SCHEDULE 1 - GLOUCESTERSHIRE SPECIFIC INFORMATION SHARING AGREEMENT

Gloucestershire Integrated Care System (ICS) – Integrated Care, Planning and Public Health Intelligence 'SISA'.

Introduction

The Specific Information Sharing Agreement (SISA) is used to outline the specific requirements of the data sharing arrangements under the overarching data sharing protocol known as the Gloucestershire Information Sharing Partnership Agreement.

This Specific Information Sharing Agreement and the organisations involved will be bound to all requirements, Terms and Conditions of the overarching data sharing protocol for the duration of this agreement.

All parties involved must have registered their commitment to the principles and agreed to the terms and Conditions of the overarching data sharing protocol in writing by completing the Declaration of Acceptance and Participation form (for GISPA) and returning it to DPO@gloucestershire.gov.uk.

This SISA is being established between the health and social care organisations across the Gloucestershire Integrated Care System (ICS) for the purposes of supporting: **Integrated Care, Planning and Public Health Intelligence.**

The SISA and accompanying Data Protection Impact Assessment (DPIA) template and Joint Controller Agreement (JCA) template are to be used where three or more organisations in the ICS are establishing data sharing. It can also be used between two organisations sharing data.

Please note that the Specific Information Sharing Agreements form an important part of our data sharing framework. However, they should not be viewed in isolation. These documents are just one component of a broader suite of governance tools and documentation required to ensure full compliance with data protection and information governance obligations. This SISA alone does not provide sufficient assurance to enable data sharing without other relevant parts of the sharing framework such as Data Protection Impact Assessments being put in place.

DPIAs for activities conducted under this SISA will be published.

This Data Sharing Agreement covers the processing of personal data for the purposes of integrated care, planning and public health intelligence, as outlined under the 'Purposes' section. It does not extend to the processing of data for safeguarding or welfare-related activities, as these are governed by separate, well-established arrangements that have demonstrated their effectiveness. Any future developments or amendments to this Agreement, including potential inclusion of additional purposes, will be communicated to all partner organisations in a timely manner.

Commencement Date:	**End Date:**
	n/a

Version	**Date**	**Author**	**Details**
V0.1	17/03/2025	Antje Carpenter, SCW	First draft for consideration.
V0.2	21/05/2025	Antje Carpenter, SCW	Feedback consideration from IG working groups
V0.3	23/05/2025	Antje Carpenter, Adam Horton-Tuckett, SCW	Final update before customer consultation.
V0.4	30/06/2024	Antje Carpenter, Adam Horton-Tuckett, SCW	Updates following consultation calls with each partner organisation.
V0.5	08/07/2025	Antje Carpenter	Clean version
V0.6	13/08/2025	Adam Horton-Tuckett	Renaming & minor feedback inclusion
V1.0	11/09/2025	Antje Carpenter	Final approved version

1. Parties to this Agreement

Health and Care organisations within the Integrated Care System in Gloucestershire. A list of signatories will be managed as an **Appendix 3** accessible to all relevant partners.

(Each one 'a Party' or together 'the Parties')

2. Agreed Purpose

2.1 This Specific Information Sharing Agreement (SISA) sets out the details for the sharing of Personal Data when one Controller discloses Personal Data to another Controller or when organisations collaborate as 'joint controllers' of data. This is used in conjunction with the overarching data sharing protocol (GISPA) that defines the principles and procedures that the Parties shall adhere to and the responsibilities the parties owe to each other.

2.2 The Parties consider this data sharing necessary to fulfil their responsibilities to provide system management functions, including the following 'sub-purposes'. The full list is set out and maintained in **Appendix 1**:

1. **Discharges and Discharge Planning and Management**
2. **Cohort Finding**
3. **Screening**
4. **Vaccination and Immunisation Management**
5. **Medication Usage and Outcomes Reviews**
6. **Individual Care Requirements**
7. **Targeted Interventions**
8. **Prevention and Wellness**
9. **Care Delivery Outcomes and Quality Improvements**
10. **Variations in Care and Referral Practice**
11. **Service Evaluation**
12. **Planning and Modelling Demand and Capacity**
13. **Public Communications**
14. **Local and National Programmes Planning, Assessment and Reporting**
15. **Pathway and Service Management**
16. **System-wide Bed State**
17. **System Flow Management**
18. **Commissioning Planning**
19. **Performance Management**
20. **Preparation and Submission of National Returns**

The list above (and in **Appendix 1**) may be used in any care setting or scenario, including, but not limited to, use of shared data in organisational care settings/services/teams and collaborative service delivery across organisations, such as Multi-disciplinary Teams (MDTs), Integrated Neighbourhood Teams (INTs) or alike.

2.3 The Parties agree to only Process Shared Personal Data, as described in any relevant DPIAs for the following objectives:
- **To improve population health through the targeting of services.**

- For the planning and improvement of services.
- For the research and innovation that will power new medical treatments.

2.4 The Parties shall not Process Shared Personal Data in a way that is incompatible with the purposes described in this clause 2 (**Agreed Purpose**).

2.5 In some situations, one party might share its Personal Data with the other. If that happens, the rules in this Agreement will apply as if the roles were reversed—meaning the receiving party is treated as the disclosing party and vice versa, specifically for that Personal Data.

3. Shared Personal Data

3.1 The following types of Personal Data will be shared between the Parties during the Term of this Agreement (DPIA for specific activity will confirm in detail):

- **Personal Data** (as defined in the UK GDPR)
- **Pseudonymous Data** (using a secure and documented process, ensuring that re-identification is only possible with separately stored and access-controlled information. Method, tools used, and access controls must be documented in the DPIA.)
- **Anonymised Data** (if truly anonymised a Data Sharing Agreement is not required, however the activities this SISA supports are likely to include personal data that during use becomes anonymised, hence it is included for this reason.)

3.2 The following types of Special Categories of Personal Data may be shared between the Parties during the Term of this agreement:

- **Health and Social Care data**
- **Genetic data**
- **Racial or Ethnic Origin data**
- **Data concerning a person's sex life and/or sexual orientation**
- **Religious or philosophical beliefs**

3.3 Further detail on the Shared Personal Data as described in clause 3.1, and clause 3.2, is set out in the **relevant DPIA for the activity** together with any access and processing restrictions as agreed and established by the Parties.

3.4 The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.

4. Lawfulness and Transparency of Processing

4.1 Each Party shall ensure that it processes the Shared Personal Data fairly, transparently, and lawfully during the Term of this Agreement.

4.1.1 Each Party must give due consideration the completion of a Data Protection Impact Assessment (individual or joint as required) as it remains a critical and potentially legally required step even with the streamlined SISA process. This is to ensure a comprehensive understanding and compliance with data protection obligations. For shared data assets a single DPIA co-developed and shared should be produced.

4.1.2 Each party accessing NHS patient data must complete the Data Security and Protection Toolkit (DSPT) annually. If a partner organisation does not meet the DSPT standards, details of areas of non-compliance will be requested to be disclosed to the Gloucestershire IG Group (GIGG), or any successor committee, to assess any potential risks around data sharing. GIGG will collectively assess any risk identified and agree an action plan and timescale to address the risk(s). Any ongoing concerns may be subject to the escalation process set out in section 8.

4.2 Each Party agrees that the legitimate grounds under the Data Protection Legislation for the processing of Shared Personal Data are:

4.2.1 Article 6 – Processing of Personal Data

c) processing is necessary for compliance with a legal obligation to which the Controller is subject

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller

The above noted lawful bases for the processing of personal data for integrated care planning and public health intelligence are most likely to be the most appropriate. However, for any specific sharing initiatives, the appropriate legitimate grounds will be determined in the relevant associated DPIA.

4.2.2 Article 9 – Processing of Special Category Data

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by UK law

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) Processing is necessary for reasons of substantial public interest

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

The above noted lawful bases for the processing of personal data for integrated care planning and public health intelligence are most likely to be the most appropriate. However, for any specific sharing initiatives, the appropriate legitimate grounds will be determined in the relevant associated DPIA.

A list of relevant legislation is available under **Appendix 2**.

4.2.3 Data Protection Act 2018 - Schedule 1 DPA conditions
- 1 Employment, social security and social protection
- 2 Health or Social Care purposes
- 3 Public Health

4.2.4 Data Protection Act 2018, Exemptions from the UK GDPR - Schedule 2,3,4

Any exemptions under DPA 2018 will be noted in the relevant associated DPIA.

4.2.5 The NHS National Data Opt-Out **might** apply to the agreed sharing of data. Specific sharing initiatives will be assessed against the requirement to apply the National Data Opt Out within the relevant DPIA.

4.2.6 Compliance with Common Law Duty of Confidentiality

a) Consent: **The default for uses of data under this SISA should be to use anonymised/aggregated or strongly pseudonymised data where possible. Some purposes may have a direct care output, for which the processing can be an implied consent.**

Where anonymisation/pseudonymisation is not possible for processing that is not direct care, the options of consent or support of NHS Act 2006, section 251 (approved by national Confidentiality Advisory Group) will be utilised as appropriate.

DPIAs conducted for sharing initiatives will address the specific circumstances.

b) Statutory Gateway: All public sector organisations signed to this SISA will have responsibilities to assure the effectiveness, improve the delivery of care services, tackle inequalities, e.g. **Health & Care Act 2022**, section 14Z34 'Duty as to improvement in quality of services' on Integrated Care Boards or **Care Act 2014**, section 1 duty on Local Authorities to promote individual well-being.

The DPIA for the specific processing initiative will detail any applicable statutory gateways.

Statutory Gateways apply directly to public sector organisations. They also apply where a non-public authority is providing services under contract to a public authority. The DPIA for the sharing activity will include the relevant detail and address any requirements with non-public sector partners as needed.

4.2.7 Human Rights Act Article 8 Right to Privacy

Interference justified as processing is lawful, necessary and proportionate to provide the managements of systems/services delivering direct care and assessed via DPIA,

4.3 The Parties agree that the data shall be processed fairly and transparently by:

- Providing an up-to-date Privacy Policy/Privacy Notice to Data Subjects

- Signage/Information Leaflets provided to Data Subjects

- Other: verbal and/or written communication

Initiative specific details will be considered and set out in the associated DPIA.

5. Data Quality

5.1 The party/ies sharing data shall take all reasonable steps to ensure that before the Commencement Date, Shared Personal Data are accurate and that it has appropriate internal procedures in place for the party/ies receiving or accessing data to sample Shared Personal Data prior to the Commencement Date and it will update the same if required prior to transferring/or providing access to the Shared Personal Data.

5.2 Shared Personal Data must be limited to the Personal Data described in clause 3.1 and clause 3.2 and any specific initiative DPIA.

5.3 Data quality expectations must be outlined in the relevant DPIA.

6. Data Retention and Deletion

6.1 Shared Personal Data must only be retained for as long as necessary to fulfil the agreed purposes, unless statutory or professional retention requirements apply. Specific retention details will be outlined in the associated DPIA.

7. Notification of Data Subject Requests and Personal Data Breaches

7.1 Where one of the Parties receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Shared Personal Data, the receiver of that request shall:

7.1.1 As individual controllers: promptly, after receiving the request, manage it under considerations and in compliance with legal deadlines and requirements and in consultation with the source organisation if required.

7.1.2 As joint controllers: promptly, after receiving the request, jointly manage it under consideration and in compliance with legal deadlines and requirements and local established processes on how to handle Data Subject Requests and in consultation with the source organisations if required.

7.1.3 Where the request relates to a jointly controlled shared asset, the organisation receiving the request will lead the response, engaging with other joint controllers as required, particularly on application of exemptions.

7.1.4 Where the request relates to jointly controlled data on an asset 'owned/managed' by one of the controllers, that controller will lead the response, whether they have received the request or not. If the recipient is a different joint controller, they will inform and consent the requestor to pass over the request. It will be passed to the contact point listed on the lead controller's privacy notice for data subject requests (or their Data Protection Officer if such contact is not clear). This principle is set on the basis the 'owner' of the asset is best placed to manage the system with response to the request. As in 7.1.3 above the responder will engage with the other joint controllers as required.

7.1.5 All parties must consider exemptions for health and social care data which might apply if disclosing the information would likely cause serious harm to the physical or mental health of any individual, as outlined in the data Protection Act 2018. Exemptions concerning health data must be applied consulting the opinion of appropriate healthcare professional(s) ensuring that the serious harm test is assessed appropriately.

7.1.6 Any detailed policies, procedures or Standard Operating Procedures (if relevant) applicable for the response to Individual's Rights must be considered as required, identified in the DPIA for the sharing activity.

7.2 The Parties shall promptly notify one another upon becoming aware of any Personal Data Breach relating to the Shared Personal Data and shall:

7.2.1 Do all such things as reasonably necessary to assist in mitigating the effects of the Personal Data Breach.

7.2.2 Implement any measures necessary to restore the security of any compromised Shared Personal Data.

7.2.3 Work with each other to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein). The party identified as or considered to be the source of the breach at this stage shall be responsible for reporting the incident.

7.2.4 Not do anything which may damage the reputation of the Parties to this agreement or their relationships with the relevant Data Subjects, save as required by Law.

7.3 Where a Party identifies that Shared Personal Data is inaccurate and the inaccuracy is more likely than not to have a significant impact on the service provided to the individual, the Parties shall notify each other as soon as possible but no later than 3 working days after identification.

7.3.1 Work collaboratively to rectify the inaccurate data and establish any impact to the processing activities or the rights and freedoms of the concerned Data Subjects.

7.3.2 Work collaboratively to assess the risks associated with the inaccurate data and assist the other Party in identifying this.

7.3.3 The party where the inaccurate data originates from shall identify where the inaccuracy originated and take the necessary action to prevent future occurrences.

8. Escalation of concerns

8.1 Parties shall aim to resolve all concerns, differences and questions by means of cooperation and consultation.

8.2 If any concern arises, the Parties in involved must first attempt to settle it with a written offer of negotiation by any of the Parties to the other Parties. During the following 15 business days period each of the Parties involved must negotiate and be represented:

a) for the first 10 business days, by a senior person (defaults to the organisations senior responsible officer nominated in the DPIA for the activity in question) who where practicable has not had any direct day-to-day involvement in the matter and has authority to settle the dispute; and

b) for the last 5 business days, by their chief executive, director, or equivalent senior individual who has authority to settle the dispute.

8.3 Where practicable, no Party in dispute should be represented by the same individual for the different stages described above.

8.4 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.

9. Variation

9.1 No variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

10. Review

10.1 The parties shall review this SISA **annually**, having consideration to the aims and purposes set out in clause 2.1 and clause 0.

10.2 The review of the effectiveness of the SISA will involve:

a) assessing whether the purposes for which the Shared Personal Data is being processed are still the ones listed in this Agreement;

b) assessing whether the Shared Personal Data is still as listed in clause 3.1 and clause 3.2 of this Agreement;

10.3 In addition, the DPIAs for sharing activities created with regard to this SISA will set review periods as appropriate to the risks within the DPIAs themselves.

11. Supplementary Documents

11.1 This agreement is to be supplemented by appropriate supporting documents: **n/a**

12. Signature of agreement

When signing this agreement on behalf of
I confirm that the terms set out above are agreed. I assert and confirm satisfactory compliance with the Data Security & Protection Toolkit compliance requirements (section 4.1.2).

I confirm that the organisation has sufficient processes in place to support review and approval of governance documents related to sharing activities conducted under this agreement, including review of data protection impact assessments, joint controller arrangements and data processing agreements.

Signature:

Name:

Role:
(e.g.Caldicott Guardian/SIRO/Partner/Director/Designated Officer/DPO)

Date:

13. Document Information

Document owner:	Nicky Birkby
Next review date:	August 2026
Version:	1.0
Summary of changes:	n/a

APPENDIX 1 – ADDITIONAL INFRMATION ON PURPOSES FOR PROCESSING

APPENDIX 1 V1.1.docx

APPENDIX 2– LEGAL GATEWAY MATRIX

APPENDIX 2 V1.0.doc

APPENDIX 3 – LIST OF SIGNATORIES

n/a