

# Information Sharing / Access Agreement

<b>Policy Number</b>	<b>IG018</b>
<b>Target Audience</b>	<b>All staff</b>
<b>Approving Committee</b>	<b>CCG Chief Officer</b>
<b>Date Approved</b>	<b>July 2018</b>
<b>Last Review Date</b>	<b>July 2018</b>
<b>Next Review Date</b>	<b>July 2020</b>
<b>Policy Author</b>	<b>GMSS IG Team</b>
<b>Version Number</b>	<b>1.0</b>

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

<b>Version</b>	<b>Date</b>	<b>Reviewed By</b>	<b>Comment</b>
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

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

## INFORMATION SHARING / ACCESS AGREEMENT

<b>Information Sharing Partners Between</b>	<i>To be completed</i>
<b>Purpose:</b>	<i>[This Agreement should only be used to share information for Controller to Controller arrangements and not for sharing information with Processors]</i>
<b>Version No:</b>	<i>To be completed</i>
<b>Commencement Date:</b>	<i>To be completed</i>
<b>Date for Review:</b>	<i>To be completed</i>
<b>Author(s)</b>	<i>To be completed</i>

## Table of Contents

1.	Introduction .....	5
2.	Definitions and Interpretation.....	5
3.	Purpose .....	8
4.	Security and Training .....	8
5.	Personal Breaches and Reporting Procedures .....	9
6.	Confidentiality, Consent and Information Sharing / Access Principles .....	9
7.	Monitoring .....	12
8.	Restrictions on Use of Information Shared / Accessed.....	12
9.	Term and Termination.....	12
10.	General.....	13
11.	Data Sharing / Access Details Table.....	15
12.	Signatories.....	20
	Appendix 1 - Data Items Table.....	21
	Appendix 2 – Data Flow Mapping.....	23
	Appendix 3 – Designated Data Sharing / Access Personnel.....	24

## 1. Introduction

In accordance with the requirements of the relevant law and guidance, this Information Sharing / Access Agreement provides a formal agreement between all parties to it, to share Information and / or access Information of another party and to fulfil their respective obligations whilst maintaining the duty of confidentiality and the patient's right to privacy. This Information Sharing / Access Agreement should be used for sharing information with Processors and so for the purposes of the Data Protection Legislation, each party shall be a Controller of the Personal Data in the Information which is shared or accessed pursuant to this Agreement.

This Information Sharing / Access 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 (May 2011).
- The Information Governance Review (March 2013).
- National Data Guardian Report (2017).

This Information Sharing / Access Agreement is also additional to any further agreements in place between the parties relating to the Information Sharing and/or Information Access. In the event of any conflict between such further agreements and this Information Sharing / Access Agreement, this Information Sharing / Access Agreement shall prevail.

## 2. Definitions and Interpretation

- 2.1. The definitions and rules of interpretation in this clause 2 shall apply in this Agreement.

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

**Information Access** means where a party to this Agreement accessing data from one of more of the other 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 information (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 Information 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 Information.

**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 Information, 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 9.

- 2.2. 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.
- 2.3. Unless the context otherwise, requires, words in the singular shall include the plural and in the plural, shall include the singular.
- 2.4. A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.
- 2.5. 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.

### **3. Purpose**

- 3.1. This Agreement sets out the framework for the Information Sharing and / or Information 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.

### **4. Security and Training**

- 4.1. A party shall only share or provide access to Information to another party by using secure methods as set out in clause 11.
- 4.2. 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 information; and
    - (ii) the accidental loss or destruction of, or damage to, the Personal Data in the Information;
  - (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.
- 4.3. 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 11. The parties shall keep such security measures under review



and shall carry out such updates as they agree are appropriate throughout the Term.

## **5. Personal Breaches and Reporting Procedures**

- 5.1. 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).
- 5.2. 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.

## **6. Confidentiality, Consent and Information Sharing / Access Principles**

- 6.1. 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 and Information.
- 6.2. Each party will endorse, support and promote the accurate, timely, secure and confidential sharing of both Patient Identifiable Data and anonymised Information (including without limitation Personal Data) where such Information sharing is essential for the care and treatment of patients.
- 6.3. The parties are fully committed to ensuring that if they share Information it 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.
- 6.4. The parties acknowledge the requirements that apply to the sharing of Information concerning 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 Information concerning patients who lack capacity to consent should be clearly recorded.
- 6.5. Where a party requests that Information 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.
- 6.6. Information 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.
- 6.7. 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 Information shared will be transferred, received, used, held and disposed of securely.
- 6.8. 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 Information 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 Information. 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 information they 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.

6.9. 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 information and work in a manner consistent with these procedures;
- (b) provide advice and guidance to staff requiring support in appropriately handling information 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 information sharing 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 information within the organisation, as well as personal information flows to other NHS and non-NHS organisations;
- (b) overseeing the establishment of procedures governing access to, and the use of, personal information and, where appropriate, the transfer of that information 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.
- 6.10. The parties are responsible for putting in place effective procedures to address complaints relating to the disclosure of Information, and information about these procedures should be made available to patients, as set out in clause 11.
  - 6.11. Where it is agreed that the sharing / accessing of Information is to be undertaken, only that Information which is needed and relevant will be shared / accessed and that would only be on a "need to know" basis.
  - 6.12. 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.
  - 6.13. 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.
  - 6.14. Personal Data must be kept accurate and up to date to comply with Article 5 of the GDPR.
  - 6.15. 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.
  - 6.16. 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.
  - 6.17. 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.

6.18. Each party receiving Information from another party shall:

- (a) keep the Information confidential; and
- (b) not use or exploit the Information in any way, except for the Purpose.

6.19. Each party may disclose the Information 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.

## **7. Monitoring**

7.1. 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.

## **8. Restrictions on Use of Information Shared / Accessed**

8.1. All Shared Information and Accessed Information, 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.

8.2. The parties acknowledge that

- (a) restrictions may also apply to any further use of Information that is not Personal Data, such as due to commercial sensitivity or prejudice to individuals may be caused by the Information's release, and this should be considered when considering secondary use for such Information. If in doubt the Information Asset Owner should be consulted.
- (b) Additional statutory restrictions apply to the disclosure of certain Information for example, information regarding a patient's HIV and AIDS status, assisted conception and abortion, or child protection.

## **9. Term and Termination**

9.1. 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.

9.2. 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 the Information.
- 9.3. Each party may terminate this Agreement on [six (6) months] written notice to each other party.
- 9.4. In the event of expiry or termination of this Agreement, the parties shall cease using the Information and return the Information to the party that provided it, or at that parties election securely destroy the Information and certify such destruction to the providing party. Each party shall also comply with the requirements concerning retention and disposal of Information set out in clause 11.

## **10. General**

- 10.1. Any proposed changes to this Agreement, including the addition or removal of parties, the purposes of the Information Sharing or Information Access, the nature or type of Information shared or the manner in which the Information 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.
- 10.2. 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.
- 10.3. 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.
- 10.4. 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.

- 10.5. 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.
- 10.6. 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.
- 10.7. 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.

## 11. Data Sharing / Access Details Table

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

<b>Controllers and Processors</b>	
Please state the relevant Controllers and Processors	
Controllers: Joint Controllers: Processors: Has due diligence been undertaken on the Processors? <b>Yes/No</b>	<p><i>Please state the Controllers and whether these are Joint Controllers.</i></p> <p><i>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.</i></p> <p><i>Please state the parties' registration numbers with the ICO, or state any relevant exemption from registration.</i></p>
<b>Data Sharing / Access Details</b>	
Please state the purpose of the information sharing and / or information access	
Click here to enter text.	<i>Please state the classes of individuals whose Personal Data is being shared / accessed between parties, for example, patients, staff.</i>
Please state the legal justification / basis for sharing / accessing personal confidential information and / or business confidential data for the purpose of the agreement?	
	<p><i>For all Personal Data, please specify which GDPR Article 6 condition(s) will be met.</i></p> <p><i>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.</i></p> <p><i>If Criminal Offence Data will be processed, please identify how the requirements of GDPR Article 10 and DPA 2018 will be met.</i></p>
How will the information sharing and/or information access be carried out?	
	<p><i>Please specify the arrangements for sharing and accessing the information, including reference to Appendix 1 and including:</i></p> <ul style="list-style-type: none"> <li><i>• the individual in each party who is responsible for oversight of sharing/access</i></li> <li><i>• which party(ies) are providing information.</i></li> <li><i>• the mechanism for sharing/access and how this is secure. Which party will have responsibility for ensuring the information is secure?</i></li> <li><i>• how will outputs from the</i></li> </ul>

	<p><i>sharing/access will be shared and how this will be secure.</i></p> <ul style="list-style-type: none"> <li>• <i>whether any information 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.</i></li> <li>• <i>how the sharing/access of information will be recorded.</i></li> </ul>
<p>Communication with Data Subjects</p>	
	<p><i>Please state who will provide information to the Data Subjects about the Processing undertaken following the information sharing/access and how this will be communicated.</i></p> <p><i>Please summarise the privacy notices of each party to this Agreement, including weblinks.</i></p> <p><i>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.</i></p> <p><i>Please specify the procedures for dealing with Data Subjects utilising their rights under Chapter III of the GDPR, FOIA access requests, complaints or queries.</i></p> <p><i>Please specify how the parties will update each other on the amendment, erasure or restriction of the use of shared or accessed Personal Data.</i></p> <p><i>If there are <b>Joint Controllers</b>:</i></p> <ul style="list-style-type: none"> <li>• <i>Specify a single point of contact for Data Subjects and set out in the privacy notice provided to Data Subjects.</i></li> <li>• <i>Specify the Joint Controller responsible for providing privacy notices.</i></li> <li>• <i>State the obligations on each Joint Controller to ensure compliance with the Data Subject's Chapter III rights.</i></li> <li>• <i>State the obligation on each Joint Controller to provide a summary of this agreement to the Data Subjects.</i></li> </ul>
<p>Benefits of sharing and / or accessing personal information / business confidential data</p>	
<p>Click here to enter text.</p>	<p><i>You should address the benefits you aim to achieve for individuals and/or society as a whole.</i></p>



Risks of not sharing and / or accessing personal confidential information / 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 information.*

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 information 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 information and for what purpose.

How will patients be informed of the information sharing or information 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 information and / or allowing access to information will take steps to ensure the information is accurate and, where necessary, up to date. If shared information 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 information 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 information

Parties to this agreement undertake to retain information 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 information 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 information this does not apply.

**Give details of the agreed retention periods that apply to this information 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 information, once the agreement has lapsed and the period of retention has ended.**

[Click here to enter text.](#)

**Storage of Information**

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

[Click here to enter text.](#)

**Individual’s information 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:

<b>Organisation</b>	<b>DPA contact details</b>	<b>FOI contact details</b>
<a href="#">Click here to enter text.</a>	<a href="#">Click here to enter text.</a>	<a href="#">Click here to enter text.</a>

**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 information 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 information sharing:

<b>Organisation</b>	<b>Complaints contact details</b>	<b>Location of complaints procedure</b>
<a href="#">Click here to enter text.</a>	<a href="#">Click here to enter text.</a>	<a href="#">Click here to enter text.</a>

## 12. Signatories

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

	<b>Signed for and on behalf of:</b> <b>[Party 1]</b>	<b>Signed for and on behalf of:</b> <b>[Party 1]</b>
<b>Name:</b>		
<b>Position:</b>		
<b>Signature:</b>		
<b>Date:</b>		

## 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

<i>Type</i>	<i>Click in box below</i>	<i>Details</i>
Forename(s)	<input type="checkbox"/>	Click here to enter text.
Surname	<input type="checkbox"/>	
Address	<input type="checkbox"/>	
Postcode	<input type="checkbox"/>	
Date of Birth	<input type="checkbox"/>	
Gender	<input type="checkbox"/>	
Telephone Numbers	<input type="checkbox"/>	
Email address	<input type="checkbox"/>	
NHS Number	<input type="checkbox"/>	

### 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)

<i>Type</i>	<i>Click in the box below</i>	<i>Details</i>
Physical or mental health	<input type="checkbox"/>	
Social care	<input type="checkbox"/>	
Criminal activity	<input type="checkbox"/>	
Racial or ethnic group	<input type="checkbox"/>	
Financial	<input type="checkbox"/>	
Religious beliefs or similar	<input type="checkbox"/>	
Political opinions	<input type="checkbox"/>	
Sexual life	<input type="checkbox"/>	
Trade union membership	<input type="checkbox"/>	
NHS Number	<input type="checkbox"/>	
Hospital Number	<input type="checkbox"/>	
Social Care Reference	<input type="checkbox"/>	
NI Number	<input type="checkbox"/>	

### Health Care Records (if applicable) – please click in the box which data items are to be shared / accessed between parties

<i>Type</i>	<i>Click in</i>	<i>Details</i>
-------------	-----------------	----------------

	<b><i>the box below</i></b>	
Patient Alerts (Inc. risks)	<input type="checkbox"/>	
Casenotes (paper)	<input type="checkbox"/>	
Electronic Health Records	<input type="checkbox"/>	
Laboratory Results	<input type="checkbox"/>	
Third Party Information	<input type="checkbox"/>	
Pharmacy Notes	<input type="checkbox"/>	
Occupational Therapy Notes	<input type="checkbox"/>	
Speech Therapy Notes	<input type="checkbox"/>	
Physiotherapy Notes	<input type="checkbox"/>	
Risks Assessments	<input type="checkbox"/>	

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

<b><i>Type</i></b>	<b><i>Details</i></b>

## Appendix 2 – Data Flow Mapping

**Purpose:** [insert purpose]

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

Data	From	To	Method of Transfer of Information or Access to Information	Frequency
<i>Example</i>	<i>Organisation 1</i>	<i>Organisation 2</i>	<i>Electronic, Hard copy, Safe Haven Fax, Email etc and state how it will be sent securely (e.g. encrypted, recorded delivery, courier)</i>	<i>Daily, weekly or monthly etc or by the 12<sup>th</sup> of each month</i>

### Appendix 3 – Designated Data Sharing / Access Personnel

**Purpose:** [insert purpose]

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

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