NHS
Yorkshire
Ambulance Service
NHS Trust

Information Sharing Policy

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

Approved: August 2026

Document Reference	PO – Information Sharing Policy – August 2029
Version	V4.0
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	August 2026
Review Date	August 2029
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
2.0	April 2023	Risk Team	A	Approved at TMG
3.0	Feb 2025	Risk Team	A	Policy approved at IGWG, published internally and externally
3.1	May 2025	Risk Team	A	Link in 1.5 updated
3.2	June 2026	Helen Jones	D	Associated Documentation – Incident and Serious Incident Management Policy amended to Incident Management Policy. 3.2.13 - Wording amended. Removed reference to Code of Practice re anonymising data. Appendix A updated to reflect NHSE template.
3.3	July 2026	Risk Team	D	Formatted to Trust template
4.0	August 2026	Risk Team	A	Approved in August 2026 IGWG
A = Approved D = Draft				
Document Author = Helen Jones, Head of Risk & Assurance and DPO				
Associated Documentation: 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 and Communications Policy Internet Policy Social Media Policy Safety and Security Policy Incident Management Policy Surveillance Camera Systems Policy Safeguarding Policy (Children Young People and Adults at Risk) Disciplinary Policy, Procedure & Guidance YAS Code of Conduct Domestic Abuse Policy and Management Guidance Coroners and Courts Policy				

Staff Summary

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/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/**

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

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. YAS' Privacy Policy can be found at: https://www.yas.nhs.uk/tc/privacy-policy/.

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 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.

3.2.10 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.

3.2.11 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.

3.2.12 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. Please see the Information Commissioner's Anonymisation Guidance.

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 and 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

3.6.5 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.

3.6.6 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.

3.6.7 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.

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

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

3.6.10 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:

3.7.4 What is the lawful basis for processing (Article 6 of the UK GDPR)?

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

3.7.5 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

3.7.6 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

7.1 This Policy includes the following Appendices

Appendix A: Information Sharing Agreement Template

Appendix A: Information Sharing Agreement Template

Health and care:
Template information sharing agreement (ISA)

Information Sharing Agreement (ISA) title:	Add the name of the initiative, programme, project or process
Information Asset Owner (IAO):	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?	

Organisation Name	
Address	
Responsible Manager	
Contact Details	
Source/Recipient?	

Date of Agreement	

1. Summary of how data will be used and shared.
Expand to see guidance notes

Add details here

2. Confirm the level of identifiability of the data for each Party.
Expand to see guidance notes

Add details here

a. If using pseudonymised data, provide further details.
Expand to see guidance notes

Add details here

b. If using anonymised data, provide further details.
Expand to see guidance notes

Add details here

3. What are the purposes for using or sharing the data?
Expand to see guidance notes

Add details here

4. What are the benefits of using or sharing the data?
Expand to see guidance notes

Add details here

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

Expand to see guidance notes

Put an ☒ next to all that apply.

- ☐ Forename
- ☐ Surname
- ☐ Address
- ☐ Postcode full
- ☐ Postcode partial
- ☐ Date of birth
- ☐ Age
- ☐ Gender
- ☐ Physical description, for example height
- ☐ Phone number
- ☐ Email address
- ☐ GP details
- ☐ Legal representative name (personal representative)
- ☐ NHS number
- ☐ National insurance number
- ☐ Other numerical identifier

Please state

- ☐ Photograph / picture of people
- ☐ IP address
- ☐ Other location data

Please state

- ☐ Audio recordings
- ☐ Video recordings
- ☐ Other

Please state

- ☐ None

Explain 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 use or share?

Expand to see guidance notes

Put an ☒ next to all that apply.

☐ Information relating to an individual's physical or mental health or condition, for example information from health and care records

Expand to see guidance notes

Explain why this is needed

☐ Biometric information in order to uniquely identify an individual, for example facial recognition

Explain why this is needed

☐ Genetic data, for example details about a DNA sample taken as part of a genetic clinical service

Explain why this is needed

☐ Information relating to an individual's sexual life or sexual orientation

Explain why this is needed

☐ Racial or ethnic origin

Explain why this is needed

☐ Political opinions

Explain why this is needed

☐ Religious or philosophical beliefs

Explain why this is needed

☐ Trade union membership

Explain why this is needed

☐ Information relating to criminal or suspected criminal offences

Explain why this is needed

☐ None of the above

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

Embed your description here

7. Who are the individuals that can be identified from the data?
Expand to see guidance notes

Put an ☒ next to all that apply.

☐ Patients or service users

☐ Carers

☐ Staff

☐ Wider workforce

☐ Visitors

☐ Members of the public

☐ Other - please state

If you have selected 'Other', please state who this is here

8. Describe the flows of data.
Expand to see guidance notes

Describe the data flow, or embed a map here, or use the table below.

Example table of data flows
[Replace sample text with your own data flows]

Data flow name	Going from (source)	Going to (destination)	Data description

Admission data	Hospital electronic patient record system	Local authority social care team	Extract of admission data from patient health record: demographic data only
GP health record data	GP health record	Hospital trust	Extract of GP health record for a patient made available through the GP Connect API

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

Expand to see guidance notes

Put an ☒ next to the one that applies.

☐ (a) **We have consent**

Expand to see guidance notes

☐ (b) **We have a contractual obligation**

Expand to see guidance notes

☐ (c) **We have a legal obligation**

Expand to see guidance notes

☐ (d) **We need to protect a person's vital interests**

Expand to see guidance notes

This is very unlikely to be appropriate within health and care, as it only applies in emergency life or death situations, where another lawful basis such as public task, recognised legitimate interest or legitimate interest cannot be applied.

☐ (e) **We need it to perform a public task**

Expand to see guidance notes

☐(f) **We have a recognised legitimate interest**

Expand to see guidance notes

Put an ☒ next to the one that applies.

The recognised legitimate interest falls under:

☐ Sharing with another organisation for its public task or official functions

☐ National security, public security and defence

☐ Emergencies

☐ Detecting, investigating or preventing crime

☐ Safeguarding vulnerable individuals

☐ (f) **We have another legitimate interest**

Expand to see guidance notes

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

Expand to see guidance notes

Put an ☒ next to the one that applies:

☐ (a) **We have consent**

Expand to see guidance notes

☐ (b) **We need it for employment purposes**

Expand to see guidance notes

☐ (c) **We need it to protect a person's vital interests**

Expand to see guidance notes

☐ (d) **We need it for our not-for-profit organisation's activities, and it relates to our current or former members, or people who have regular contact with us**

Expand to see guidance notes

☐ (e) **The person who the data is about has made that data public**

Expand to see guidance notes

☐ (f) **We need it for legal claims, to seek legal advice or judicial acts**

Expand to see guidance notes

☐ (g) **There is a substantial public interest, as set out in this list**

Expand to see guidance notes

☐ (h) **We need it to provide or manage health or social care services**

Expand to see guidance notes

☐ (i) **We need it for public health purposes**

Expand to see guidance notes

☐ (j) **We need it for archiving, research and statistics where this is in the public interest**

Expand to see guidance notes

☐ **Not applicable**

Expand to see guidance notes

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

Expand to see guidance notes

Put an ☒ next to the one that applies.

☐ **Implied consent**

Expand to see guidance notes

☐ **Explicit consent**

Expand to see guidance notes

☐ **Section 251 support**

Expand to see guidance notes

☐ **Legal requirement**

Expand to see guidance notes

☐ **Overriding public interest**

Expand to see guidance notes

☐ **Not applicable**

Expand to see guidance notes

a. **Please provide further information or evidence.**
Expand to see guidance notes

Add details here, or state 'not applicable' if you selected implied consent or not applicable for question 13

12. How will the Parties ensure that information is safe and secure?
Expand to see guidance notes
If this Agreement is intending to cover the use of AI, provide details of how the AI supplier protects data that flows into the AI.

Put an ☒ next to all that apply.

☐ Encryption

Specify the level of encryption, such as AES 256

☐ User identity verification and authentication

Specify the measures in place, for example, multi factor authentication and provide details on how this is done

☐ Role based access controls (RBAC)

Expand to see guidance notes

Please give details of what role-based access and permissions will be set

☐ Physical controls

Expand to see guidance notes

Please give details of what physical controls will be in place

☒ Security policies

Expand to see guidance notes

All Parties confirm that appropriate security policies are in place for the data it holds on local systems.

☐ Business continuity plans

Expand to see guidance notes

Please state or embed the relevant business continuity plans

☐ Other

Please describe the other ways in which you will ensure data is safe. Or embed any other relevant documents, such as a cyber security risk assessment, confirming who has reviewed it and the outcome.

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

Expand to see guidance notes

Clearly state here if there are differing time periods for different Parties.

Type your answer here

14. For this Agreement, how long do the Parties intend to keep the data?

Expand to see guidance notes

Add details here of the retention period for each Party

15. What will happen to the data at the end of this Agreement?

Expand to see guidance notes

Put an ☒ next to all that apply.

☐ Secure destruction

Provide details of how the data will be destroyed, for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction. Confirm who will manage and be accountable for this

☐ Long term preservation by transferring the data to a National Archives' approved Place of Deposit

Expand to see guidance notes

Provide details of where the data will be retained and who will be accountable for it

☐ Transfer to another organisation

Expand to see guidance notes

Provide details of the organisation(s) it will be transferred to and who will be accountable for this

☐ Extension to retention period

Provide your approved justification for this here

☐ It will be anonymised and kept

Provide details of how it will be done and who will be accountable for this

☐ The controller(s) will manage as it is held by them

Provide details here

☐ Other

Please explain what will happen to the data

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

Expand to see guidance notes

a. The right to be informed

The right to be informed about the collection and use of personal data.

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 the other way(s) in which you will comply

☐ Not applicable

b. Describe how the communication methods above meet your obligation to comply with the right to be informed.

Expand to see guidance notes

Add your description here

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.

Describe the arrangements

The right to rectification

The right to have inaccurate personal data rectified or completed if it is incomplete.

Describe the arrangements

The right to erasure
The right to have personal data erased, if applicable.

Expand to see guidance notes

Describe the arrangements

The right to restrict processing
The right to limit how their data is used, if applicable.

Expand to see guidance notes

Describe the arrangements

The right to data portability
The right to obtain and re-use their personal data, if applicable.

Expand to see guidance notes

Describe the arrangements

The right to object
The right to object to the use and sharing of personal data, if applicable.

Expand to see guidance notes

Describe the arrangements

17. Will the national data opt-out need to be applied? Which organisation is responsible for managing this process?
Expand to see guidance notes

Put an ☒ next to the one that applies.

☐ Yes Please provide details of how this will be applied

☐ No

Please provide details of why this does not apply

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

Expand to see guidance notes

Add details here

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

Expand to see guidance notes

Add details here

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

Expand to see guidance notes

Add details here

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

Expand to see guidance notes

Add details here

22. Describe how data breaches will be managed.

Expand to see guidance notes

Add details here

23. Set out the review period for this agreement.

Expand to see guidance notes

Add details here

24. Reviewers

Expand to see guidance notes

This Agreement has been reviewed by:

Reviewer 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

25. Signatories

Authorised signatory on behalf of the Controller

Expand to see guidance notes