Healthier Together
Improving health and care in Bristol, North Somerset and South Gloucestershire

NHS
Bristol, North Somerset and South Gloucestershire
Integrated Care Board

BNSSG ICS Information Sharing Charter

The framework to establish effective information sharing in support of health and care services.

January 2025

Healthier Together
Improving health and care in Bristol, North Somerset and South Gloucestershire

Executive Summary

NHS
Bristol, North Somerset and South Gloucestershire
Integrated Care Board

It is essential that health and care organisations within Bristol, North Somerset and South Gloucestershire (BNSSG) share information to deliver high quality and safe care and protect the privacy and security of that information.

All organisations seek to do this through a risk mitigation approach to information sharing, to ensure safe practices are adopted and to build trust with stakeholders. Assurances are sought from receiving organisations that are regularly reviewed and updated to adapt to changes in technology, regulations and organisational processes.

As a way of standardising and streamlining these assurances and reducing individual organisational effort, information sharing frameworks are adopted in sectors, such as healthcare, where collaboration and timely sharing of information is essential for high quality and safe patient care. Without effective information sharing it is not possible for our Integrated Care System (ICS) to deliver its potential benefits to our local population.

This document describes the proposed Information Sharing Charter being developed within BNSSG that balances the need for information exchange to enhance the provision of care with the imperative to protect privacy, security, and compliance with relevant legal and regulatory obligations.

Healthier Together
Improving health and care in Bristol, North Somerset and South Gloucestershire

Information Sharing Charter Overview

NHS
Bristol, North Somerset and South Gloucestershire
Integrated Care Board

Purpose and Scope

The **BNSSG Information Sharing Charter** (the Charter) is the overall commitment to enable sharing information between the organisations that make up the BNSSG ICS. It is supported by a **Framework** of documents that support and enable information sharing. Organisations signal their willingness to become a Member of the Charter by signing the **Membership Agreement**.

The primary purpose of this Charter is to move the approach to information sharing across BNSSG from one where each individual project or service requires individual agreements and documentation to a more purpose based (e.g. Population Health Management, Commissioning or Public Health) approach. In this new approach, agreements and supporting documents are standardised: this will mean that proposed individual projects and/or services involving information sharing which falls within the scope of an existing approved purpose do not require individual agreement and documentation. This should reduce the number of documents and signatures required while still maintaining privacy and transparency.

This Charter does this by establishing and documenting a systematic and secure approach to the sharing of information while addressing privacy, security, and other legal considerations. By documenting and standardising privacy considerations this Charter ensures organisations can meet the concurrent legal duties placed upon health and care commissioners and providers to ensure that no restrictions (other than those specified in this Charter) are placed on sharing citizen and patient information for relevant purposes between their teams.

This Charter is written to cover all types of information sharing set out in the four key purposes which are established in Data Saves Lives as being critical to the successful delivery and improvement of health and care in line with patient and citizen expectations.

These are:

- For the direct care of individuals.
- To improve population health through the proactive targeting of services.
- For the planning, funding and improvement of services.
- For the Research and innovation that will power new medical treatments and/or the improvement of delivery to existing treatments and procedures.

  (NB where any use of data is subject to other approval mechanisms, such as ethical approval for research, establishing data sharing via the approach set out in the Charter does not replace the need for any other approval mechanism).

To aid understanding the information sharing supported and enabled by this Charter covers both "direct care" and "secondary uses" as set out above and includes, but is not limited to, members of Multi-Disciplinary Teams (MDT) who work in different "parent" organisations having conversations about the citizens they have responsibility for. It also covers standardised and unstructured data and both quantitative and qualitative data (i.e. administrative data, data related to interviews and other service user feedback), as well as images, audio and video. That is to say it covers all types and forms of information, not just the movement of digital files between different systems.

The aim of this Charter is to enable BNSSG partner organisations to operate in the "sweet spot" of enabling information sharing while ensuring high trust and adequate (not excessive) control. This aim is visualised in Figure 1 below.

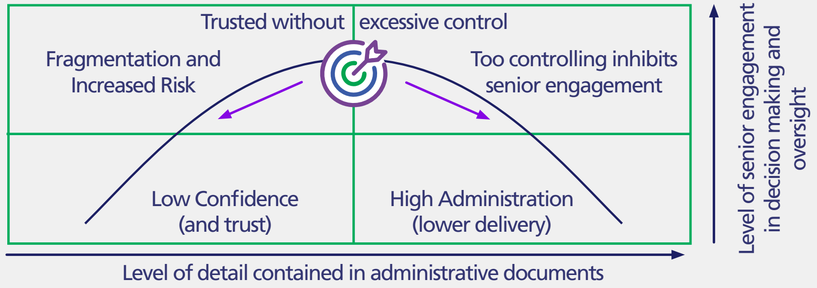


Figure 1. An illustration of the impact of culture on IG management effectiveness[1]

Statements of Law governing information sharing across BNSSG
Following legal advice and a review of the citizen and patient information and data sharing solutions established in other ICS regions, this Charter establishes the following principles that underpin the approach to information sharing outlined in this Charter;

- Articles 6 and 9 of UK GDPR and Schedule 1 of the DPA 2018 allow the sharing of information for the purposes and in the manner set out in this Charter provided certain criteria are met.
- Controllers are responsible for confirming these standards and processes are met and followed. They are not responsible for breaches that happen in other organisations that information has been shared with.
- The ICO is concerned with actual not theoretical data breaches. In the case of actual breaches, the ICO is concerned with whether controllers acted suitably and in line with the requirements outlined above. The ICO accepts it is not possible to entirely eliminate risk when processing data, but expects reasonable endeavours to be made.

[1]Diagram re-produced with credit to www.regisa.uk (Regional Health and Social Care ISA).

Information Sharing across BNSSG that requires no special agreements beyond signing this BNSSG Information Sharing Charter

- Information sharing for direct care (as defined in Appendix A) and other statutorily established direct service provision to individuals (e.g. Safeguarding) where information is not being flowed into a joint system or asset (i.e. teams sharing information on patients and or citizens with whom they have a Legitimate Relationship between themselves but recording that information on their own systems) do not need Data Sharing Agreements or any further documentation.

This form of information sharing is routine across the health sector and is entirely permissible between all direct care teams working in organisations who are Members of this Charter.

Joint control and secondary uses

Where information is being shared into a joint asset and/or system (e.g. Connecting Care, or joint access to one organisations Electronic Patient Record) or where the purpose to which the information is to be put is not direct care (i.e. secondary uses) data protection and privacy laws require further clarity and assurance to be documented before such sharing can happen. This Charter aims to provide the majority of that clarity and assurance in one place to simplify and enable effective data sharing, whilst maintaining compliance, transparency and safety. This is achieved by following the principles and activities laid out in the Framework that the Charter is part of.

Information sharing beyond the scope of this BNSSG Information Sharing Charter

This Charter covers purpose-based information sharing between its members. There will also be data initiatives which are wider than the scope of this Charter e.g. regional and national Secure Data Environments, and so they are not covered in the Charter.

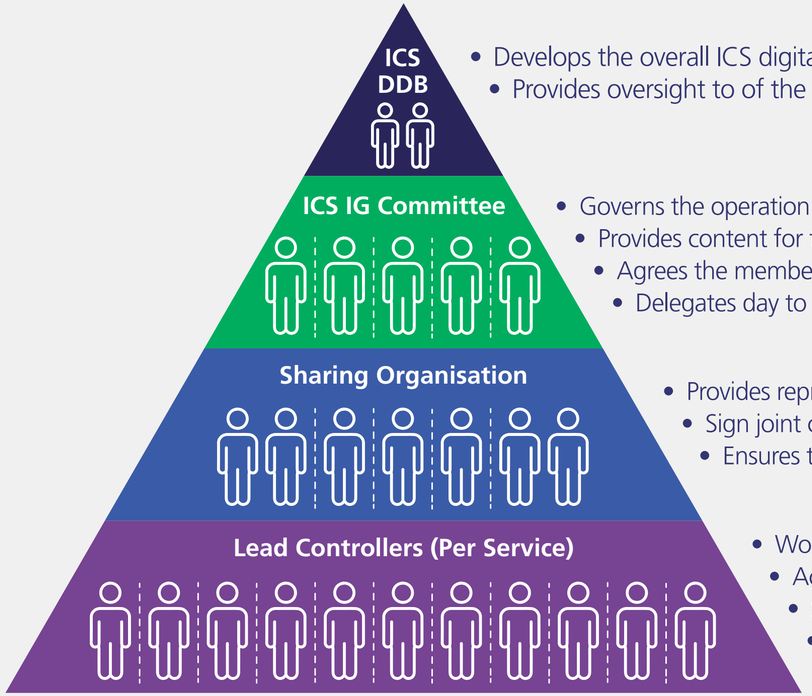
Principles of information sharing for this BNSSG Information Sharing Charter

Members of this Charter will establish joint controller arrangements of shared data and assets as appropriate. The arrangements for governing this joint controllership, including responsibility for administrative tasks and breaches, are set out in more detail in Technical Annex 1.

- Data Protection Impact Assessments will be completed for sharing activities that fall within the scope of the Charter. Where a controller organisation is requested to share data, but is not a joint controller, (e.g. they provide views of their data already to one of the joint controllers outlined in the DPIA but make no further determinations of its uses once shared) the DPIA will be provided to them. Provided the DPIA in question identifies no new risks and that the information sharing falls under the scope of the existing agreement(s) and this Charter then no further action or sign-up is required from that controller organisation for the work outlined in the DPIA. i.e. the combination of sign up to this Charter, provision of the DPIA and their enablement of any data flow/ provision will be taken as their approval to share data for the activity covered by the DPIA.

- Each Member understands its responsibilities with regards to Special Category Personal Data, as defined in the Data Protection Act (2018), the UK General Data Protection Regulation (as subsequently amended through relevant future legislation) and will abide by the Caldicott principles. This is set out in more detail in Technical Annex 2.
- Patient and data subjects rights are clear and processes for responding to requests for people about their data are defined. This is set out in Technical Annex 3.
- Each organisation has in place internal policies for data protection and the protection of patient confidentiality, and for staff training and system audit. This is set out in more detail in the qualifying standards set out in Technical Annex 4.
- Organisations that sign up to this Charter agree to pool and share risk for information sharing governed by this Charter. Details on this are set out in Technical Annex 5.
- This Charter is a living agreement, the process for its review, refresh and possible termination, as well as the addition and removal of members is set out in Technical Annex 6.

BNSSG Information Sharing Charter Operational Model:
The proposed governance and operational structure of this framework and how it aligns to and fits within the wider ICS digital and data governance structure is as:



- Develops the overall ICS digital approach (which includes system IG approach)
- Provides oversight to of the ICS IG committee

- Governs the operation of the ICS Data Sharing Charter
- Provides content for the upward report to Digital Delivery Board
- Agrees the membership and participation of Sharing Organisations
- Delegates day to day operations and responsibility to an agreed administrator

- Provides representatives to the Joint Controller Committee
- Sign joint controller agreements to enable specific projects to work
- Ensures the compliance of Lead Controllers and associated organisational approvals

- Works with Approvers* in Sharing Organisations (*Caldicott Guardian, SIRO, DPO)
- Acts as business owner for a specific services identified and reportable to the Committee
- Supports FOI, SAR delivery (may or may not be reportable to the Committee)
- One organisation might be the lead controller across multiple projects/services

Healthier Together
Improving health and care in Bristol, North Somerset and South Gloucestershire

Technical Annex 1

BNSSG ICS Information Governance Committee

NHS
Bristol, North Somerset and South Gloucestershire
Integrated Care Board

The BNSSG ICS Information Governance Committee (the Committee) will be established to, amongst other objectives, oversee the Charter setup and operational delivery. The Committee consists of individuals drawn from Members of this Charter. It decides upon the development, monitoring and administration of the information sharing covered by this Charter, ensuring the qualifying standard for organisations joining this Charter and the policies/steps required for specific sharing activities that happen under this Charter. Full terms of reference are available here (BNSSG IG Committee ToR September 2024.docx).

Through its work, the committee will provide assurance to the Members of this Charter that the rules and procedures put in place by the Membership Agreement are being effectively managed. The Committee will demonstrate to Members and the public that personal and confidential citizen and patient information will be processed, used, and shared lawfully and that data protection requirements and legislation are being effectively satisfied and complied with.

For the purposes of clarity, the Committee structure and joint controllership model established under the Charter does not mean the Committee will have the right to agree information sharing on behalf of controllers. The Committee simply agrees that a proposed project or service is in line with what has already been agreed in this Charter, and if the proposed project is within the scope of an existing joint controller agreement.

Where the Committee determines that a new joint controller agreement is required all relevant controllers (but only the relevant controllers i.e. only the organisations whose information is required, not all parties of this Charter) would still be required to agree to the specific information sharing being proposed.

How the process will work

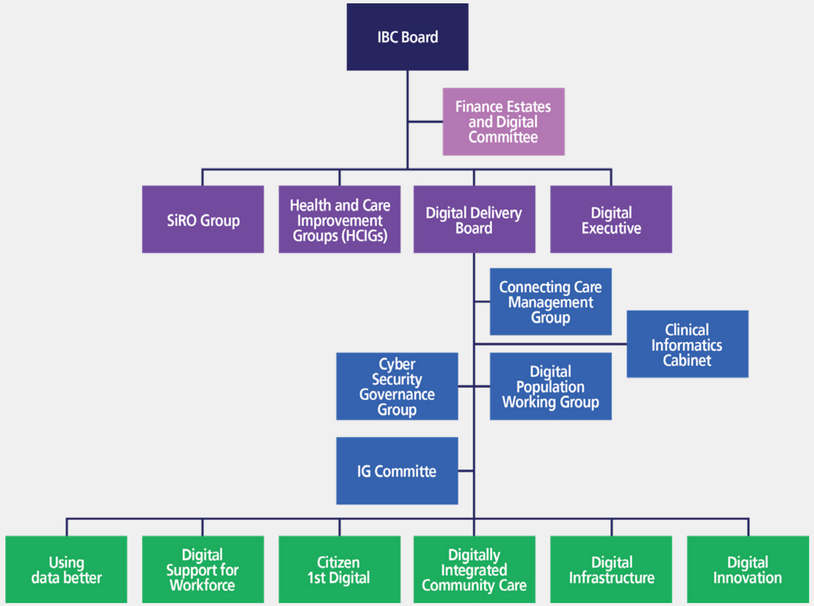
In addition to this Charter, certain document(s) that enable specific information to flow between specific controllers for specific services will still be required. As a minimum, this includes:

- Establishing the "lead" controller for that specific service or project.
- This "lead" controller then leads on the completion of a DPIA. This DPIA as a minimum will:
  - Cover the proposed information and data flow.
  - Set out if the purposes for information sharing is direct care, secondary uses or a blend of both.
  - Set out which other organisations (including processors) are involved in this information sharing.
  - Cover what specific systems are being used to share information between these organisations and if information and data is being moved between them or access granted to one system for employees of the other signatories.

- This DPIA is submitted to the Committee who review the information flow against the agreed purposes in existing joint controller agreements.
- The Committee's review will;
  - Confirm that proposed new projects/services presented to it by the parties that want to be joint controllers to support information sharing are within the scope of what has been agreed to (both direct care and the secondary uses) in this Charter.
  - Advise if the relevant parties need to sign a new joint controller agreement to enable information sharing between their organisations, amend (and re-sign) an existing agreement or if the proposed project/service is wholly covered by an existing agreement (and so no further action is required, and sharing can begin immediately).
  - In cases where the Committee deems the proposed information sharing is beyond the scope of this Charter the respective controllers can still agree to share information between themselves. However, this information sharing will not be covered by the agreements and protections set out in this Charter.

Where a new joint controller agreement is required, a template has been prepared and can be found here (Joint Controller assessment & agreement v1.0 Nov 2024.docx)

How the Information Governance Committee fits in with wider system governance



The Charter administration – supported by ICB IG

To support the initial set-up and operation of this Charter there is a need to establish a supporting administration function. This will originally be hosted and resourced by BNSSG ICB. The tasks required of this function include, but are not limited to, organising meetings, sending out documents, recording decisions and keeping a record of organisational sign up. The administrative arrangements will be reviewed as part of the annual review of this Charter.

Roles of the Parties

Joint controllership

In the context of data protection law (UK GDPR Article 26), joint controllership refers to a situation where two or more entities jointly determine the purpose and means of processing Personal Data. The key elements typically include a shared decision-making process and a common purpose for the information sharing. Importantly, joint controllers must establish their respective responsibilities for compliance with the UK GDPR, particularly regarding the exercise of data subjects' rights. The DPA 2018, mirrors these principles and provides additional details and guidance on the concept of joint controllership. When entities are joint controllers, they are required to have an agreement in place. This Charter and the detail within the joint controller agreements meet these requirements.

Lead controller

Although not a legally recognised role under either the UK GDPR or DPA 2018 'lead project controllers' are a commonly used concept in ICS data and information sharing arrangements, whereby one particular controller takes overall delegated responsibility from the other participating joint controllers to deal with the operational aspects of a particular processing purpose. The joint controllers will designate the lead controller as the effective lead for the purposes of supporting that specific project through signing up to a dedicated joint controller agreement. The lead controller will also be responsible for providing evidence to the IG Committee to demonstrate that the systems being proposed to support specific information flows set out in the joint controller agreement and outlined in the accompanying DPIA have demonstrated they meet the qualifying standards set out in this document in place and/or a record of effective and safe working already across BNSSG.

Reporting and Responding to Data Breaches

Reporting data breaches to the ICO will be the responsibility of the organisation from which the breach originated. They will notify all other relevant joint controllers of their intention to do so. The need to informing data subjects affected by the data breach, which has a higher threshold than the need to notify the ICO, will be considered and agreed by the relevant controllers on a case-by-case basis, and by reference to the presence or absence of particular risk or mitigation factors.
The organisation responsible for the breach must also notify the other signatories of this agreement, regardless of whether there is a requirement to notify the ICO (and/or data subjects).

Responsibility for investigating and responding to the breach will be agreed through the joint controllers covering the specific agreement(s) that are relevant to the particular breach.

Requests from other agencies

Requests from other agencies (e.g. Police, Court Orders etc) are handled by the individual organisational policies of the organisation receiving the request, with the additional elements of:

- Where there is no doubt on the basis for disclosure from jointly controlled information, the joint controller who received the request shall disclose, informing the other joint controllers.
- Where there is any notable concern about the basis for disclosure from joint controlled information, the joint controller who received the request will liaise with other affected joint controllers where time allows. The other joint controllers will prioritise responding. If responses are not received in time, decision will reside with the receiving joint controller.

Technical Annex 2

Compliance with Data Protection and Privacy law

The key ways information sharing governed by this Charter complies with and demonstrates compliance with the relevant legal requirements is set out in detail below (covering both direct care and secondary uses).

Direct Care

UK GDPR and the DPA:
There are lawful bases for processing personal and special category data for direct care under Articles 6 and 9 of the UK GDPR respectively which mean that data subject consent is not required. Members of this Charter acknowledge that for the purposes of direct care the following apply:

Article 6 of the UK GDPR

- The lawful basis for processing Personal Data for direct care is that 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' (Article 6(1)(e)).

Article 9 of the UK GDPR
The special category data condition for processing for direct care is that processing is:

- 'Necessary for the purposes of preventative 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...' (Article 9(2)(h)).

In addition to a UK GDPR Article 9 condition for processing, it is also necessary to identify an additional condition in Schedule 1 of the DPA 2018. For the provision of direct care, the relevant condition is 'Health or social care purposes' (Schedule 1, Part 1 (2)).

The processing must also be undertaken by or under the direction of a health professional in accordance with Article 9(3) UK GDPR, which would be satisfied in circumstances where Members are sharing data to support direct care.

The Common Law Duty of Confidentiality:
As set out above when relying on Articles 6(1)(e) and 9(2)(h) to share data and/or information for the provision of direct care, consent under UK GDPR is not needed.

However, in addition to the UK GDPR, data controllers must also satisfy the Common Law Duty of Confidentiality (CLDC).

To satisfy the CLDC data controllers can continue to rely on implied consent to share confidential health data and/or information for the provision of direct care, provided that data subjects have been made reasonably aware of the proposed uses of their data for direct care purposes (which will be addressed through Member privacy notices).

For all secondary uses

As an overall principle of this Charter all data for secondary uses will at least be pseudonymised, where anonymity is not possible, and otherwise anonymised. Where data or information is not treated in such a manner, clear justification will have to be provided to, agreed and recorded by, the IG Committee.

Whilst Anonymised Data falls outside the scope of the UK GDPR and common law of confidentiality, pseudonymised data is considered Personal Data and the applicability of the legislation needs to be considered. In addition, the anonymising of Personal Data is also a data processing task covered by the legislation.

UK GDPR and the DPA:
As with direct care there are lawful bases for processing personal and special category data for secondary uses under Articles 6 and 9 of the UK GDPR respectively which means that consent is not required to satisfy UK GDPR. Members of this Charter acknowledge that for the purposes of secondary uses statutorily established organisations with legal responsibilities for health and social care the following apply:

Article 6 of the UK GDPR

- The lawful basis for processing Personal Data for secondary care is that 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' (Article 6(1)(e)).

Article 9 of the UK GDPR

- Article 9(2) condition (h) health or social care (and DPA Schedule 1 condition 2) or (i) public health (and DPA Schedule 1 condition 3) whichever is most suitable for Population Health Management and Commissioning
- Article 9(2) condition (j) Archiving, research and statistics (with a basis in law) and DPA Schedule 4 for Research.

In addition to the articles stipulated above organisations must be able to demonstrate that the processing is necessary for reasons of public interest in the area of public health when relying on Article 9(2)(i). The term 'public interest' is not defined, but organisations need to point to a benefit to the wider public or society as a whole, rather than to their own interests or the interests of the particular individual.

For the purposes set out in this Charter that is met by the set of secondary uses agreed between the controllers.

In particular, recital 54 (UK GDPR) makes clear this condition should not enable processing for other purposes by employers, or by insurance or banking companies. The Members to this Charter therefore explicitly rule this processing out in all cases governed by this Charter. Any sharing requests rejected by the committee will be held in a register. In addition, the conditions depend on the organisation being able to demonstrate that the processing is 'necessary' for a specific purpose.

According to the ICO website on special category data "This does not mean that processing has to be absolutely essential". However, it must be more than just "useful or habitual." It must be a targeted and proportionate way of achieving that purpose.

Pre-agreeing specific purposes for which information can be shared should therefore provide data controllers with the full oversight they need to be assured that the signatories to this agreement are only processing information for useful, specific purposes and sharing is therefore legitimate. These specific purposes for secondary uses are set out below:

- Population Health Management
- Commissioning
- Invoice Validation
- Research.

The Common Law Duty of Confidentiality:
As with direct care, data controllers must also satisfy the CLDC where "confidential patient information" is processed. Where a processing activity uses information that is anonymised or sufficiently pseudonymised then the CLDC does not apply.

Where confidential patient information (i.e. where the information is identifiable) is processed then the CLDC does apply. In this case, CLDC controllers cannot rely on implied consent to share confidential health information for the provision of secondary uses because that only applies to direct care.

To satisfy the CLDC the processing of confidential citizen information (in order to anonymise/pseudonymise it) must comply with at least one of the following justifications;

1. The information is pseudonymised "at source" (i.e. within the same system in which the patient data and/or information was originally collected) before being shared on for linkage elsewhere.
2. Patient data and/or information is processed by wholly automated means, to mean in such a way that no actual person can view any of the special category data before any further processing occurs.
3. The processing is largely automated, but some matching is done on the non-confidential part of the patient's information.
4. Section 251 approval from the Confidentiality Advisory Group (CAG) is provided which establishes that the CLDC is set aside for the specific approved purpose.
5. Explicit consent from the individuals whose information is being processed. Processing related to consent can only be for specific individuals who have provided consent and for the specific purposes they consented to.

Demonstrating compliance with the laws for specific secondary uses.

Table 1 Specific ways UK data protection and the CLDC is complied with against specific secondary uses

Purposes	GDPR Article 6	GDPR Article 9	Common law of confidentiality
Service planning and commissioning	Necessary for the performance of a task carried out in the public interest or in the exercise of official authority.	management of health or social care systems and services on the basis of member state law	Requires linkage between information sources, via pseudonymised data either at source or via controlled environment where data processing is automated and not conducted manually by users (compliance options i, ii, iii above).
Managing finances, quality and outcomes			
Planning, implementing and evaluating population health strategy			
Data driven clinical support (e.g. AI tools, risk prediction)			
Undertaking Research sponsored or conducted only by Parties to this Charter and within the BNSSG geographic "footprint" – and EXCLUDING the Secure Data Environment(s) – whose data controllership and sharing agreements are separate to this.	Necessary for the performance of a task carried out in the public interest or in the exercise of official authority. (Public Authority) Legitimate interests (subject to appropriate legitimate interest test) or 'Recognised legitimate interest list' (Private organisation)	necessary for … scientific research purposes or statistical purposes in accordance with Article 89 (1) based on member state law (see legal gateways) 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 rights and interests of the data subject.	Requires linkage between information sources, via pseudonymised data either at source or via controlled environment where data processing is automated and not conducted manually by users.

Table 1 sets out that for the majority of purposes and use cases covered by this Charter confidentiality is assumed to be protected by automated pseudonymisation techniques. Consent will not be sought as it is impractical given the number of individuals involved and not needed for the purposes, we wish to put the data and/or information to. Section 251 (National Health Service Act 2006) support will be sought, if during a DPIA/ risk assessment undertaken prior to beginning processing of the full lifecycle of the data and/or information the review indicates that at any stage of the process confidential citizen information (i.e. clearly identifiable to all, or identifiable to a recipient based on what they already have) is required by an activity.

Technical Annex 3

Rights and obligations to individuals/data subjects

Right to object
Under the UK GDPR individuals have a general right to object to their Personal Data being processed in certain circumstances. This right applies unless the data controller can demonstrate 'compelling legitimate grounds for the processing'. In the face of an objection from a citizen, in many cases NHS organisations are likely to be able to demonstrate 'compelling legitimate grounds' to continue processing Personal Data because it is necessary for the safe provision of direct care and/or processing which is necessary for compliance with a legal obligation (e.g. where health and care organisations are compelled to share data with other statutory organisations such as the Police or Courts).

Individuals also have the right to object to any processing where their Personal Data is used as an input to *fully* automated decision making (i.e. AI driven algorithms with no human review or oversight).

Should an individual request, from any joint controller, that their Personal Data is not shared with another healthcare organisation for the purposes of their own care then this will be governed by the specific clinical teams involved in their care.

Right to opt out of processing
Other opt-outs do not apply to direct care and will not be applied to information sharing governed by this Charter relating to that usage only. Opt-outs do apply for all secondary uses where confidential patient information is used at any point of the process and will apply to all information sharing governed by this Charter that meets this criteria.

In particular, the National Data Opt-Out enables patients to opt out of any proposed secondary uses of their data which relies on section 251 approval. Responsibility for investigating and responding to the data subject enquiries outlined below will be agreed between the joint controllers and supported by the administrator.

Subject Access Requests
For subject access requests related to information shared through the specific joint controller arrangements, all parties identified in that arrangement will be notified by the organisation in receipt of an enquiry of this nature from a data subject or their representative. Individual controller organisations who manage an asset that is shared will be responsible for extracting information to respond to a request. The joint controllers will agree appropriate assessment of any exemptions prior to provision.

Requests related to records of the deceased
For requests related to the records of the deceased and relating only to information shared through a specific joint controller arrangement, all parties identified in that arrangement will be notified by the organisation in receipt of an enquiry of this nature from the requestee. Individual controller organisations who manage an asset that is shared will be responsible for extracting information to respond to a request. The joint controllers will agree appropriate assessment of any exemptions prior to provision, although noting that the UK GDPR does not apply to requests for medical records concerning deceased individuals which are governed by the Access to Health Records Act 1990.

Other data subject rights

The data subject shall have, subject to exceptions, the following additional rights under the UK GDPR concerning their data as processed by the joint controllers:

- Rectification of data
- Erasure of data
- Restriction of processing
- Object to solely automated decision making.

Complaints

For complaints related to information shared through a specific joint controller arrangement, all parties identified in that arrangement will be notified by the organisation in receipt of the complaint of this nature from the complainant or their representative.

Privacy notice

As a minimum parties signed to this Charter will adopt a standard item into their privacy notice which will also contain a link to a specific website that provides more details on this agreement and the way it is governed (hosted by the ICB).

Freedom of Information (FOI) Requests

FOIs are handled by the individual organisational policies of the organisation receiving the FOI request.

Healthier Together
Improving health and care in Bristol, North Somerset and South Gloucestershire

Technical Annex 4

Qualifying standard for member organisations

NHS
Bristol, North Somerset and South Gloucestershire
Integrated Care Board

To access personal confidential information on citizens shared under this Charter Members must ensure they comply with the standards set out below. Failure to do so could lead to the organisation in question being prevented from sharing information and removed from this Charter. Details of how this works (and support available for those organisations who may struggle to demonstrate these standards) are set out in the Review and Termination section below.

- Staff access to confidential personal information is monitored and audited. Where care records are held electronically, audit trail details about access to a record can be made available to the auditors and the data subject on receipt of specific request.
- The use of computing systems is controlled, monitored, and audited to ensure their correct operation and to prevent unauthorised access.
- Procedures are in place to ensure the accuracy of service user (data subject) information on all systems that support the provision of care.
- All contracts with staff, contractors and third parties contain clauses that clearly identify information governance responsibilities and the professional obligation to protect confidentiality.
- All staff members are provided with appropriate training on information governance requirements and are up to date with such training.
- Staff members are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users.
- Background checks are carried out for staff, contractors and third parties given access to confidential and sensitive information.
- Processes and technical measures including but not limited to role-based access controls are in place to ensure as far as possible that only those staff, contractors and third parties with a lawful purpose to access confidential information on citizens they have a Legitimate Relationship with are able to do so.
- Responsibility for Information Governance (IG) and for the scrutiny and approval of all Information Governance matters including but not limited to information sharing protocols and information risk management policies has been assigned to an appropriate member, or members, of staff.
- There are approved and comprehensive Information Governance policies with associated strategies and/or improvement plans in place in each organisation.
- There are documented Information Governance incident management and reporting procedures.
- All information assets that hold, or are, personal information are protected by appropriate organisational and technical measures.
- All new processes, services and systems are developed and implemented in a controlled and secure manner.

- Operating and application information systems that store and process confidential and sensitive information that are used by the organisation to support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.
- Policy and procedures are in place to ensure that information technology networks operate securely.
- The requirements of the Data Security and Protection Toolkit (DSPT) are satisfied (where not already specifically covered above) or equivalent assurance provided to be determined by the IG Committee.
- Unauthorised access to the premises, equipment, records and other assets is prevented.
- Ensure service users and citizens are informed of how the information the organisation holds on them is used (e.g. privacy notice).
- Ensuring the organisation is appropriately registered with the ICO.

Healthier Together
Improving health and care in Bristol, North Somerset and South Gloucestershire

Technical Annex 5

NHS
Bristol, North Somerset and South Gloucestershire
Integrated Care Board

Risk sharing and liabilities

The risk sharing and indemnity arrangements are restricted to the Members of this Charter and applies only to the cases outlined below. By entering into this Charter, the Members effectively pool risk by the mutual acceptance as a whole system (with all the collective expertise and experience) that the accountability and oversight measures outlined are deemed sufficient to meet their respective duties as data controllers (to include where acting jointly with other Members).

This avoids the need for any individual organisation to establish or demonstrate the suitability of any other Member's accountability and oversight arrangements for every sharing request.

In particular this relates to data protection breaches concerning data which has been shared with another Member in accordance with this Charter, in circumstances where the Member who originally shared the data is not responsible for the breach.

The Members agree to support any Member who has shared data in accordance with this Charter to demonstrate that they are not responsible for a data breach concerning that data by a recipient Member. This is provided that:

- The original data sharing in question was for purposes outlined by a valid and approved joint controller agreement and data protection impact assessment
- The original data sharing was to another Member
- The relevant Member can demonstrate it is compliant with the organisational responsibilities outlined above.

The level and type of support will vary depending upon the legal requirements that govern relationships between the signatory organisations of this Charter and is set out below.

Indemnity

In order to facilitate and support information sharing across the system, this Charter establishes indemnity arrangements that can apply to sharing information under the guidelines set out within this Charter.

Indemnity, in this specific context, aims to provide financial support to the "small" data controllers across the system. A list of qualifying organisations will be agreed and maintained by the IG committee. To help clarify specific examples will include GPs and local third sector providers of health and care services who may not have the financial resources immediately available to defend themselves suitably against a claim raised in relation to data breaches that occur in other Member organisations but connect to information sharing set out in this Charter by the qualifying organisation. The indemnity will be provided solely by the ICB to the qualifying organisations.

The scope of the indemnity applies to data protection breaches relating to the use of information where the breach has been caused by a member's use of that information and in the following cases:

- Data breaches associated with the electronic patient record information assets and the associated information flows.
- Data breaches associated with sharing arrangements and information assets where joint control applies.
- Data breaches as associated with sharing arrangements relating to information sharing approved by the IG committee and with a signed joint controller agreement covered by this agreement.

The indemnity proposes to reimburse the reasonable legal costs not covered by any other indemnity/insurance arrangements incurred by the organisation as a direct result of responding to civil or regulatory actions which relate to the circumstances outlined above and where formal claims or notifications have been issued. Any costs associated with this indemnity will be funded solely by BNSSG Integrated Care Board.

Legal defence cost pooling

Outside of the specific situation where certain qualifying organisations receive indemnity provided by the ICB, all Members may elect to contribute to and receive support from a data sharing defence fund. Organisations on the list that qualify for indemnity support will not be expected to contribute to the defence fund.

Given that legal cases are uncommon and there are always financial pressures on organisations, no contributions will be requested until there is a case against a Member that warrants it and the Member requests support. At that time legal costs will be estimated and contributions determined by the ICS Information Governance Committee. For the avoidance of doubt, the committee cannot compel any Member to contribute.

The scope of the cost pooling applies to data protection breaches relating to the use of information where the breach has been caused by a member's use of that information and in the following cases:

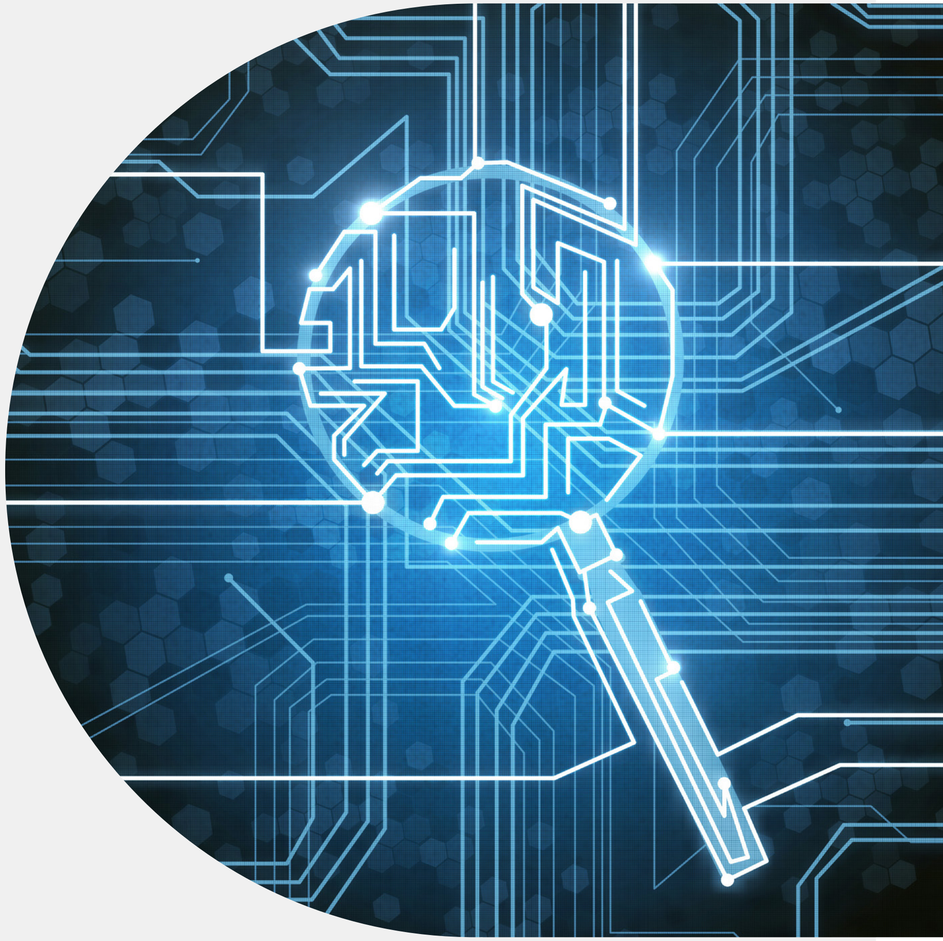
- Data breaches associated with the electronic patient record information assets and the associated information flows.
- Data breaches associated with sharing arrangements and information assets where joint control applies.
- Data breaches as associated with sharing arrangements relating to information sharing approved by the joint controller oversight committee and with a signed joint controller agreement covered by this agreement.

The risk pooling proposes to cover the reasonable legal costs incurred by the relevant member as a direct result of responding to civil or regulatory actions which relate to the circumstances outlined above only and where formal claims or notifications have been issued.

Limits to indemnity and legal defence

The indemnity and legal defence for information sharing covers legal costs incurred by any Member required to establish that they were not responsible for the breach in question only and does not cover any damages awarded or agreed by way of settlement in connection with civil claims or penalties imposed by the ICO.

Further, it does not apply where a Member is responsible for the breach itself or arising out of processing activities not covered by this Charter or for which the Member is otherwise solely responsible.



Technical Annex 6

Review, variation and termination of this Charter

Variation of the Charter and framework
Minor changes (as set out in the finalised Terms of Reference (ToRs) of the Committee) will be made by the Committee (i.e. there will be no need for the Membership Agreement to be signed again).

Major changes (As set out in the finalised ToR of the committee) must be agreed by the individual Members (i.e. the full set of documents must be reviewed and signed again).

Adding new members to this Charter
Providing any Members joining this Charter after the original commencement date can demonstrate compliance against the terms set out in this Charter and the organisational responsibilities (as assessed by the joint controller committee) then the new member organisation can be added to this Charter (it does not require approval of all existing Members).

Review and termination
This Charter and all subsidiary direct care and secondary uses processing and sharing specifications begin on the commencement date.

Individual Members can withdraw or be removed from this Charter in the following situations. The Members of this Charter may withdraw from this Charter:

- On reasonable written notice to the Joint Controller Oversight Committee
- With reasonable notice being the period required to remove:
  - Any shared information
  - Access to shared information in respect of user organisations
  - The shared information itself and any related operational system processes in respect of sharing organisations
- Where the withdrawing member has provided the necessary resources and information for the shared information to be identified and removed.

Should a Member organisation cease to/fail to comply with the qualifying standards set out above then within three (3) months of the date that the user organisation is not able to demonstrate compliance with the qualifying standards the user organisation must:

- Implement the corrective measures necessary to satisfy the qualifying standard, or
- Cease to make use of the personal confidential information shared under the agreement (i.e. access will be withdrawn to the shared information and assets governed by this Charter). However, the flow of information from the organisation that has not met/maintained the standards will continue to enable compliant organisations to continue to benefit from the information).

- Has a derogation approved by the IG Committee to continue to provide and/or access shared information. In this case the organisation that has not met the qualifying standards will provide a plan on how it is planning to meet the standards and the IG Committee will set out the support from other Members that will be provided to help the organisation to meet the qualifying standards.

Where a member withdraws or is removed from this Charter the administrator (as appointed by the Joint Controller Oversight Committee) is delegated the task of ensuring the relevant information is identified and removed from information sharing assets and processes and that access rights and processes are removed for the exiting organisation as well.

An individual Member withdrawing or being removed from this Charter does not affect the information sharing governed by this Charter for the other Members (except for the information that organisation was the supplier of information for).

This Charter will be reviewed every 12 months to ensure Members remain satisfied it meets the purposes of supporting seamless information sharing across BNSSG and/or following major policy and/or legislative changes. This is to ensure it continues to meet the applicable criteria. If Members of the Charter identify improvements and/or changes they believe are required, then they can propose changes for discussion at this review.

Annex A

Definitions

Word (Alphabetical)	Definitions
Anonymised data	Anonymous (otherwise known as effectively anonymised) data is data that is no longer personally identifiable. Anonymised data is not considered as Personal Data under UK GDPR, nor as confidential citizen information under the common law duty of confidentiality. This means it is not subject to the same restrictions as data to which these regimes apply. Anonymised data may be presented as general trends or statistics. For example, by removing direct identifiers such as NHS number and name and translating e.g. age into an age range (25-40) and grouping postcodes together. However, information about small groups or people with rare conditions could potentially allow someone to be identified and so would not be considered anonymous. (Sources: ICO and Understanding Patient Data) On the other hand, reidentification risk does not have to be eliminated completely for data to be considered anonymous, provided that the risk is mitigated sufficiently so that in the hands of the recipient it meets anonymisation requirements. Any onward transfer of (or remote access to) the data may change its status to be Personal Data again, depending on any additional information and means available to the onward recipient.
Anonymisation	Anonymisation involves the application of one or more anonymisation techniques to personal information. When done effectively, the anonymised information cannot be used by the recipient to identify the data subject either directly or indirectly, taking into account all the means reasonably likely to be used by them. This is otherwise known as a state of being rendered anonymous in the hands of the recipient. (Source: ICO)
Care Team	Care teams may include doctors, nurses, and a wide range of staff on regulated professional registers, including social care professionals. Relevant information should be shared with them when they have a Legitimate Relationship with the citizen or service user. Care teams may also contain members of staff, who are not registered with a regulatory authority. (Source: Information: To share or not to share? The Information Governance Review, National Data Guardian).
Common Law Duty of Confidentiality	A duty of confidentiality arises when one person discloses information to another (e.g. patient to clinician or service user to social care staff) in circumstances where it is reasonable to expect that the information will be held in confidence. (Source: Confidentiality: NHS Code of Practice 2003).

Word (Alphabetical)	Definitions
Confidential Patient Information	The term 'confidential patient information' (also known as 'confidential patient and service user' information) is a legal term defined in section 251 (11) of the National Health Service Act 2006. Patient or service user information is "confidential patient information" where (1) the identity of the individual in question is ascertainable from that information, or from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information; and (2) that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual. It encompasses health and care information, both clinical and demographic (such as name and address), relating to, or in connection with, an identified or identifiable individual's past or present use of services (NHS or adult social care).
Data-Driven Technologies	Technologies that work by collecting, using, and analysing patient and service user data to support the care of individuals, NHS services, public health, or medical Research and innovation. (Source: Our data-driven future in healthcare, Academy of Medical Sciences.)
Data Processing	The terms "processing" and "process" mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as viewing, editing, printing, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Protection Legislation	This is an overarching term that encompasses the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018. See section 3(9) DPA 2018.

Word (Alphabetical)	Definitions
Data Subjects	For the purposes of the agreement the recipients of care and the natural persons providing care are the data subjects to whom the agreement applies and are referred to as "the individual." For the purposes of the agreement the individual includes the terms data subject, patient, client, customer, carer, relative and family member. For the purposes of the agreement the terms Personal Data, personal confidential data, non-sensitive Personal Data, and sensitive Personal Data have the meaning defined in Article 4(1) of the General Data Protection Regulation ("GDPR"): information relating to an identified or identifiable natural person ("data subject"); and an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Deployment	To put into therapeutic use.
Direct Care	A clinical, social, or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a Legitimate Relationship for their care. (Source: Information: To share or not to share? The Information Governance Review, National Data Guardian).
Health Research Authority (HRA) Approval	HRA approval is the approval needed prior to the conduct of health or social care Research in the NHS (including in independent providers of NHS commissioned primary care services) in England.

Word (Alphabetical)	Definitions
Implied Consent	Implied consent is applicable only within the context of direct care of individuals (and local clinical audit undertaken by members of the care team). It refers to instances where the consent of the individual patient or service user is implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed. Examples of the use of implied consent include doctors and nurses or social care professionals sharing personal confidential data during handovers without asking for the patient's or service user's consent. Alternatively, a physiotherapist may access the record of a patient who has already accepted a referral before a face-to-face consultation on the basis of implied consent. Implied consent should only be used if it is reasonable to expect the patient understands how the information will be used. (Source: Information: To share or not to share? The Information Governance Review, National Data Guardian).
Indirect Care	Activities that contribute to the overall provision of services to a population as a whole or a group of patients or service users with a particular condition, but which fall outside the scope of direct care. It covers health and/or care services management, preventative medicine, and medical Research. Examples of activities would be risk prediction and stratification, Service Evaluation, needs assessment, financial audit. (Source: Information: To share or not to share? The Information Governance Review, National Data Guardian).
Legitimate Relationship	The legal relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care. (Source: Information: To share or not to share? The Information Governance Review, National Data Guardian. For further information on the appropriate criteria for determining whether the health or social care professional has a legitimate relationship with the patient or service user, see section 3.6 of this report.)

Word (Alphabetical)	Definitions
Medical Device	According to the Medical Devices Regulations 2002 (SI 2002 No 618, as amended) (UK MDR 2002), a medical device is described as any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnosis or therapeutic purposes or both and necessary for its proper application, which is intended by the manufacturer to be used for human beings for the purpose of: Diagnosis, prevention, monitoring, treatment or alleviation of disease Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap Investigation, replacement or modification of the anatomy or of a physiological process, or control of conception A medical device does not achieve its main intended action by pharmacological, immunological or metabolic means although it can be assisted by these. A medical device includes devices intended to administer a medicinal product or which incorporate as an integral part a substance which, if used separately, would be a medicinal product and which is liable to act upon the body with action ancillary to that of the device. (Source: Medical devices: how to comply with the legal requirements in Great Britain - GOV.UK (www.gov.uk))
Members	Members are current parties of the BNSSG ICS Information Sharing Charter who have signed the Charter/Membership agreement. See also "Parties."
National Data Opt-Out	The national data opt-out is a service that allows patients to opt out of their confidential patient and service user information being used for Research and planning in specified circumstances.
Parties	Parties are current members of the BNSSG ICS Information Sharing Charter who have signed the Charter/Membership agreement. See also "Members"
Personal Data	Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. (Source: Article 4 (1) UK GDPR)

Word (Alphabetical)	Definitions
Pseudonymisation	Pseudonymisation can be defined by considering Article 4 (5) and Recital 26 of the UK GDPR, whereas the assessment of identifiability may be considered from the perspective of the recipient of the data that has undergone pseudonymisation: Article 4 (5) UK GDPR - The processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person. Recital 26 UK GDPR – The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. As a privacy-enhancing process, pseudonymisation is typically applied before information is shared with a third party (recipient) in circumstances where the link between individuals and the data that relates to them needs to be reduced – to offer protection against accidental disclosure - but not removed entirely. For example, it could involve replacing an NHS number, a name, or an address, with a unique number or code (a pseudonym). This has the effect that the recipient cannot identify an individual directly from that data without access to this additional information held separately and securely elsewhere using appropriate technical and organisation measures. (Source: ICO)
Post-Market Surveillance	Once a medical device has been placed on the UK market, the manufacturer is required to submit vigilance reports to the MHRA when certain incidents occur in the UK that involve their device. They must also take appropriate safety action when required. The manufacturer must ensure their device meets appropriate standards of safety and performance for as long as it is in use.

Word (Alphabetical)	Definitions
Research	Research is defined as the attempt to derive generalisable or transferable new knowledge to answer or refine relevant questions with scientifically sound methods. This excludes audits of practice and Service Evaluations. It includes activities that are carried out in preparation for or as a consequence of the interventional part of the research, such as screening potential participants for eligibility, obtaining participants' consent and publishing results. It also includes non-interventional health and social care research (i.e. projects that do not involve any change in standard treatment, care, or other services), projects that aim to generate hypotheses, methodological research, and descriptive research. Projects whose primary purpose is educational to the researcher, either in obtaining an educational qualification or in otherwise acquiring research skills, but which also fall into the definition of research, are included in this definition. (Source: UK Policy framework for Health and Social Care Research).
Service Evaluation	Service evaluation is designed and conducted solely to define or judge current care and should answer the question: "What standard does this service achieve?" It should measure current service without reference to a standard and involve an intervention in use only. The choice of treatment is that of the clinician and patient or social care professional and service user according to guidance, professional standards, and/or patient or service user preference, and this should happen before Service Evaluation. Service evaluation usually involves analysis of existing data but may include administration of interview or questionnaire. There should be no randomisation. (Source: HRA decision tool).
Sharing and user organisations	The members/parties of the agreement who have signed a joint controller agreement to share specific data between themselves. Note, organisations may be both a sharing organisation in respect of the member's own information and a user organisation in respect of other members' information.
Special Categories of Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (Source: Article 9 UK GDPR).
Synthetic Data	Synthetic data is information that is artificially created (algorithmically) rather than generated by real-world events. It can simulate synthetic populations that resemble the characteristics as well as diversity of actual people. It can also be generated to be statistically consistent with a real data set, which it may then replace or augment.
UK GDPR	The United Kingdom General Data Protection Regulation (UK GDPR) became effective on 1 January 2021. The law covers the key principles along with rights and obligations when processing Personal Data in the UK and is a regulation under the Data Protection Act 2018. More information on the application of UK GDPR in a healthcare Research context can be found at: GDPR guidance - Health Research Authority (hra.nhs.uk). The ICO has also published general guidance: Guide to the UK General Data Protection Regulation (UK GDPR) | ICO.

Healthier Together

Improving health and care in Bristol,
North Somerset and South Gloucestershire