Data Sharing Agreement

Policy Number	**IG018**
Target Audience	**All staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**28th May 2020**
Last Review Date	**April 2020**
Next Review Date	**28th May 2022**
Policy Author	**IG Team**
Version Number	**V1.1**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	June 2018	GMSS IG Team	Draft – document development
0.1	June 2018	IG Board	Approved
1.0	July 2018	CCG Chief Officer	Approved
1.1	April 2020	IG Team	Review for Approval

Analysis of Effect completed:	By: M Robinson	Date: July 2018

DATA SHARING AGREEMENT	
Data Sharing Partners **Between**	
Purpose:	
Version No:	
Commencement Date:	
Date for Review:	
Author(s)	

Contents

Introduction

A Data Sharing Agreement provides a formal agreement between all parties to it, to share data and / or access data of another party and to fulfil their respective obligations whilst maintaining the duty of confidentiality and the individual's right to privacy.

It is good practice to have a Data Sharing Agreement in place unless is it required by law. All parties are able to be clear about the nature of the arrangement, setting out the purpose of the data sharing, covering what is to happen to the data at each stage, setting standards and also helps all the parties understand their respective roles. It supports organisations demonstrate their accountability under Data Protection legislation, specifically the General Data Protection Regulation (GDPR).

The agreement should help an organisation to justify their data sharing and to demonstrate that they have been mindful of, and have documented, the relevant compliance issues.

This Data Sharing Agreement should be used for sharing data with Data Processors and so for the purposes of the Data Protection Legislation, each party shall be a Data Controller of the Personal Data in the data which is shared or accessed pursuant to this Agreement.

This Data Sharing Agreement is in addition to, and does not replace, any Data Guidance (as defined below) contained in other documents which address the sharing of information by organisations within the NHS. This includes (without limitation):

- Confidentiality: NHS Code of Practice (November 2003).
- Information Security Management: NHS Code of Practice (April 2007).
- A Guide to Confidentiality in Health and Social Care (HSCIC, September 2013).
- The NHS Records Management Code of Practice for Health & Social Care (2016).
- ICO Data Sharing Code of Practice.
- The Information Governance Review (March 2013).
- National Data Guardian Report (2017).
- Bolton CCG Data Protection Impact Assessement Procedure
- Bolton CCG Information Governance Clause

This Data Sharing Agreement is additional to any further agreements in place between the parties relating to the Data Sharing and / or Access. Data Controllers must adhere to the GDPR and ensure that mandatory documents are in place, such as Data Protection Impact Assessments (DPIAs) and Contracts. This Data Sharing Agreement will sit alongside such documents.

Drafting and adhering to an agreement does not in itself provide an organisation with any form of legal indemnity from action under the data protection legislation or other law. However the Information Commissioner's Office (ICO) will take this into account if it receives a complaint about your data sharing.

There is no set format for a Data Sharing Agreement; it can take a variety of forms, depending on the scale and complexity of the data sharing in question. Since a Data Sharing Agreement is a set of common rules binding on all the organisations involved in a data sharing initiative, the agreement should be

clear, concise language that is easy to understand. This document aims to cover the key areas.

Definitions and Interpretation

1.1. The definitions and rules of interpretation in this clause 0 shall apply in this Agreement.

Agreement means this Data Sharing / Access Agreement.

Business Day means a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

Caldicott Guardian means the individual designated by each party (where applicable) with responsibility for ensuring that such party complies with the principles set out in the Caldicott Report.

Caldicott Report means Report on the Review of Patient-Identifiable Information by the Caldicott Committee published in December 1997.

Caldicott Principles means the principles set out in the Caldicott Report.

Commencement Date means the date of the last party to sign this Agreement.

Controller has the meaning given in the Data Protection Legislation.

Data Guidance means any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding information governance, confidentiality, privacy or compliance with the Data Protection Legislation (whether specifically mentioned in this Agreement or not) to the extent published and publicly available or their existence or contents have been notified to a party by another party and/or any relevant Regulatory or Supervisory Body. This includes but is not limited to guidance issued by NHS Digital, the National Data Guardian for Health & Care, the Department of Health, NHS England, the Health Research Authority, Public Health England, the European Data Protection Board and the ICO.

Data Item means a specific item of data as listed in Appendix 1 to be shared or accessed by the parties pursuant to this Agreement.

Data Protection Legislation mean (i) the GDPR, the LED and any applicable national laws implementing them as amended from time to time; (ii) the DPA 2018; (iii) all applicable law concerning privacy, confidentiality or the Processing of Personal Data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations.

Data Access means where a party to this Agreement accessing data from one of more of the other parties to this Agreement.

Data Sharing means the disclosure of data (including without limitation, Personal Data and Patient Identifiable Data) between two or more parties to this Agreement.

Data Subject has the meaning given in the Data Protection Legislation.

DPA 2018 means the Data Protection Act 2018.

DPIA or Data Protection Impact Assessment has the meaning given in the Data Protection Legislation.

DPO or **Data Protection Officer** means the individual designated by each party (as applicable) as required by Article 37 of the GDPR.

EIRs means the Environmental Information Regulations 2004 (SI 2004/3391) together with any guidance and/or codes of practice issued by the ICO or relevant government department in relation to such regulations.

FOIA means the Freedom of Information Act 2000 together with any guidance and/or codes of practice issued by the ICO or relevant government department in relation to such legislation.

GDPR means the General Data Protection Regulation (Regulation (EU) 2016/679).

Information means the data items (including without limitation, Personal Data) as set out in Appendix 1, to be shared between, or accessed by, one or more parties to this Agreement.

Information Asset Owner means the individual at a party with the responsibility for the control and safeguarding of a particular Data Item.

Information Governance and Data Quality Lead means the individual designated by each party to lead on the development of interactions and projects which engage the sharing of data (including without limitation, Personal Data) by the relevant parties.

Joint Controller has the meaning given in the Data Protection Legislation.

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

Line Managers mean the individuals at each party who have managerial responsibility for staff of that party who access Data and/or Personal Data.

Personal Data has the meaning given in the Data Protection Legislation.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the data.

Patient Identifiable Data has the meaning given in the Caldicott Report.

Process, **Processing** and similar terms have the meaning given in the Data Protection Legislation.

Processor has the meaning given in the Data Protection Legislation.

Purpose means the purpose of the parties sharing or permitting access to the data, as specified above.

Regulatory or Supervisory Body means any statutory or other body having authority to issue guidance, standards or recommendations with which the relevant party must comply or to which it or they must have regard, including:

(a) CQC;

(b) NHS Improvement;

(c) NHS England;

(d) the Department of Health;

(e) NICE;

(f) Healthwatch England and Local Healthwatch;

(g) Public Health England;

(h) the General Pharmaceutical Council;

(i) the Healthcare Safety Investigation Branch;

(j) Information Commissioner;

(k) European Data Protection Board.

Special Categories of Personal Data shall mean the categories of Personal Data as defined in Article 9 of the GDPR.

Subject Access Request means the exercise by a Data Subject of his or her rights under Article 15 of the GDPR.

Supervisory Authority means the relevant supervisory authority in the territory(ies) where the parties to this Agreement are established.

Term means the term of this Agreement as set out in clause 0.

1.2. The Appendices form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Appendices.

1.3. Unless the context otherwise, requires, words in the singular shall include the plural and in the plural, shall include the singular.

1.4. A reference to a statue or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

1.5. Any words following the terms including, include, in particular or for example or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

Purpose

1.6. This Agreement sets out the framework for the Data Sharing and / or Data Access by the parties. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other. Each party shall comply with the terms and conditions of this Agreement and with their responsibilities, principles and processes set out in this Agreement.

Security and Training

1.7. A party shall only share or provide access to data to another party by using secure methods as set out in clause 0.

1.8. The parties undertake to have in place throughout the Term appropriate technical and organisational security measures to:

(a) prevent:

(i) unauthorised or unlawful processing of the Personal Data in the data; and

(ii) the accidental loss or destruction of, or damage to, the Personal Data in the data;

(b) ensure a level of security appropriate to:

(i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and

(ii) the nature of the Personal Data in the Personal Data to be protected.

1.9. The level of technical and organisational measures agreed by the parties as appropriate as at the Commencement Date having regard to the state of technological development and the cost of implementing such measures is set out in clause 0. The parties shall keep such security measures under review and shall carry out such updates as they agree are appropriate throughout the Term.

Personal Breaches and Reporting Procedures

1.10. Each party shall comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) Data Subjects under Article 33 of the GDPR and shall inform each other party of any Personal Data Breach irrespective of whether there is a requirement to notify any Supervisory Authority or Data Subject(s).

1.11. The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an efficient and compliant manner.

Confidentiality, Consent and Data Sharing / Access Principles

1.12. It is the responsibility of each party always have consideration of the privacy and confidentiality of Data Subjects and to take account of their legitimate expectations and rights regarding the use of that individual's Personal Data andData.

1.13. Each party will endorse, support and promote the accurate, timely, secure and confidential sharing of both Patient Identifiable Data and anonymised data (including without limitation Personal Data) where such data sharing is essential for the care and treatment of patients.

1.14. The parties are fully committed to ensuring that if they share datait is in accordance with their legal, statutory and common law duties (including without limitation, the Data Protection Legislation) and that such sharing meets the requirements of any Data Guidance.

1.15. The parties acknowledge the requirements that apply to the sharing of dataconcerning patients who lack capacity to consent. Where appropriate, explicit consent should be obtained from the person with legal authority to act on the person's behalf. The reasons for final decision to share or permit access to dataconcerning patients who lack capacity to consent should be clearly recorded.

1.16. Where a party requests that data supplied by it be kept confidential from the patients who use its services, the outcome of this request and the reasons for taking the decision will be recorded.

1.17. Data will not be used for any other purposes or further shared without the prior consent of the patient, other than as set out in this Agreement.

1.18. The parties to this Agreement have in place policies and procedures to meet the national requirements for the Data Protection Legislation and Data Guidance. The existence of, and adherence to, such policies provides all parties with confidence that data shared will be transferred, received, used, held and disposed of securely.

1.19. All parties will ensure that all relevant staff are aware of, and comply with, their responsibilities regarding both the confidentiality and security of Information. All staff working for the parties to this Agreement are personally responsible for the safekeeping of any data they obtain, handle, use and disclose responsibly and promote a good information management practice through the following sub-clauses:

(a) all staff will be made aware of and fully trained in their obligations to safeguard the confidentiality of the data . It is an offence to knowingly or recklessly obtain or disclose Personal Data without the consent of the party in control of the Personal Data, or without lawful excuse. Every member of staff shall be trained to know how to obtain, use and share datathey legitimately require to do their job and seek advice when necessary. It should be noted that the control of Personal Data may require the consent of the patient unless there is a legal requirement or an overriding public interest justification;

(b) all staff must be made aware of their obligations through training and/or job induction procedures. Such training will be recorded and periodically reviewed;

(c) all staff will be made aware of the sanctions and audit trails in place and the consequences of Personal Data Breaches; and

(d) audit trails will be regularly reviewed to ensure investigations can be properly pursued and to ensure consistency of standards.

All staff should be aware that any Data Protection Breach, violation of privacy or breach of confidentiality is unlawful and their involvement in the same could result in a disciplinary matter that could lead to their dismissal, subject to the relevant policies and processes of the relevant employing party. Staff should also be informed that criminal proceedings might also be brought against that individual in respect of any violation of privacy or breach of confidentiality.

1.20. The individuals designated by the parties to undertake the following roles shall have the following responsibilities:

Line Managers have a responsibility to:

(a) ensure all current and new staff are instructed in their responsibilities in relation to the appropriate sharing & disclosure of data and work in a manner consistent with these procedures;

(b) provide advice and guidance to staff requiring support in appropriately handling data sharing & disclosure;

(c) in certain circumstances support equality and diversity by considering the individual requirements of staff in order to support them in complying with these procedures;

Information Asset Owners have a responsibility to authorise access to system/information;

Information Governance and Data Quality Leads have a responsibility to:

(a) deal with enquires; provide advice and guidance to support the appropriate use and sharing of personal data and support the role of the Caldicott Guardians;

(b) support the development of datasharing agreements;

Caldicott Guardians will operate as a key component of the broader information governance framework of the relevant parties and shall have responsibility for:

(a) safeguarding and governing the uses made of personal datawithin the organisation, as well as personal data flows to other NHS and non-NHS organisations;

(b) overseeing the establishment of procedures governing access to, and the use of, personal data and, where appropriate, the transfer of that data to other bodies;

(c) taking account of the codes of conduct provided by professional bodies, including without limitation, HSCIC's a Guide to Confidentiality in Health and Social Care and Confidentiality: NHS Code of Practice (November 2003), in addition to the Caldicott Principles;

(d) Supporting the relevant party in their development of strategy and process to maintain compliance with the Caldicott Principles and other relevant legislation in all aspects of their work e.g. National Care Recovery Service; and

(e) Keeping abreast of developments concerning safeguarding Personal Data.

Data Protection Officers will:

(a) inform and advise the party and its employees about their obligations to comply with the Data Protection Legislation.

(b) monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.

1.21. The parties are responsible for putting in place effective procedures to address complaints relating to the disclosure ofdata, and information about these procedures should be made available to patients, as set out in clause 0.

1.22. Where it is agreed that the sharing / accessing of data is to be undertaken, only that datawhich is needed and relevant will be shared / accessed and that would only be on a "need to know" basis.

1.23. Personal Data must be held securely whether electronically or on paper in relevant filing systems, to maintain contemporaneous records and to enable legitimate processing in accordance with the Data Protection Legislation.

1.24. Personal Data will not be used for any other purpose other than the Purpose stated in this Agreement in compliance with Article 5 of the GDPR.

1.25. Personal Data must be kept accurate and up to date to comply with Article 5 of the GDPR.

1.26. Retention of Personal Data will be in accordance with each individual party's retention schedule and / or the Department of Health and Social Care's Records Management Health & Social Care Code of Practice.

1.27. The parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.

1.28. Each party acknowledges that any other party may be subject to the requirements of the FOIA and the EIRs. Each party shall provide all necessary assistance and cooperation as reasonably requested by a party to enable it to comply with its obligations under the FOIA and EIRs.

1.29. Each party receiving data from another party shall:

(a) keep the data confidential; and

(b) not use or exploit the data in any way, except for the Purpose.

1.30. Each party may disclose the data to the minimum extent required by:

(a) any order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or taxation authority of competent jurisdiction; or

(b) the laws or regulations of any country to which its affairs are subject.

Monitoring

1.31. Each party shall designate a senior officer, e.g. Caldicott Guardian or Data Protection Officer who will oversee the implementation of this Agreement and subsequent revisions.

Restrictions on Use of Data Shared / Accessed

1.32. All shared data and accesseddata, whether constituting Personal Data or otherwise, must only be used for the Purpose unless obliged under statute or regulation or under the instructions of a court or as agreed elsewhere between the parties.

1.33. The parties acknowledge that

(a) restrictions may also apply to any further use of data that is not Personal Data, such as due to commercial sensitivity or prejudice to individuals may be caused by the data's release, and this should be considered when considering secondary use for such data. If in doubt the Information Asset Owner should be consulted.

(b) Additional statutory restrictions apply to the disclosure of certain data for example, data regarding a patient's HIV and AIDS status, assisted conception and abortion, or child protection.

Term and Termination

1.34. This Agreement shall have an initial term of [1] year(s) from the Commencement Date, which may be extended in [1] year extensions, up to a maximum contract length of [•] years, subject to a [1 year] notice period, being applicable and available to either party.

1.35. Each party may terminate this Agreement immediately on written notice to each other party if:

(a) another party commits a material breach of any term of this Agreement which breach is irremediable or (if such breach is remediable) the breaching party fails to remedy that breach within a period of [30] days after being notified in writing to do so;

(b) the other party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts;

(c) the other party commences negotiations with all or any class of its creditors with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with any of its creditors;

(d) a petition is filed, a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of the other party;

(e) an application is made to court, or an order is made, for the appointment of an administrator, or a notice of intention to appoint an administrator is given or an administrator is appointed, over the other party (being a company);

(f) any other party commits a Data Protection Breach in respect of thedata .

1.36. Each party may terminate this Agreement on [six (6) months] written notice to each other party.

1.37. In the event of expiry or termination of this Agreement, the parties shall cease using the data and return the data to the party that provided it, or at that parties election securely destroy the data and certify such destruction to the providing party. Each party shall also comply with the requirements concerning retention and disposal of data set out in clause 0.

General

1.38. Any proposed changes to this Agreement, including the addition or removal of parties, the purposes of the Data haring or Data Access, the nature or type of data shared or the manner in which the data is to be used must be notified promptly to the relevant Information Governance and Data Quality Leads so that the impact of the proposed changes can be assessed. No variation of this Agreement shall be effective unless it is in writing and signed by all of the parties to this Agreement.

1.39. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.

1.40. This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement. Transmission of an executed counterpart of this agreement (but for the avoidance of doubt not just a signature page) by email (in PDF, JPEG or other agreed format) shall take effect as delivery of an executed counterpart of this Agreement. No counterpart shall be effective until each party has executed at least one counterpart.

1.41. A person who is not a party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

1.42. Each party acknowledges that in entering into this Agreement it does not rely on, and shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement.

1.43. This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England.

1.44. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims), provided that nothing in this clause shall prevent a party from enforcing any judgement obtained in the court of England and Wales in any other court with jurisdiction over the other party.

Data Sharing / Access Details Table

Please complete details for the data sharing and / or data access in the table below:

Controllers and Processors	
Please state the relevant Controllers and Processors	
Controllers: Joint Controllers: Processors: Has due diligence been undertaken on the Processors? **Yes/No**	*Please state the Controllers and whether these are Joint Controllers.* *Please also state if any Processors are or will be engaged by any Controller and whether due diligence has been or will be conducted on the Processors. A copy of any due diligence report may be requested here.* *Please state the parties' registration numbers with the ICO, or state any relevant exemption from registration.*
Data Sharing / Access Details	
Please state the purpose of the data sharing and / or dataaccess	
Click here to enter text.	*Please state the classes of individuals whose Personal Data is being shared / accessed between parties, for example, patients, staff.*
Please state the legal justification / basis for sharing / accessing personal confidential data and / or business confidential data for the purpose of the agreement?	
	For all Personal Data, please specify which GDPR Article 6 condition(s) will be met. *For any Personal Data that is within the Special Categories of Personal Data, please specify which GDPR Article 9 condition(s) will be met. Please specify any additional requirements from the DPA 2018 and how these will be met.* *If Criminal Offence Data will be processed, please identify how the requirements of GDPR Article 10 and DPA 2018 will be met.*
How will the data sharing and/or data access be carried out?	
	Please specify the arrangements for sharing and accessing the data, including reference to Appendix 1 and including: • *the individual in each party who is responsible for oversight of sharing/access* • *which party(ies) are providing* data. • *the mechanism for sharing/access and how this is secure. Which party will have responsibility for ensuring the* data *is secure?* • *how will outputs from the sharing/access will be shared and how this will be secure.*

	• *whether any* data *will be transferred outside the EEA. If Personal Data is to be transferred, please specify how this will be done in compliance with the GDPR.* • *how the sharing/access of data will be recorded.*
Communication with Data Subjects	
	Please state who will provide information to the Data Subjects about the Processing undertaken following the data sharing/access and how this will be communicated. *Please summarise the privacy notices of each party to this Agreement, including weblinks.* *Please state the measures undertaken to ensure that communication with Data Subjects is consistent between the parties to this Agreement. Please state if a single point of contact will be made available for Data Subjects for make queries or exercise their rights under the Data Protection Law. If Personal Data of children is Processed, how will the parties' privacy notices be made accessible.* *Please specify the procedures for dealing with Data Subjects utilising their rights under Chapter III of the GDPR, FOIA access requests, complaints or queries.* *Please specify how the parties will update each other on the amendment, erasure or restriction of the use of shared or accessed Personal Data.* *If there are* ***Joint Controllers****:* • *Specify a single point of contact for Data Subjects and set out in the privacy notice provided to Data Subjects.* • *Specify the Joint Controller responsible for providing privacy notices.* • *State the obligations on each Joint Controller to ensure compliance with the Data Subject's Chapter III rights.* • *State the obligation on each Joint Controller to provide a summary of this agreement to the Data Subjects.*
Benefits of sharing and / or accessing personal data / business confidential data	
Click here to enter text.	*You should address the benefits you aim to achieve for individuals and/or society as a whole.*
Risks of not sharing and / or accessing personal confidential data / business confidential data?	

Click here to enter text	*What might be the consequences for individuals and/or society of not sharing?*
Is a Data Protection Impact Assessment (DPIA) required? If a DPIA is required, please attach a copy.	
Yes/No	*GDPR Article 35 requires a DPIA where the processing is likely to result in a high risk to the rights and freedoms of natural persons.*
Relates to use of patient personal confidential data - Why can the benefits not be achieved by using anonymous / pseudonymised or aggregated data?	
Click here to enter text.	*This question ensures that you have properly considered the necessity of using person-identifiable* data*.*
Relates to use of patient identifiable data - Please state how the common law duty of confidentiality and assurances provided to patients at national level will be met. If you are sharing with the consent of the individuals concerned, how will that consent be obtained and recorded? How can you demonstrate compliance of individual rights? (Right of access, Right to rectification and right to erasure, right to restriction of processing, right to object?)	
Click here to enter text.	*To comply with the common law of confidentiality and national assurances, patient identifiable data should only be shared if one of following conditions are met:* • *the sharing is to provide health and social care;* • *the sharing is covered by a section 251 authorisation;* • *the sharing is through NHS Digital;* • *the Data Subject has given their informed and express consent.* *If the sharing is under the patient's consent, please attach a copy of consent form(s) and specify (if applicable) any procedure for children or patients who lack capacity. Ensure that consent procedures of each organisation are covered if they differ from each other.* *Please state if the sharing of* data *will interfere with Article 8 of the Human Rights Act (right to respect for private and family life) and if so, please state why it is necessary and proportionate to do so.*
Relates to use of patient identifiable data - In what circumstances (if any) might you share without consent or if consent is refused? How will the decision to disclose be recorded?	
Click here to enter text.	*Please state statute / legislation which allows data to be shared and / or risk assessment process.*
Relates to use of patient identifiable data - Except in the most exceptional circumstances (and where there is a legal exemption) individuals must be informed which organisations are sharing their personal data and for what purpose. How will patients be informed of the data sharing or data access, for example Privacy notices, fair processing	

statements, statements on website?	
Click here to enter text.	*This might already be covered through a standard privacy notice or fair processing notice. If so, give details of where a copy is available.* *Different parties to the agreement might have different approaches so ensure you cover arrangements for all parties.*
Data Protection Officers	
	Please specify the name and contact details of the Data Protection Officer for each party.

Data quality Organisations sharing data and / or allowing access to data will take steps to ensure the data is accurate and, where necessary, up to date. If shared data is found to be inaccurate, it is the responsibility of the organisation discovering the inaccuracy to notify the originating organisation. The originating organisation will ensure that the source data is corrected and will notify all recipients, who will be responsible for updating the data they hold.
Please state how data will be checked within the organisations to ensure it is accurate, reliable and up to date and who will make changes if data is not correct?

Click here to enter text.	*For example, spelling of names, correct addresses details. Who will amend records if data is inaccurate?*

Retention and disposal of data Parties to this agreement undertake to retain data received for no longer than necessary and to dispose of it securely when it is no longer needed. Where the purpose of the information sharing means that shared data will become part of the receiving organisation's record for the individual concerned, organisations undertake to maintain an up to date retention and disposal schedule. Please note if you are accessing / viewing data this does not apply. **Give details of the agreed retention periods that apply to this data below, including, where relevant, details of where a copy of each organisation's retention and disposal schedule can be obtained.**
Click here to enter text.
Give details of the agreed method(s) of the destruction / removal of access to the data, once the agreement has lapsed and the period of retention has ended.
Click here to enter text.

Storage of Data
Storage of datareceived must comply with Article 5 of the Data Protection Act 2018 (adequate security). **Please state where the data will be held, for example physical location / electronic location and method of storage.**

Click here to enter text.

Individual's data rights (only answer if dealing with patient personal confidential data)
This section must provide enough information to answer the following questions:

- Who is responsible for dealing with individuals' concerns or queries in each organisation?
- Who is responsible for dealing with individuals' Right of access, Right to rectification and right to erasure, right to restriction of processing, right to object?
- What complaints contacts exist for each organisation?

Parties to this agreement will comply with the rights of individuals under the Data Protection Act 2018, GDPR and (for public authorities) the Freedom of Information Act 2000. It is recommended that this agreement is published through the Freedom of Information publication scheme of each public authority other than in exceptional circumstances agreed by all parties

Contact details for individuals to exercise their DPA 2018 and FOIA rights:

Organisation	DPA contact details	FOI contact details
Click here to enter text.	Click here to enter text.	Click here to enter text.

Complaints (only answer if dealing with patient personal confidential data)
Organisations will use their standard organisational procedures to deal with privacy/data protection complaints from the public arising from data sharing / accessing under this agreement and will co-operate (with the complainant's permission) where complaints relate to more than one party.

Contact details for individuals wish to complain about data sharing:

Organisation	Complaints contact details	Location of complaints procedure
Click here to enter text.	Click here to enter text.	Click here to enter text.

Signatories

This Agreement is agreed between the parties by the signature of their authorised signatories below:

	Signed for and on behalf of: [Party 1]	**Signed for and on behalf of: [Party 1]**
Name:		
Organisation and Position:		
Signature:		
Date:		

Appendix 1 - Data Items Table

Purpose: [insert purpose]

Please indicate the Data Items which are to be shared / accessed between the parties.

Personal Data – please click on the box to state which data items are to shared / accessed between parties		
Type	***Click in box below***	***Details***
Forename(s)	☐	Click here to enter text.
Surname	☐	
Address	☐	
Postcode	☐	
Date of Birth	☐	
Gender	☐	
Telephone Numbers	☐	
Email address	☐	
NHS Number	☐	
Special Categories of Personal Data – please click on the box to state which Data Items of Special Categories of Personal Data are to shared / accessed between parties (includes special category as defined by DPA 2018(Article 9) and data generally considered sensitive)		
Type	***Click in the box below***	***Details***
Physical or mental health	☐	
Social care	☐	
Criminal activity	☐	
Racial or ethnic group	☐	
Financial	☐	
Religious beliefs or similar	☐	
Political opinions	☐	
Sexual life	☐	
Trade union membership	☐	
NHS Number	☐	
Hospital Number	☐	
Social Care Reference	☐	
NI Number	☐	
Health Care Records (if applicable) – please click in the box which data items are to be shared / accessed between parties		
Type	***Click in***	***Details***

	the box below	
Patient Alerts (Inc. risks)	☐	
Casenotes (paper)	☐	
Electronic Health Records	☐	
Laboratory Results	☐	
Third Party Information	☐	
Pharmacy Notes	☐	
Occupational Therapy Notes	☐	
Speech Therapy Notes	☐	
Physiotherapy Notes	☐	
Risks Assessments	☐	

Please state below details of other data to be shared / accessed which is not covered above

Type	***Details***

Appendix 2 – Data Flow Mapping

Purpose: [insert purpose]

The following table should be completed to document how data is shared and / or accessed.

Data	From	To	Method of Transfer of Data or Access to Data	Frequency
Example	*Organisation1*	*Organisation 2*	*Electronic, Hard copy, Safe Haven Fax, Email etc and state how it will be sent securely (e.g. encrypted, recorded delivery, courier)*	*Daily, weekly or monthly etc or by the 12th of each month*

Appendix 3 – Designated Data Sharing / Access Personnel

Purpose: [insert purpose]

This table details all the staff who are involved in the Data Sharing or Data Access from each party.

Organisation	Designated Person(s) and Position Held	Contact Details:
Click here to enter text.	Click here to enter text.	Click here to enter text.