	Full review Amendments of Responsible committee Amendment of Author Amendment of responsible director 1.1 – 2018 added to Data Protection Act sentence 1.3 – As above 1.4 – Disclosure policy added to list 3.1.2 – Disclosure policy added to list Appendix A – New ISA template added
3.0	Feb 2025	Risk Team	A	Policy approved at IGWG, published internally and externally.

A = Approved D = Draft

Document Author = Head of Risk & Assurance and DPO

Associated Documentation: Insert names of associated Policies or Procedures here

Data Protection Policy
Information Governance Framework
Records Management Policy
Data Quality Policy
Disclosure Policy
Freedom of Information Policy
ICT Security Policy and Associated Procedures
Email Policy
Internet Policy and Procedure
Social Media Policy
Safety and Security Policy
Incident and Serious Incident Management Policy
Surveillance Camera Systems Policy
Safeguarding Policy
Disciplinary Policy and Procedure
YAS Code of Conduct
Domestic Abuse Guidance
Prevent Strategy Guidance
Courts and Evidence Policy

Staff Summary

This section should be used to summarise the top 10 bullet points of the policy or strategy. It should highlight the key points in short, concise sentences placed into a table.

This document sets out the Trust's policy on information sharing. It also defines how information should be shared with outside bodies and partners.
The Trust is committed to ensuring that it handles all information securely and that it takes due care over the movement and disclosure of data.
This document is intended to provide guidance on the overarching requirements relating to all regular transfers and sharing of information and it is intended that all new data transfer/sharing arrangements will comply with the relevant parts of this guidance.
The scope of this guidance is especially targeted at regular transfers of information.
All personal data should be treated with the utmost confidentiality and will only be shared by the Trust with those organisations which can demonstrate a professional or legal requirement for having access.
All data transfer and sharing arrangements with external parties should be the subject of a formal documented information sharing agreement (ISA).
The aim of any ISA is to define how information should be treated between organisations or parties and to help organisations to understand and comply with their legal obligations.
An ISA should be created for any regular planned transfer of personal or special category data.
There is a general expectation that any partners to a data transfer or sharing arrangement will act lawfully, honestly and in accordance with the conditions contained within any signed ISA.
It is recommended that all ISAs be reviewed on a regular basis.

1.0 Introduction

1.1 In the course of its day-to-day operations, Yorkshire Ambulance Service NHS Trust ('the Trust') utilises information of all kinds. An integral part of business operations is the need to transfer or share such information, whether this is within the organisation (between departments) or externally to other Trusts, public bodies and partners.

1.2 The Trust has a number of legal obligations in respect of the use, disclosure and security of the information it uses. For example, the Data Protection Act 2018 relates to the way in which the Trust can deal with personal data. However, it is necessary to ensure that all of its data is appropriately handled and adequately protected, and this includes the movement and disclosure of information in whatever form and by whatever means.

1.3 The four main pieces of legislation that govern information sharing are the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000

1.4 The Trust is committed to ensuring that it handles all information securely and that it takes due care over the movement and disclosure of information. Any information shared or issued by Trust employees should be carried out in accordance with existing Trust policies and procedures, namely the:

- Data Protection Policy
- Disclosure Policy
- Data Protection Impact Assessment Procedure
- Freedom of Information Policy
- ICT Security Policy and Associated Procedures

1.5 Information sharing may have to be carried out without a formal agreement in conditions of real urgency and sometimes without the individual's knowledge. This would occur for example in a situation when someone's life was in danger. The Data Protection Act 2018 is still applied in these cases and professional judgement must be exercised by the sharer. Further information on how to deal with ad-hoc requests for information can be found in the ICO's Data Sharing Code of Practice:

https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

2.0 Purpose/Scope

2.1 This document sets out the Trust's policy on information sharing. It also defines how information should be shared with outside bodies and partners.

2.2 The Trust is committed to ensuring that it handles all information securely and that it takes due care over the movement and disclosure of data.

2.3 It will provide the basic principles to ensure the Trust is compliant with relevant legislation as well as its own policies and procedures. It will help to ensure the secure and legal management and processing of any information shared between the Trust and its

partners. The principles of this document should be used as guidance where no formal information sharing agreement is in place or until one is agreed.

2.4 This document is not itself an information sharing protocol as individual projects, initiatives, pieces of work or research should have a bespoke information sharing agreement drawn up between all the relevant parties that suit their requirements. This process can sometimes take some time to draw up and ratify, as it is often necessary to scope the exact requirements and establish the necessary approval from the relevant responsible officers. Other organisations may draw up a protocol and the Trust may only need to sign up to this or agree it is fit for purpose. In the absence of any protocol or agreement, a template document has been supplied in Appendix A.

2.5 This document is intended to provide guidance on the overarching requirements relating to all regular transfers and sharing of information and it is intended that all new data transfer/sharing arrangements will comply with the relevant parts of this guidance. However, it is recognised that there may be some existing data transfer/sharing arrangements in place that may not fully comply with the contents of this guidance. Existing arrangements must be brought into alignment with the guidance as and when they are either renewed or reviewed.

2.6 The scope of this guidance is especially targeted at regular transfers of information. It is especially important, in the context of transferring information to, or sharing information with external bodies and partners, that the recipient has in place the required data security and handling mechanisms and can provide appropriate assurances on the safe custody of the Trust's information.

2.7 Generally, information sharing takes place in a pre-planned and routine way. However, in conditions of urgency, for example in an emergency, ad hoc or 'one-off' information sharing may be necessary.

3.0 Process

3.1 Roles and Responsibilities

3.1.1 All employees need to be aware of the Information Sharing Policy.

3.1.2 Any information shared or issued by Trust employees should be dealt with in accordance with all relevant policies and procedures, namely the:

- Data Protection Policy
- Disclosure Policy
- Freedom of Information Policy
- ICT Security Policy and Associated Procedures
- Disclosure Policy

3.1.3 It is the duty of all employees to ensure that they fully understand their responsibilities in respect of all aspects of handling, securing and disclosing information in the course of their work, as they may be held liable in the event of unauthorised or inappropriate actions.

3.2 Types of Data

3.2.1 For the purpose of this policy, there are essentially four types of data. These are:

- Personal Data;
- Special Category data;
- Personal Data Relating to Criminal Convictions or Offences;
- Anonymised and Aggregated Data.

3.2.2 Wherever possible anonymised or aggregated data should be used, unless there is legitimate reason for sharing personal and special category data.

3.2.3 Personal Data

Data protection legislation and the UK GDPR apply only to personal data about a living, identifiable individual. However, the definition of personal data is highly complex and for day-to-day purposes it is best to assume that all information about a living, identifiable individual is personal data.

3.2.4 Such personal data might include, but not be limited to:

- Name;
- Address;
- Telephone number;
- Age;
- A unique reference number, if that number can be linked to other information which identifies the data subject, such as National Insurance number, NHS number or Payroll number.

3.2.5 The law imposes obligations and restrictions on the way that the Trust and its partners process personal data. Data protection legislation and the UK GDPR regard ‘processing’ of data to include collecting, storing, amending and disclosing data. The conditions for processing personal data are set out in Article 6 of the UK GDPR.

3.2.6 The individual who is the subject of the data (the ‘data subject’) has the right to know who holds their data and how such data will be processed, including how such data is to be, or has been, shared. It is the responsibility of the data processor to communicate this appropriately, for example at the point the data is collected, and through privacy notices.

3.2.7 Special Category Data

The UK GDPR refers to certain types of data as ‘special category data’, for example:

- Ethnic origin;
- Political opinions;
- Religious beliefs;
- Trade union membership;
- Genetics;
- Biometrics;
- Health;
- Sexual orientation.

3.2.8 The law says that for Public Authorities to use special category data they should seek, where possible, explicit consent regarding what the information will be used for, and with whom it will be shared. The conditions for processing special category data are set out in Article 9 of the UK GDPR.

3.2.9 The individual who is the subject of the data (the 'data subject') has the right to know who holds their data and how such data will be processed, including how such data is to be, or has been, shared. It is the responsibility of the data processor to communicate this appropriately, for example at the point the data is collected, and through privacy notices. YAS' Privacy Policy can be found at: https://www.yas.nhs.uk/tc/privacy-policy/

3.2.10 Personal Data Relating to Criminal Convictions and Offences

This would include information relating to the commission or alleged commission of any offence, or any proceedings for any offence committed, or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings. The conditions for processing of personal relating to criminal convictions and offences are set out in Article 10 of the UK GDPR.

3.2.11 Anonymised and Aggregated Data

Anonymised and aggregated data can be used in very similar ways. Anonymised data are individual data records from which the personally identifiable fields have been removed.

3.2.12 Aggregated data is data which has been processed to produce a generalised result, from which individuals cannot be identified. However, care must be taken when such aggregations could lead to an individual being identified, e.g. groupings with small distribution leading to isolation of individual characteristics.

3.2.13 On the basis that anonymised and aggregated data does not identify individuals, the processing of such data is not regulated by data protection and the UK GDPR. In 2012, a code of practice was published on anonymising data, designed to reduce the likelihood and risk of individuals being identified through re-identification. The code of practice is available on the Information Commissioner's Office (ICO) website:

https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

3.3 Confidentiality of Information

3.3.1 All personal data should be treated with the utmost confidentiality and will only be shared by the Trust with those organisations which can demonstrate a professional or legal requirement for having access. No information should be used outside the organisation for commercial gain or advantage without the prior agreement of the Trust.

3.3.2 The following key rules should always apply:

- Confirm the identity of the person you are sharing information with;
- Obtain consent to share if safe, appropriate and feasible to do so;
- Confirm the reason the information is required;
- Be fully satisfied that it is necessary to share;

- Be fully satisfied that you are able to share and there are no legal impediments to doing so;
- Check with the Information Asset Owner (IAO) or the Information Governance (IG) Team if you are unsure;
- Do not share more information than is necessary;
- Inform the recipient if any of the information is potentially inaccurate or unreliable;
- Ensure that the information is shared safely an securely;
- Be clear with the recipients how the information will be used;
- Ensure that all parties are aware of their responsibilities and obligations;
- Ensure that the recipient has adequate security and data protection arrangements in place before information is provided;
- Be clear that the information will be disposed of securely after use;
- Record what information is shared, when, with whom and why.

3.4 Information Sharing Agreements (ISAs)

3.4.1 The Trust may enter into partnership agreements that involve the supply of information to meet the requirements of statutory and local initiatives. The parties to these arrangements can potentially be either public or private sector organisations.

3.4.2 All data transfer and sharing arrangements with external parties should be the subject of a formal documented information sharing agreement (ISA).

3.4.3 The aim of any ISA is to define how information should be treated between organisations or parties and to help organisations to understand and comply with their legal obligations. It provides a set of common rules that are binding on all the organisations involved. An ISA should be created for any regular planned transfer of personal or special category data.

3.4.4 Partners should satisfy themselves that any ISAs are compliant with their statutory duties and legislation. Personal information will only be disclosed when the purpose of the ISA requires that disclosure and it satisfies the provisions of the Data Protection Act 2018 and UK GDPR.

3.5 The Information

3.5.1 Data Formats

To provide a consistent approach when exchanging data an agreed format should be stated. The format will depend on what the data consists of, but where possible a consistent recognised standard should be used. The Information Governance Team hold the ISA template for the sharing of information and it is recommended that this is requested and used to ensure consistency and standards in the form of data supplied externally.

3.5.2 Data Audit

All information stored, processed and/or passing through the Trust should be tracked and recorded. This provides an audit trail of where the information has come from and where it is going.

3.5.3 All ISAs should be approved by the IG Team before sign off. Final, signed copies should be forwarded to the IG Team to be logged on the register and stored centrally.

3.6 Expectations when entering into an ISA

3.6.1 There is a general expectation that any partners to a data transfer or sharing arrangement will act lawfully, honestly and in accordance with the conditions contained within any signed ISA.

3.6.2 Where there is a requirement for the parties to an ISA to comply with a specific technical or regulatory standard or condition, the details of these should be clearly expressed within the ISA so that there is no possible avoidance of the need to comply.

3.6.3 It is reasonable to expect that risks associated with sharing, transfer and subsequent use of YAS data should be set out in a balanced way that reflects the issues that could arise, and who would be likely to be primarily responsible for creating and managing them. Care should be taken to ensure that the Trust is not exposed to avoidable risks and associated liabilities.

3.6.4 All partners should be expected to adhere to the requirements of the Data Protection Act 2018 and the following key principles set out in the UK GDPR:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality (security);
- Accountability.

In addition, all partners should declare that they have current, up to date and relevant registrations under the Act with the Information Commissioner that specifically permits the uses and disclosures required in relation to the specific ISA.

3.6.5 There should be ongoing and open communication between the parties during the operation of the ISA so that problems, issues and revisions can be promptly brought to general attention and effectively managed; this is especially important in respect of data quality and any detected errors or shortcomings, which should be resolved as a matter of urgency.

3.6.6 The ISA should allow for the periodic review of long-running arrangements so that circumstantial, regulatory and legislative changes can be taken into account and the ISA updated to reflect them.

3.6.7 The recipient(s) of data should have adequate and effective physical and logical security arrangements in place.

3.6.8 As a minimum requirement, all partners should have ratified information security and data protection policies in place that are actively promoted throughout their organisations.

3.6.9 Partners should have confidentiality policies and privacy notices covering all affected patients and staff.

3.7 Deciding on whether to share data

3.7.1 All decisions to share data should be fully considered in light of the legislation contained in the UK GDPR, and decisions recorded to provide an audit trail. It is important that when deciding to enter into an agreement to share data you must be clear on the objective that it is meant to achieve.

3.7.2 More in-depth guidance on the sharing of data can be found in Articles 6, 9 and 10 of the UK GDPR. The links are given below:

- Art. 6 UK GDPR - Lawfulness of processing: https://gdpr-info.eu/art-6-gdpr/
- Art. 9 UK GDPR - Processing of special categories of personal data: https://gdpr-info.eu/art-9-gdpr/
- Art. 10 UK GDPR - Processing of personal data relating to criminal convictions and offences: https://gdpr-info.eu/art-10-gdpr/

3.7.3 For each of the above, the following questions need to be answered:
What is the lawful basis for processing (Article 6 of the UK GDPR)?

- Consent
- Contractual necessity
- Legal Obligation
- Vital interests
- Public task
- Legitimate interests

What is the lawful basis for processing (Article 9 of the UK GDPR)?

- Consent
- Obligations in connection with employment
- Vital interests
- Legitimate activities of a not for profit body or association
- Information has been made public by the data subject
- Necessary in relation to legal rights
- Necessary for public functions
- Necessary for medical purposes
- Necessary for reasons of public interest in the area of public health
- Necessary for archiving purposes

What is the lawful basis for processing criminal offence data (Article 10 of the UK GDPR)?

- Legal authorisation
- Official capacity

3.8 Data Protection Impact Assessment (DPIA)

3.8.1 A DPIA must be carried out when new information sharing arrangements with third parties are being put in place (including those providing a service to the Trust), but only where personal data is involved.

3.8.2 The Data Protection Impact Assessment Procedure (and template) is an appendix to the Data Protection Policy on Pulse; an editable version of the DPIA template is also available through the IG Team.

3.9 Content of the ISA

3.9.1 Organisations may have their own ISA template. If this is sufficient and complies with UK GDPR, it may be just a case of signing this. However, to ensure that the UK GDPR is fully adhered to and nothing is omitted, it may be more appropriate to use the Trust's template at Appendix A of this document.

3.9.2 An ISA should contain the following:

- Parties to the agreement;
- Purpose of the sharing;
- Type and status of information to be shared;
- Context of the processing;
- Legal basis for sharing;
- Information items to be shared;
- Information transfer method;
- Review date;
- Retention and disposal details;
- Signatures.

3.10 Review of Existing ISAs

3.10.1 It is recommended that all ISAs be reviewed on a regular basis. Each ISA should state when the agreement commences, where possible the duration of the agreement and the review date.

3.10.2 Before any changes can be made, the organisations affected must be informed of the changes and given the chance to comment upon them before they take effect. If necessary, a new ISA should be drawn up. All parties should sign to acknowledge they agree to the changes made.

3.10.3 The IG Team will contact employees responsible for such agreements when they are due for review, asking them to ensure that any changes are appropriately considered in relation to this policy.

4.0 Training expectations for staff

4.1 Training is delivered as specified within the Trust Training Needs Analysis (TNA).

5.0 Implementation Plan

5.1 The latest ratified version of this policy will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted to how to find and access this policy and associated procedures during Trust Induction.

6.0 Monitoring compliance with this Policy

6.1 Failure to comply with this policy may result in disciplinary action being taken.

7.0 Appendices

Appendix A: Information Sharing Agreement Template

Information Sharing Agreement (ISA)

Information Sharing Agreement (ISA) title:	[add the name of the initiative, programme, project or process]
Information Asset Owner:	[add name and title]
ISA reference number:	[to be added by Information Governance team following sign off]
Data Protection Impact Assessment (DPIA) reference number:	[to be added by Information Governance team following sign off]

Organisation Name	Yorkshire Ambulance Service NHS Trust
Address	Springhill 2, Brindley Way Wakefield 41 Business Park Wakefield WF2 0XQ
Responsible Manager	
Contact Details	
Source/Recipient?	
Authorised Signatory/Date **(Caldicott Guardian/SIRO)**	

Organisation Name	

Address	
Responsible Manager	
Contact Details	
Source/Recipient?	
Authorised Signatory/Date **(Caldicott Guardian/SIRO)**	

Date of Agreement	

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

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

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

2. **Confirm the level of identifiability of the data being shared.**

[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.]

a. 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 DPIA:

- DPIA Section 1 question 1(b) – Description of the data].

b. 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 DPIA:

- DPIA Section 1 question 1(b) – Description of the data]

3. What are the purposes for 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 DPIA:

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

4. What are the benefits of sharing the data?

[Set out the benefits of sharing the data. This should cover the benefits to the individuals whose data is being shared, 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 DPIA:

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

5. For this agreement, which types of personal data do the Parties need to share and why?

[This information can be taken from the following question in the 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.]

6. Which types of sensitive (including special category) data do the Parties need to share?

[This information can be taken from the following question in the 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	

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

[This information can be taken from the following question in the 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]

8. Describe the flows of data.

[This information can be taken from the following question in the 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

9. 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 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** [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 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 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]

10. 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 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 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** [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 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 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 for the most likely laws that apply when using and sharing information in health and care. See HRA guidance on legal basis for processing data for research. Processing must be in the public interest to rely on this lawful basis. This agreement should not

	normally be used for health and care research involving NHS organisations. In cases where no other arrangements have been made, this agreement may be used.
☐	**Other** [please state]
☐	**Not applicable** [the use of special category data is not proposed]

11. What is the legal basis for sharing health and care data under the common law duty of confidentiality?

[This information can be taken from the following question in the 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** [for individual care or local clinical or care audits]
☐	**Explicit consent** [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 (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.]

a. Please provide further information or evidence.

[Provide evidence as follows depending on your selection in question 11]

- 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…
-

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

[This information can be taken from the following question in the 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]

13. 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 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].

14. 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 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 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.]

15. 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 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 provides detail about what happens once a retention period has been reached.]

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

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 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, or if you have selected health and care services, public health or archiving, research or statistical purposes in question 12.]	
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.]	

17. 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 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 in which it would not apply to programmes with section 251 support.

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

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

18. List the organisation(s) that will decide why and how the data is being shared.

[This information can be taken from the following question in the 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.]

19. List the organisation(s) that are being instructed to share the data.

[This information can be taken from the following questions in the 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

20. 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 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.

21. 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.]

22. 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.]

23. Reviewers

This Agreement has been reviewed by*:

Name	Role	Organisation
		Yorkshire Ambulance Service NHS Trust
		[Add organisation name]

*Please send ISA to the Information Governance team for review, yas.yasinformationgovernance@nhs.net

24. Signatories

Name	Role	Organisation	Signature	Date
	[Caldicott Guardian/SIRO]	Yorkshire Ambulance Service NHS Trust		
		[Add organisation name]		