NHS
Yorkshire
Ambulance Service
NHS Trust

Information Sharing Policy

Document Author: Head of Risk and Assurance

Date Approved: April 2023

Document Reference	PO – Information Sharing Policy
Version	V2.0
Responsible Committee	Trust Management Group
Responsible Director (title)	Executive Director of Quality, Governance and Performance Assurance, Deputy Chief Executive
Document Author (title)	Head of Risk and Assurance
Approved By	Trust Management Group
Date Approved	April 2023
Review Date	April 2025
Equality Impact Assessed (EIA)	Yes
Protective Marking	Not protectively marked

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

A = Approved D = Draft

Document Author = Head of Risk and Assurance

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 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

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 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 Act (GDPR) 2016
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act

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

3.1.2 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 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

Yorkshire Ambulance Service NHS Trust

Information Sharing Agreement

This agreement is to be used in conjunction with the Inter Agency Information Sharing Protocol and complies with all the guidance therein.

1. Parties to this Agreement

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, Chief Executive, Director etc.).**	

Organisation Name	
Address	
Responsible Manager	
Contact Details	
Source/Recipient?	
Authorised Signatory/Date **(Caldicott Guardian, SIRO, Chief Executive, Director etc).**	

Date of Agreement	

2. Specific purpose(s) for which the information sharing is required (all intended purposes should be described, it may be appropriate to describe each one on a separate pro forma) and necessity for the sharing

3. Type and status of information shared

Is the information 'person identifiable'?	Yes/No
Does it include special category personal data?	Yes/No
Does it include criminal offence data?	Yes/No
Has explicit consent been given and recorded?	Yes/No
Has implied consent been recorded?	Yes/No
Is the subject aware that sharing will take place?	Yes/No
Is the information anonymised?	Yes/No

4. Context of the Processing

What is the nature of your relationship with the individuals?	
How much control will they have?	
Would they expect you to use their data in this way?	
Do they include children or other vulnerable adults?	
Are there prior concerns over this type of processing or security flaws?	
What is the current state of technology in this area?	
Are there any current issues of public concern that you should factor in?	
Are you signing up to any approved code of conduct certification scheme (once any have been approved)?	

5. Legal basis for sharing - please tick as appropriate

Article 6 (required if processing personal information):

Consent	
Contractual necessity	
Legal obligation	
Vital interests	
Public task	
Legitimate interests	

Article 9 (required if processing personal information, including special category data*):

*racial or ethnic origin, political opinions,religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life, data concerning a person's sexual orientation

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	

Article 10 (required if processing personal information, including criminal offence data)

Legal authorisation	
Official capacity	

6. Duty of Confidentiality

Does a Duty of confidentiality exist?	Yes/No	
What justification is there for overriding this? Please tick as appropriate	Explicit consent	
	Substantial Public interest	
	Vital Interests	

7. Information Items shared

This list must be comprehensive and include ALL data items that are to be shared. All data items to be shared must be justifiable as necessary for the purpose. The service user/staff member should be aware that the information will be. For the purpose of delivering care implied consent is sufficient.

Service User Information	**Yes/No**	**Comment**
Name, address, Date of Birth, Gender, GP		
Identifying numbers (e.g. NHS number or YAS incident or job number)		
Next of Kin, Emergency Contact, Carer Details		
Clinical Details (Clinical details should only be shared where there is a justifiable purpose)		
Basic Clinical Details (Condition and relevant care requirements)		
Full Clinical Details		

(May include medical history, test results, clinical letters, reports etc.)		
Criminal Offence Data		
Other (Should only be shared where there is a justifiable purpose)		
Risk Factors		
Other (Please Explain)		
Staff Information	**Yes/No**	**Comment**
Name, Job Title, Work Base, Work Team, Line Manager		
Identifiers Such As Payroll No. NI Number		
Home Address, Date of Birth and Next of Kin		
Full Employment Record		

8. Protective Marking

Is Protective marking/Classification relevant to this information?	Yes/No
If Yes, to what level	
1	
2	
3	

9. Information Transfer Method

All parties to this agreement are responsible for ensuring that appropriate security and confidentiality procedures are in place to protect the transfer and use of the shared, person identifiable information.

Regular transfer (specify frequency)	
Ad hoc	

More than 21 items per transfer	
Less than 21 items per transfer	

Give full details of how the transfer will be made and what security measures will be in place e.g. encryption, business secure mail or recorded signed for etc.

Face to face	
Telephone	
Electronically (state method)	
Secure E Mail	
Secure Mail	
Secure Courier	
Encrypted Removable Media	
Other	
Transfers outside the UK	• *State whether the information be transferred outside of the UK* • *If you are transferring data outside the UK then you must record the measures that the organisation receiving the personal data has taken to provide adequate safeguards under UK GDPR Chapter V.*

Has a risk assessment been carried out on the chosen methods of transfer?	**Yes/No**

What are the identified risks?	

10. Audit and Review

Organisation Name	
Address	
Responsible Manager	
Contact number	
Review Date	

INCIDENTS
Any incidents occurring as a result of this agreement should be reported to the signatories of all affected organisations. They will then pass on the information
in accordance with incident reporting procedures within their own organisation
if appropriate. Organisations will agree to share information in order to help investigate any such incidents

11. Subject Access

Subject Access Requests Will Be Directed To	
Special Arrangements For Subject Access Requests	

12. Retention and Disposal

Retention Period For Information	
Disposal Method For Information	

Acknowledgements

YAS is a signatory to the Inter-agency Information Sharing Protocol which has been signed by several Yorkshire and Humberside public and third sector organisations. This template has been adopted from that protocol as a good practice tool.