Bristol, North Somerset and South Gloucestershire

Connecting Care

Data Sharing Agreement

Document Control	
Version	**9.4**
Author(s)	Helena Ashton
Last updated and date issued	October 2018

Contents

1. Introduction

The purpose of this agreement is to set out the arrangements for the sharing and use of personal and sensitive personal/special categories data (as defined in the Data Protection Act 2018 and the General Data Protection Regulation) for the Connecting Care Programme between the signatory partner organisations.

The agreement also sets out how the sharing of data within the Connecting Care Programme is compliant with relevant legal and regulatory requirements. This agreement does not provide full detail of all compliance requirements, such as detailed technical security, and must be read in conjunction with other documents (such as the Connecting Care System Security Statement).

This agreement operates in conjunction with the current version of the Information Sharing Principles Agreement (see www.protectinginfo.nhs.uk).

This document contains a number of legal definitions and references and the term 'individual' is used to cover the sector specific terms for members of the public in receipt of services such as 'patient', 'client', 'service user' or similar for adults and children.

2. Purposes & Benefits of Information Sharing

2.1. Background

Across Bristol, North Somerset and South Gloucestershire, care for individuals is carried out by different organisations including health, social care and early intervention services. Individuals frequently move between primary care to acute hospital care, to community health care and social care. In other cases, individuals are cared for within multi-disciplinary teams that draw on expertise from different parts of health and social care and early intervention.

However, despite the rarity of an individual's journey being limited to one particular organisational 'silo', most information systems are specific to one particular organisation, or even to a particular service within an organisation. Thus information is dis-connected across care pathways. These 'silos of information' adversely impact care in terms of:

- The ability to safeguard vulnerable individuals
- The individual s experience
- The quality of care
- The ability to fully support care pathways (e.g. for long term conditions)
- The efficiency of services
- The ability to provide 'joined up care' – and care provided by the right person at the right time

Connecting Care is the Bristol, North Somerset and South Gloucestershire's [BNSSG] programme delivering a detailed, local, shared record. The programme integrates health and social care information sourced from a variety of existing information systems currently in use – thus providing a unified view of information that can be used to facilitate improved care provision and decision-making.

Use of the Connecting Care Portal helps to improve on the security and auditability of the current methods of data sharing including verbal (phone calls and face to face) and written (correspondence, emails and faxes) by reducing and replacing them where possible.

2.2. Benefits

Benefits of sharing data for Connecting Care include:

- Improved security of information; reducing the risk of misdirected communications
- Care professionals will have the ability to find up-to-date information about the individuals they provide care for, and their encounters with other care professionals, in one place
- It supports better, more effective clinical/care decision making
- Improved care and outcomes for individuals
- Improved safety for individuals e.g. allergy information will be available to care professionals, reducing the risk of adverse drug reactions
- Reduction of administrative costs; Connecting Care partner organisations frequently get asked to provide information to other services about the individuals they care for via telephone, fax, letter etc.
- Reduced duplication of work e.g. duplicate tests being ordered or repeat requests for information

2.3. Primary purposes & legal basis for information sharing

The key purposes of sharing information for Connecting Care are:

- For delivering integrated care and treatment across Connecting Care partner organisations, based on a model of reasonable expectations and legal powers to upload information to the portal and legitimate relationship access, utilising legal powers and duties to access relevant information or explicit consent to access where this is necessary.
- The delivery of urgent and safeguarding care, where the failure to do so effectively carries a significant risk of harm to the individual(s) based on a model of 'vital interests', legitimate relationship model or utilising explicit consent justification for processing data.

Each partner organisation accessing information will ensure the use of information relates to the above purposes as required by Data Protection Act principles, the General Data Protection Regulation articles and any other relevant legislation.

The Connecting Care justifications model is described in detail in section 4.

2.4. Secondary uses of data from Connecting Care:

Data accessed via Connecting Care is used primarily for the delivery of direct care and, when approved, consented research studies, and service improvement.

- Where Connecting Care is used for research, or service improvement purposes, the principle of minimisation will be applied in **all** uses. These core principles are agreed:

    - Identifiable data will not be available without clear documented legal justification
    - Where identifiable data is not necessary the data will be made available in three levels: aggregate, pseudonymised, and de-identified data. To support improvements in care (joined up pathways, integrated working), analysis of data at an individual 'row' level will be required. Such activities will use either pseudonymised data, de-identified data or identifiable data (where there is clear documented legal basis).

All secondary uses will comply with the National Data Guardian's consent model.

3. Legal Framework

Within a health and social care context there is legislation and regulation that relates to information sharing and the requirement to deliver a good quality of care; some of it places regulatory control on the sharing of data, and others provide powers to share data. A list of some of the relevant legislation that supports this data sharing can be found in **Appendix 3**. This agreement is set within the relevant legal framework with specific references as follows:

3.1. Regulatory controls on the use of information:

3.1.1. Data Protection Act (DPA) 2018:

This is the key legislation to control the processing and sharing of personal data. All signatories to the agreement are required to comply with the requirements of the DPA. The processing of data within Connecting Care must be compliant with the DPA. The principles are referenced throughout this document:

In particular these matters have been agreed and documented:

- When an individual makes a request to an organisation for access to the data it holds on them, the organisation will follow its standard process to provide information. An organisation is not required to provide access to data that it can access from other controllers. When an individual makes a request to see information that has been viewed in Connecting Care, the Connecting Care Subject Access Request Policy and Process should be followed.
- Technical and organisational security – this is described in the Connecting Care System Security Statement (overview in section 6).

All data is processed within the UK. A Data Protection Impact Assessment (DPIA) has been conducted by the programme and this is regularly reviewed within the Information Governance work stream. Impacts on individuals' privacy will be considered for any change to the system, including expansion of data shared by existing or new stakeholders or increased functionality, or changes to key information/relevant legislation.

3.1.2. General Data Protection Regulation (GDPR) 2016/679

All signatories to this agreement are required to comply with the requirements of the GDPR. The processing of data within Connecting Care must be compliant with the GDPR principles. The GDPR principles, like the DPA principles, are referenced throughout this document. The lawful bases for processing data in Connecting Care taken from the relevant articles in the GDPR are referenced in section 3 of appendix 3.

In addition to the existing subject rights e.g. the right to request access to a copy of their personal data and the right to be informed, this legislation introduces some new subject rights, some of

which are qualified and only applicable **when individual consent** has been obtained as the legal basis for processing their information, these are:

- Data Portability – an individual must be given a copy of their data, which had been provided by them directly to the data controller in a structured, commonly used and machine readable format.
- Erasure – data controllers must delete personal data on request, if the data subject withdraws their consent and no other legal ground for processing applies.

The legal basis relied on to process personal data via Connecting Care for direct care, is not individual consent and therefore these two rights are not engaged.

Other new rights include:

- Right to rectification – an individual has the right to obtain rectification of their inaccurate personal data from the controller without delay.
- Restriction of processing – where it is claimed that data is inaccurate, or the right to object has been exercised, individuals can require the controller to restrict processing until verification checks have been completed. Individuals may also require controllers to restrict processing where they claim there is no legal basis for the processing to take place.
- Right to object – Individuals have the right to object, at any time to processing of personal data concerning them which is based on point (e) or (f) of Article 6(1) and the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing.

3.1.3. Human Rights Act (HRA) 1998 and Common Law duty of confidentiality:

In accordance with article 8 of the HRA, everyone has the right to respect for his private and family life, his home and his correspondence. Privacy is protected by the agreed role based access and processes to manage users of the system. To meet the condition that a public authority should not interfere with this right, individuals have the right to opt out of information being viewed via Connecting Care unless there is a public safety (safeguarding) concern.

The Common Law Duty of Confidentiality is considered when deciding role based access to ensure that professionals are not given more information than is necessary to perform their role.
Where information is held in confidence (confidential information should meet the 3 limb test, quality and obligation of confidence and detriment to the provider) the consent of the individual concerned should normally be sought before further sharing, this can be implied consent as the threshold is lower than that required for the GDPR.
The circumstances where consent under the Common Duty of Confidentiality does not have to be gained would be:

- Where information is not held in confidence as it does not meet the 3 limb test
- There is a robust public interest and where it is in the interest of an individual's health or in the interests of the person concerned
- Where there is a legal requirement to do so, for example a court order or a statute (legislation)

3.1.4. Legal powers for sharing data (Legal gateways):

Data sharing of health and care information is intrinsic to the direct provision of health and care to individuals in receipt of services and the ongoing management and provision of those services. Therefore, sharing is done within the existing legal powers ('vires') of the participating organisations.

Any new organisation wishing to share and access, or just access, data in Connecting Care, will, as part of the 'take on' process identify and ensure there are sufficient legal gateways for the sharing of data between the relevant parties. A list of the legal gateways that may be used by Connecting Care partners can be found in **Appendix 3**.

3.1.5. Requests to share data for non-direct care purposes:

Information held within Connecting Care is currently for the purposes described in sections 2.3 and 2.4 of this document. Therefore, any request for information held on an individual within the Connecting Care system, other than for these purposes, must have a lawful reason to do so, e.g. to assist a partner organisation with an investigation into system misuse, to assist the police with an enquiry.

If there is a lawful reason, the receiving organisation should consider the following when responding:

- Establish whether the request is appropriate, by liaising with their Information Governance Lead
- Only disclose information from their own source systems, in line with their own organisational policy
- If deemed appropriate, refer the requester direct to another organisation, within Connecting Care

4. Justifications for creating and accessing the Connecting Care record

4.1. The Creation of Connecting Care Records (Lawful basis model)

The approach to the creation of Connecting Care records is as follows:

Legal Requirement to Share information

It may be necessary for information to be shared between organisations either because of a direct legal obligation or in order to assist in meeting a statutory requirement placed on any of the Connecting Care partner organisations. Where this is the case, all Connecting Care organisations must be aware of this legal requirement, agree and understand the limit of the information that is to be shared, and the purpose it is to be shared for, and ensure that individuals are adequately informed about this data sharing. Appendix 3 contains a list of the Legal Gateways that, where applicable, allow the lawful sharing of data.

Consideration of applicable legislation

The legal powers that exist to permit the creation of a combined health and care record as per 3.1.4 above and the data protection justifications to process data to create the record, must be identified and agreed.

Confidential information

Where information is held in confidence (for information to be considered "confidential information", it should meet the 3 limb test - quality, obligation of confidence, detriment to the provider). The consent of the individual concerned should normally be sought before further sharing/access.

The consent gained to comply with the requirements in the Common Law Duty of Confidentiality is not to be confused with 'consent' as one of the possible lawful bases for processing data in the GDPR. A relevant lawful basis under GDPR must be met in addition to any consent required under the Common Law Duty of Confidentiality. The circumstances where consent under the Common Duty of Confidentiality does not have to be gained are:

- Where information is not held in confidence as it does not meet the 3 limb test
- There is a robust public interest and where it is in the interest of an individual's health or in the interests of the person concerned
- Where there is a legal requirement to do so, for example a court order or a statute (legislation)

Informing individuals

At the start of the Connecting Care programme in 2013, a mass mailing to all individuals in Bristol, North Somerset, South Gloucestershire (aged 15+) was undertaken as a key exercise to inform and advise them of their rights to opt out.

Materials to promote the use of Connecting Care have been created and are available to all partner organisations. These include posters, leaflets and web based materials. Partner organisations are expected to actively promote these materials to individuals.

The following additional informing has since taken place:

- Letters from maintained, academy and independent schools to all parents/carers
- In newsletter articles to citizens of South Gloucestershire and North Somerset
- A Connecting Care external website has been designed and published

The following informing materials have been updated and will be issued to new patients and service users where appropriate:

- Local Authority Website Pages
- Patient Information Leaflet
- Local Authority Privacy Notices
- Children's Centres Registration Forms
- Child Health Card issued by Health Visitors

In preparation for the full implementation of the GDPR all Connecting Care Partners reviewed their informing materials and techniques and ensured that all of their relevant informing includes applicable information about Connecting Care.

4.2. User access to information held in Connecting Care Records

The approach to allowing access to the information held in Connecting Care records is as follows:

Legitimate reasons to access information held in records

All users of Connecting Care are required to select a legitimate reason for access to a record, these are tied to the relevant data protection conditions for processing in the GDPR and are as follows:

Ongoing Care Relationship

This includes both direct care and promoting well-being (early intervention) for which a legal basis has already been identified and agreed by the Connecting Care partnership.

Consent

Consent is only necessary where other legitimate reasons are not applicable, for example for approved and previously consented research by each participant.

Vital Interests

In circumstances where the individual is unable to give consent and no other legitimate reason is applicable, such as where there is severe injury or distress or where gaining consent would delay or put individuals at increased significant risk, information will be shared on the basis of 'vital interests' of the individual(s).

Safeguarding Concerns

This is only used when there are legitimate concerns for the individual and these concerns arise outside of a care episode. The same decision making process that is used when sharing personal data outside of Connecting Care for a safeguarding concern must be used when accessing information in Connecting Care.

Appropriateness of referral and clinical audit

This is only used where it is necessary to check the appropriateness of a referral to a service. There should be the possibility that the referral will be rejected as unsuitable and therefore no care based Legitimate Relationship will be established.

4.3. Opt-Out

If an individual over the age of 18, or a parent or other acting on behalf of their child or adult who lacks capacity, requests to Opt-Out of Connecting Care, they should be instructed to complete a Connecting Care Opt-Out form. Staff dealing with individuals asking to Opt-Out will be expected to discuss the benefits of the system and the impacts of opting out. They must ensure that these individuals are informed that their information will remain in Connecting Care, but that their records will not be viewed by users of the system, unless there is a safeguarding concern, in which case it will be available to those with explicit safeguarding duties. This is based on the legal duties identified in Appendix 3.

All Opt-Outs will be managed within the Connecting Care portal by the Connecting Care Team, once a written request to opt out of information being accessible via the system, has been received.

All individuals who have opted out of having their records accessible to users of Connecting Care have the right to opt back in at any time. There is an Opt-In form which can be requested from a member of care staff, to be completed by the individual. All Opt-Ins will be managed within the Connecting Care portal by the Connecting Care Team, once a written request to opt back in to allow information to be accessible via the system, has been received.

5. Information Exchanged or Shared Between Partners

5.1. Data to be shared

The detail of the data to be shared between partner and sponsored organisations and the roles that can view it, is available in **Appendix 1** (please note this appendix is correct at the time of issue and subject to change in agreement with all parties affected by a proposed change).

5.2. How information will be shared

Data for Connecting Care is shared electronically through the Orion Health Cross Community Care Record (CCCR) solution.

Further detail on the Orion Health CCCR solution can be found in ***Section 6 – Security***.

5.3. Data Accuracy

As required by the GDPR, all of the Connecting Care partner organisations agree that the data to be used is:

- Accurate
- Valid
- Timely
- Relevant
- Complete

Parties are responsible for the accuracy of data from their own clinical/social care IT system. In addition all parties as 'joint controllers' are responsible that the loading and access routines in Connecting Care promote and maintain accuracy. There are three categories of reporting processes when inaccurate data is identified:

- **Direct care impact** – where a user identifies an issue of accuracy that will have a direct and immediate impact on the provision or administration of a service to an individual. It is proposed that the identifying user reports issues directly to the service/team responsible.
- '**Anecdotal' concern** – where users generally feel data from other organisation(s) has frequent minor inaccuracies (with limited impact on the individual's care). These issues need to be captured as part of the project feedback.
- '**Individual' raises accuracy issue** – where an individual with access to their record or concern over something that may relate to accuracy makes this known. As the issue will be with data in source system(s), then the originating organisation must follow their policy of managing such issues.

5.4. Data retention

Retention of data is the responsibility of the originating organisation. If a data source removes information or a record, it will be removed from Connecting Care where the interface supports automatic purging. Where the interface does not support automatic purging a manual purge request must be made to Connecting Care.

5.5. Principles of using shared data

The information shared by Connecting Care partner and sponsored organisations, is only done so for the specific purposes detailed in this Data Sharing Agreement (see sections 2.3 & 2.4).

Much of the data being shared via the system is already shared via other, often less-secure methods, such as post, phone calls, emails and faxes. Connecting Care will negate the need for care professionals to gather key information using these methods.

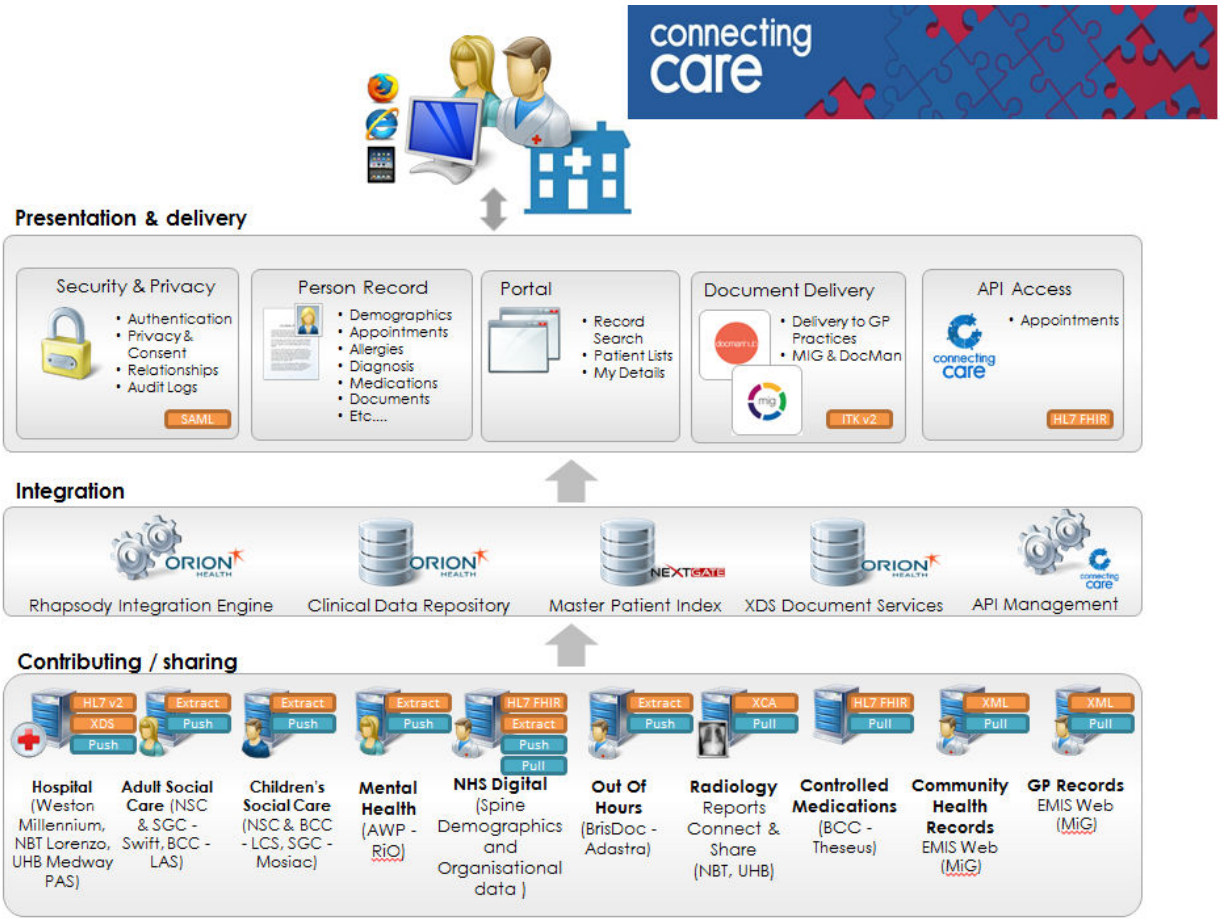
The Connecting Care solution contains functionality to allow some areas of the portal to be printed e.g. encounters, alerts and hazards.

For these areas a disclaimer is printed within the page footer, outlining the individual's details, document details e.g. printed by user, user email address X at date/time Y.

6. Security

6.1. Overview of the solution

The diagram below provides an overview of the Connecting Care Solution. The solution is provided by Orion Health and is known as the Cross-Community Care Record (CCCR). It comprises a number of components, as shown in the diagram below.



The current Connecting Care platform consists of five key pieces of technology, described below. These components may be built on over time.

Some of the data that flows into Connecting Care is redirected to other systems

Component	Description
1. An integration engine (Rhapsody)	Connecting Care uses the Rhapsody Integration Engine. Rhapsody is a well-established global product, and has been used for many years by many different NHS organisations. An Integration Engine allows us to receive and process many thousands of pieces of data a day from different health and social care systems in use in BNSSG.
2. A data repository / platform (CDR)	Connecting Care has 'Clinical Data Repository'[1]. This holds all of the local health and social care records that are shared with Connecting Care.
3. A view on combined data in a 'Portal'	The Orion Health Clinical portal is the current web browser based view of the *Integrated Digital Care Record*. It provides role based access to data held in the 'Clinical Data Repository'. It also links directly with EMIS systems to display GP and Community Records. Note that the portal also links to the XDS document sharing architecture. (See below).
4. A Master Patient Index (MPI)	Connecting Care combines health and social care records from many different systems. In order to match records from these systems, we use the NextGate 'MatchMetrix' product. This is a globally recognised product that essentially provides Connecting Care with our electronic master patient index (EMPI). An EMPI links the right patient to the right data. It cross-references patient identifiers from disparate systems and unites them using an algorithm and weighted set of criteria.
5. XDS document sharing architecture (XDS.b registration service, PCTI Docman and EMIS/MIG Document Work-flow	Connecting Care has created a standards based framework / approach to enable documents to be shared by any organisation in BNSSG to any organisation in BNSSG. The framework we are using is XDS. XDS is a set of standards to support sharing of documents across the continuum of care. It means that Connecting Care partners can publish / share information to the registry but retain the actual documents in their own source system or repository. This framework can be used to share any document from any organisation – using the same standards. It is currently used to share UHBristol documents into the Connecting Care Portal and to deliver electronic discharge summaries from UHBristol to GP Practices. This delivery is being done by PCTI Docman and EMIS/MIG Document Work-flow (depending on the GP practice's preferences) This is the same framework that we will use to share Radiology Reports…and indeed any other form of correspondence or documentation.

[1] Currently this is an Orion Health product

The solution has been accredited to NHS Interoperability Toolkit Standards. These are a set of national standards, frameworks and specifications to support interoperability of IT systems across local health communities.

6.2. Connecting Care Portal

The Connecting Care solution is hosted in the University Hospitals Bristol (UH Bristol) Data Centre, with a fail over site at Wynford House (Yeovil). The data centres have the following security features:

- Site Security
    - The Data Hall is run as a dark site, with no staff residency. Access is only given for maintenance and system changes.
    - The building is a purpose built data centre with strict staff access controls. These are multi-layer systems within the data hall having a secondary security system.
    - Only listed and approved 3rd level support staff can access the room. Contractors will be managed and accompanied at all times and follow strict change control guidelines for access.
    - The site is used for storing Patient identifiable Data for the UH Bristol trust, and NHS Trust Information Governance rules apply to all NHS staff who are given access to the data hall.

- Data and System Security
    - South, Central & West Commissioning Support Unit (SCW) managed systems and applications are on an entirely separate data network than UHBristol.
    - All SCW managed Data Networks, both Wide Area and Local Area are firewalled and managed by SCW IT Services staff, located in South Plaza, Bristol. Anti-Malware devices are in place between public data network and internal networks.
    - Wide Area Network links are point to point and have VPN encryption.
    - Standard Anti-Virus systems are in place on all SCW managed application servers and storage arrays located in UH Bristol DC and the back-up site in Wynford House.

6.3. Access Control

Access is managed by SCW with each partner organisation managing a process to identify and authorise their users. Each partner organisation has specific 'authorisers' who can approve access to Connecting Care, with user management centrally administrated by the SCW.

Access to data is based on a user's role and their need to access specific data items with respect to the needs of their role. Providers of data are advised to refer to the access control matrix in

Appendix 1 of this protocol. These matrices have been set out to meet the principle of adequate, relevant and not excessive access to data.

Access to the portal will be via a username and password. Once a user is logged onto the system, the solution will:

- Only grant access to applications to which he or she has clearance
- Only allow tasks to be carried out if the user has correct authorisation
- Deny access to specific individual's records or other information within the system (where the user is not authorised to view them)

6.4. Security Audit and reassurance

Auditing and testing of the Connecting Care solution will take place in line with the Connecting Care Information Security Policy. This includes penetration testing of the system used and the ability to audit access to information held on the Connecting Care Record. All Connecting Care partner organisations will receive quarterly audit reports which highlight specified activity and have the ability to request audit reports on individual users, where necessary.

7. Incident Management

7.1. Personal Data Breaches

Management of personal data breaches will vary depending on the sort of incident encountered. The process outlined in the Connecting Care Incident Management Policy should be followed. The policy is in line with the reporting recommendations in the NHS Digital guidance on the DSP Toolkit requirements, the Information Commissioner's Office (ICO) guidance and the requirements of the GDPR.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Any incident related to a breach of health or care data will be assessed for the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely there will be a risk, the ICO must be notified; if it is unlikely there is a risk it does not need to be reported to the ICO. However, if it is decided that it is not necessary to report the breach, this must be justifiable if queried, and must be documented.

A reportable breach will be reported to the ICO following the ICOs breach reporting procedures https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Where multiple organisations are involved, they will agree reporting between themselves as the incident does not need to be reported multiple times.

7.2. Informing individuals

Where an incident identifies that the confidentiality of an individual may have been breached, consideration will be given to informing the individual. Decision making will start from a position of informing the individual, unless there is good reason not to. Decisions on informing individuals will be taken by the senior health or social care professional in charge of service provision to the individual affected, taking advice from their Caldicott Guardian/Information Governance lead.

Where the breach has been caused by an individual in a different organisation, it will be the senior professional in the organisation(s) whose data has been compromised who will determine whether the affected individual should be informed as they will have the greatest knowledge as to the impact on the individual of the breach in relation to the type of data in question. If a situation such as this was to arise involving more than one other organisation, the senior staff involved will collaborate on deciding whether to inform the individual.

7.3. Responsibilities of parties

This protocol cannot set out management processes for all possible types of incidents, so other than the above, if an incident is encountered, all parties agree to:

- Act swiftly, but not recklessly to investigate any reports
- Engage any other affected organisation at the earliest opportunity
- Commit sufficient resources to conclude investigations in a timely manner
- Abide by the disciplinary policy of employing organisations.

8. Awareness Training/Communication to Involved Individuals

All users will have Information Governance training provided by their employers and will be advised of the User Guidance available at
http://nww.connectingcare.swcsu.nhs.uk/training.aspx

9. Monitoring & Review

A review of this agreement will be made, using the Data Sharing Agreement Change Process, in the following circumstances:

- In the event of any incident or 'near miss'
- Legislative/regulatory change
- Significant functionality change within Connecting Care programme
- For the addition of new data into Connecting Care
- For the addition of new organisations to the Connecting Care Partnership – partners or sponsored organisations
- Annually or at the request of a stakeholder

The appendices, as shown, may change following the circumstances described above. Rather than review and update the Data Sharing Agreement each time and require all organisations to reconfirm, the amended appendices will be agreed with each effected 'data controller' directly. Changes may not affect all parties, so any change in the appendices will be put to the relevant partner organisations.

10. Glossary

Aggregated data	Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data.
Anonymisation	Data rendered into a form that does not identify individuals and where identification is not likely to take place.
Controller	'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
De-identified data	Personal data that has been through anonymisation in a manner conforming to the ICO Anonymisation code of practice
Episode	Services provided to an individual with a medical or social care related problem within a specific period of time e.g. a visit to an emergency department for medical treatment is an episode of care
Direct care	A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of the 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.
Individual	Generic term used to cover the sector specific terms for members of the public in receipt of services such as 'patient', 'client', 'service user' or similar.
Legitimate relationship	The legal relationship that exists between an individual and the health and social care professionals and staff supporting their care.
Processing	'processing' means 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 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;
Pseudonymisation	'pseudonymisation' means 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;

11. List of Appendices

11.1. Appendices

The following Appendices are part of the Connecting Care Data Sharing Agreement.

Title	Description	Version	Last Updated
Appendix 1	Information sharing matrix – Roles and System	5.11	July 2020
Appendix 2	Information sharing matrix – Further description of items in Appendix 1	2.4	July 2019
Appendix 3	Legal Gateway matrix	5.0	October 2018
Appendix 4	Data Sharing Agreement signatory page	2.0	October 2018

11.2. Document Information

Document version	Date	Contributing Authors	Notes
V9.1	25/10/18	Helena Ashton	Final version following annual review and legislative changes
V9.2	23/05/2019	Phoebe Parsons	Appendix 1 and 2 version numbers updated
V9.3	30/07/2019	Phoebe Parsons	Appendix 1 and 2 version numbers updated
V9.4	29/08/2019	Phoebe Parsons	Appendix 1 version numbers updated

12. Signatures of Parties Agreeing to Sharing & Using Data

By signing this agreement, each organisation agrees to share information (as listed in Appendix 1 and 2) with Connecting Care, for the purposes outlined in this document.

Organisation name/ Practice	
Name	
Designation	
***GP Practice Only* - CDB number**	
Signed (on behalf of the organisation/practice)	
Date	

Please sign and send this Data Sharing Agreement back to

BY POST	BY EMAIL
Connecting Care **South West Commissioning Support** **3rd Floor** **South Plaza** **Marlborough Street, Bristol BS1 3NX**	**If you would prefer to send back a signature via email, please send attach the signed Data Sharing Agreement and email to connecting.care@swscu.nhs.uk**

If you have any questions please contact connecting.care@swcsu.nhs.uk

13. Signatures of Organisations Using Data ONLY

By signing this agreement, each organisation agrees to view information within Connecting Care, for the purposes outlined in this document.

Organisation name	
Name	
Role (Designation)	
Signed (on behalf of the organisation)	
Date	

Please sign and send this Data Sharing Agreement back to

BY POST	BY EMAIL
Connecting Care **South West Commissioning Support** **3rd Floor** **South Plaza** **Marlborough Street, Bristol BS1 3NX**	**If you would prefer to send back a signature via email, please send attach the signed Data Sharing Agreement and email to connecting.care@swcsu.nhs.uk**

If you have any questions please contact connecting.care@swcsu.nhs.uk