South West Strategic Information Governance Network (SIGN)

Information Sharing Agreement (Tier 1)

Version: V5.2

Date: May 2019

Document change history		
Version	**Date**	**Comments**
1.0 (draft)	01/05/2001	Initial draft based upon existing guidance and review of Draft Protocol developed in Gloucestershire
1.1 (draft)	28/03/2002	Incorporating initial comments received and updating to reflect organisational change
1.2 (draft)	08/05/2002	Incorporating amendments discussed with AL (South and West Devon Health and Social Care Community), RW (Plymouth Social and Housing Department) and SS (Information Governance Co-ordinator North and East Devon Health and Social Care Community)
1.3 (draft)	13/05/2002	Amending approval date for establishment of North and East Devon Information Governance Board and minor changes to organisational names
1.4 (draft)	17/05/2002	Acknowledgement of future expansion of review arrangements to operate elsewhere than North & East Devon (page 2). Removal of reference to x.400 protocol from Para 5.3 to reflect adoption of SMTP.
1.5 & 1.6 (drafts)	13/06/2002 & 08/07/2002	Incorporating amendments received during consultation with partner agencies
1.7b (final draft)	18/09/2002	Incorporating amendments received during consultation with partner agencies including 3rd party disclosure & addition of signatories page
1.7c	27/11/2002	Document circulated for signature following approval by Information Governance Groups in North & East and South & West Devon
1.7d	14/07/2004	Incorporating revised list of signatories
1.7e	30/08/2006	Incorporating revised list of signatories
1.7f	11/06/2007	Incorporating amendments discussed with SS, KJ, AB (Devon Primary Care Trust) and CH (Devon County Council A&CS)
1.7g	10/12/2007	Incorporating amendments received during consultation with partner agencies
2.0	03/05/2012	Review, amended and up dated in line with ICO Code of Practice by the Devon Information Governance Group
3.0	01/04/2013	Review and update in accordance with Public Health service transition to local authorities.
4.0	01/03/2016	Review and update to reflect organisational changes and legislation changes and updates
4.1	01/06/2016	Reviewed in line with guidance and documentation from across the South West SIGN
4.2	01/08/2016	Reviewed and updated based on feedback from the SW SIGN Group including GDPR update
4.3	15/10/2018	Formatting and updated following GDPR (not published)
5.0	13/02/2019	Reviewed and updated
5.1	25/04/2019	Updated following consultation with SW SIGN group
5.2	21/10/2019	Minor amendment to the declaration

Contents

1 Introduction

1.1. This agreement aims to provide partner agencies with a robust foundation for the lawful, secure and confidential sharing of personal data (information) between themselves and other public, private or voluntary sector organisations that they currently work with or would wish to work with across the evolving healthcare, social care and local authority environments.

1.2. This agreement will enable all partners to meet their statutory obligations and share information safely to facilitate the integration of service provision across the South West SIGN and to support better care outcome for individuals.

1.3. This agreement aims to support the following:

- Collaborative and integrated working in order to provide better health and social care;
- Implementation of new and national initiatives;
- Quality and audit processes;
- Health, safety and wellbeing;
- Provision of information (reporting and validation)

2 Purpose of the Agreement

2.1 The purpose of this agreement is to establish a guiding framework to manage exchanges of personal data within the South West SIGN taking into account Data Protection legislation; the General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act (DPA) 2018.

2.2 Where there needs to be more specific agreement about sharing data, it will be necessary to complete a Tier 2 information sharing agreement, see Appendix 3.

2.3 Where processing is likely to result in a high risk to the rights and freedoms of a natural person (refer to GDPR Article 35), a Data Protection Impact Assessment will need to be completed.

2.4 This agreement will:

- encourage the sharing of personal data and assist in the development of good practice across partners and integrated teams;
- provide the basis for South West SIGN wide processes which will allow monitoring and review of information flows and information sharing between partners;
- assist in the protection of partners from unlawful use of personal data;
- reduce the need for individuals to provide duplicate information when receiving an integrated service;
- reduce the reputation risk to the signatories that could be caused by the inappropriate or insecure sharing of special category data; and
- not be contractually binding but will set good practice standards that the sharing partners are required to meet.

2.5 This agreement does not imply an obligation on partner agencies to exchange data. Such decisions are subject to the policies of the signatory organisations.

2.6 This agreement should not be seen as an alternative to a Tier 2 agreement, Tier 2 agreements must be completed for specific information sharing projects between the partner organisations.

3 Scope

3.1 This agreement considers the foundation for all personal data and special category data processed by partners that is shared for the purposes of providing better care and to provide a more seamless service to the individual.

3.2 This agreement regards all personal data relating to an individual as confidential. Personal data should only be shared if there is a statutory obligation or lawful basis and is covered by associated procedures and/or agreements to this document between partners and/or specific services within that provides health and/or social care services to an individual.

3.3 This agreement refers to the Data Protection Act (DPA) 2018 for the definition of "personal data" and "data" as any information held either in manual or electronic records including that which is held virtually, on the internet and within social media, or records held by means of audit and/or visual technology about an individual who can be personally identified from that information.

3.4 The DPA further defines certain classes of personal data as 'special category', for which additional conditions must be met to ensure the information is used and disclosed lawfully. All partners under this agreement are expected to treat special category data in line with the conditions set out by the DPA.

3.5 This agreement defines processing and sharing of information as collecting, obtaining, recording, organising, discussing, holding, retrieving, altering, analysing, processing, destroying or disclosing data which can be transferred verbally, in writing or through electronic medium including images and photographs.

3.6 This agreement applies to staff working with or for the partner organisations (including voluntary or contracted staff), who manage, share and/or use information.

3.7 This agreement does not replace the need to conduct a Data Protection Impact Assessment (DPIA) on the information or processes involved.

4 Partnership Agencies Involved

4.1 This agreement requires each participating organisation, where appropriate, to have a nominated senior professional (e.g. Data Protection Officer, Caldicott Guardian or Senior Information Risk Owner (SIRO) in NHS organisations) who is responsible for:

- agreeing who in their organisation has access to the shared information;
- agreeing amendments to this agreement or any consequential arrangements; and
- ensuring mechanisms are in place to monitor the operation and to ensure compliance with this agreement.

4.2 This agreement will be developed and amended to include further changes in relation to legislation, organisational boundaries and best practice.

5 General Principles

5.1 The general principles underpinning the sharing of personal data follow the Caldicott guidelines on the protection and use of patient data:

- Justify the purpose for using confidential information;
- Only use it when absolutely necessary;
- Use the minimum that is required;
- Access should be on a strict need-to-know basis;
- Everyone must understand their responsibilities;
- Understand and comply with the law; and
- The duty to share information can be as important as the duty to protect patient confidentiality.

5.2 Tier 2 Information Sharing Agreements should be developed in line with best practice or using the template provided, which can be found in Appendix 3.

5.3 Any actual or potential breach of information security in relation to data transferred in accordance with any agreement should be reported immediately to the organisation's key contact and for them to follow their internal processes for reporting.

5.4 All data subject concerns about the processing of personal data should be addressed by the organisations involved with processing that data, by following their own internal procedures.

5.5 Disclosure of information to third parties not listed as a partner agency should involve the specific consent of the senior professional (e.g. Caldicott Guardian or SIRO) of the organisation originally supplying the information if its disclosure is for purposes other than those for which it was originally collected.

6 Defined Purposes

6.1 With reference to the general principles outlined in the General Principles section, the following justifiable purposes have been agreed by all participating organisations. These are examples and not inclusive or prioritised:

- delivering health and social care, treatment and services;
- assuring and improving the quality of care, treatment and services;
- monitoring and protecting public health;
- auditing and performance management;
- risk management;
- investigating incidents and complaints;
- managing and planning services (in line with National Data Opt Out);

- medical, health or social care research; (in line with National Data Opt Out);
- contracting for services;
- teaching;
- statistical analysis and reporting;
- where there are safeguarding concerns;
- ensuring holistic assessments of vulnerable individuals developmental needs;
- disclosure of information as appropriate for the purpose of legal proceedings; and
- sharing information in relation to carers;

6.2 When sharing information, the organisation should take appropriate, reasonable steps to ensure that the information is accurate, up-to-date and not excessive or irrelevant. Information sharing should be in accordance with:

- Section 7: Parameters; and
- Section 8: Access and Security.

7 Parameters

7.1 Transfers should contain no more than the minimum amount of personal data necessary for the task.

7.2 The NHS number and personal identification number are the main identifiers to be used in place of name and address wherever practicable.

7.3 Where information is required for a secondary purpose (i.e. for a reason other than direct care/consultation) pseudonymisation or anonymisation should be applied as appropriate, following advice from the Information Governance Lead in each organisation.

7.4 Specific agreement will be required (from the disclosing organisation's Caldicott Guardian / SIRO) prior to personal data being transferred for purposes other than those defined in the Agreement.

7.5 Where practicable, advice should be sought from the SIRO and/or Caldicott Guardian and the reasons for the final decision should be clearly recorded.

7.6 Publishing an accurate Privacy (Fair Processing) Notice is the responsibility of the organisation disclosing personal data. Guidance on developing a Privacy Notice is available on the ICO website.

8 Access and Security

8.1 All partner organisations are required to maintain policies governing levels of access and security and ensure they are adhered to. These policies should be made available to other partner organisations on request.

8.2 Staff must only have access to personal data on a need-to-know basis, in order to perform their duties in accordance with one or more of the defined purposes.

8.3 All partner organisations are required to ensure they have in place the mechanisms to enable them to address the issues of physical security, access control, security and confidentiality awareness training, and security management, and ensure they are adhered to, and/or comply with the assertions of the Data Security and Protection Toolkit appropriate for their organisation or have a robust action plan in place to achieve the assertions. Details of these should be made available to other partner organisations on request.

8.4 Data that has been shared with an organisation should be securely destroyed when no longer needed or in line with organisational guidance.

8.5 When transferring personal data between organisations by email then the transmission must use a secure method.

8.6 For further details in relation to the use of NHS Secure to encrypt information to non-encrypted email accounts, please refer to NHS Digital for advice and guidance.

8.7 It is the responsibility of the sender to ensure that the method is secure and that they have the correct contact details for the receiver. Any exchange of information must be part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated.

8.8 The receiver should only access the information from a secure device which is managed to the standards outlined in the National Cyber Security Centre (NCSC) guidance entitled “End User Device Security Collection” and any related documents that may be published by CESG or the NCSC from time to time.

8.9 Devices must not be left unattended unless they are locked so that the data is protected in the event of the device being lost or stolen.

9 Development, Monitoring and Review

9.1 This agreement will be developed to include purposes required by partner agencies and will be reviewed annually.

9.2 The nominated holder identified through the South West Strategic Information Governance Network, on behalf of the agencies shall:

- Subsequently review this document on an annual basis or after changes which will affect the content of the agreement; and
- Circulate all requests for change, co-ordinate responses, obtain agreement for the changes from the partnership and distribute codes of practice and guidance as these become available

9.3 Any partner may request changes to this agreement, however these will not be approved without agreement from all agencies.

Appendix 1: Legal Context and Basis for Sharing Information

Access to Health Records Act 1990
Gives patients' representatives right of access to deceased patient's medical records.

Caldicott Principles
The principles, which guide and reflect good Data Protection practice in the health and social care sector, are:

1. Justify the purpose(s) for using confidential information
2. Don't use Personal Confidential Data unless it is absolutely necessary
3. Use the minimum necessary Personal Confidential Data
4. Access to Personal Confidential Data should be on a strict need-to-know basis
5. Everyone with access to Personal Confidential Data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

Care Act 2014
Local Authorities have updated functions, to make sure people who live in their areas:

- Receive services that prevent their needs becoming more serious
- Receive information to make good decisions about care
- Have a range of quality services to choose from

Children Act 1989
Section 47 gives Local Authorities a duty to investigate or make enquiries to enable them to decide whether they should take any action to safeguard or promote child's welfare.

"(b) are informed that a child who lives, or is found, in their area- (i) Is the subject of an emergency protection order; or

(ii) Is in police protection; or

(iii) Has contravened a ban imposed by a curfew notice within the meaning of Chapter 1 of Part 1 of the Crime and Disorder act 1998; or

(c) have reasonable cause to suspect that a child who lives, or is found, in their area is suffering, or is likely to suffer, significant harm"

Data Protection Act 2018
Sets out the Data Protection framework in the UK, alongside the GDPR and sets out the key principles, rights and obligations for processing personal data.

Freedom of Information Act 2000
Gives individuals rights of access to know whether information is held by public authorities, and have copies of that information.

General Data Protection Regulation 2016
A regulation by which the European Parliament, the Council of the EU and the European Commission intend to strengthen and unify data protection for all individuals within the EU. The main principles with regard to the processing of Personal Data are:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

At least one of the conditions in GDPR Article 6 is met, and in the case of special category data at least one condition in Article 9 is also met.

Health Act 1999
Under Section 30 health authorities are encouraged to enter into partnership arrangements with social care services, in order to manage and provide services more effectively.

Health and Social Care (Safety and Quality) Act 2015: Duty to Share Information
Places onto a legislative footing the requirement of the seventh Caldicott Principle, that the duty to share information can be as important as the duty to protect patient confidentiality.

Mental Capacity Act 2005
Impacts on all staff working with or caring for adults (16+) who have impaired capacity to make their own decisions about health, social care and financial matters, making it clear who has authority to make decisions for them.

NHS Act 2006
Section 72 imposes a duty on NHS bodies and local authorities to "it is the duty of NHS bodies to cooperate with each other".

Privacy and Electronic Communication Regulations 2003
The Regulations compliment Data Protection legislation, giving people specific privacy rights in relation to electronic communications, with specific rules on:

- Marketing calls, emails, texts and faxes
- Cookies and the like
- Keeping communications services secure
- Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Appendix 2: Glossary

Anonymised information – information from which no individual can be identified

Data Controller – a 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.

Data Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Protection Impact Assessment (DPIA) – is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

Data sharing – the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. It can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.

Data Sharing Agreements/Protocols – set out a common set of rules to be adopted by the various organisations involved in a data sharing operation.

Data Subject Rights – established by legislation and each organisation is responsible for cooperating with other relevant organisations to implement these rights. See the Information Commissioners web site for further details.

Personal data – data that relates to a natural person who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from the information in combination with other information.

Processing of data – in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including —

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the
- information or data.

Pseudonymisation - is the process of disguising individual identity, and classifies as personal data. In contrast to fully anonymised data, pseudonymisation allows future or additional data to be linked to the current data, whereby the identity of the patient remains undisclosed. Key-coded data is a classic example of pseudonymisation.

Special category data – personal data consisting of information as to—

a) racial or ethnic origin of the data subject

b) political opinions

c) religious or philosophical beliefs

d) member of a trade union

e) Genetic data

f) Biometric data

g) data concerning health

h) sex life, or sexual orientation

Appendix 3: Template Tier 2 Information Sharing Agreement

Introduction

This Information Sharing Agreement provides a commitment by the signatories to ensure that a framework is in place that facilitates the sharing of information between partners and respects the individual's right to privacy. Information sharing is increasingly important in the provision of services to our communities.

Purpose

This Information Sharing Agreement facilitates the sharing of information for the purposes set out below.

We need to share this information because
You should explain why sharing this information will help each of the signatories to provide better services to our service users and communities.
Specifically information is shared to achieve:
What is expected to be delivered because of the sharing of this information.

Information being shared

This Information Sharing Agreement covers the following information, set out in the table below.

Information to be shared
List of all the information being shared.

Frequency of Transfer

Frequency of Transfer
How often is the data shared

Security of Transfer

Security of Transfer
How is the data shared and what are the security arrangements

Access to the information

Who will have access to this information
Named people, job roles and departments

Fair Processing (Privacy Notice)

How will data subjects be informed
Details of privacy notice, what information is available at the point of collection.

Right of Access

Right of Access
What arrangements need to be in place to provide individuals with access to their personal data if they request it

Legal Basis

Information must be shared lawfully. The Data Protection Act provides a legal basis for the processing of personal data which ensures information is disclosed fairly and lawfully. Other specific Acts will allow for this information to be shared.

Applicable Legislation
You need to remember that some information is protected from sharing or disclosure by legislation or Home Office guidance (certain health information, convictions) so you need to make sure that no such restrictions apply to the information you want to share. The legislation entered here should be the specific legislation relevant to the work that is being undertaken, for example in the case of Social care it would be the care act, if relating to a specific crime, it should be that particular act. All other service specific legislation should be entered, which relates to this piece of work. The legislation that should not be entered here is the Data Protection Act or other legislation which protects the information, as this is covered further down the document.

Data Protection Act Principles

The 6 principles of the Data Protection Act must be met in this Information Sharing Agreement. The table below identifies how the 6 principles will be met by both parties subject to this agreement. Please see the Data Protection Act 2018 for the full wording of the principles. The parties will ensure this agreement and the manner in which information is shared adheres in all respects to these principles.

These are all 6 Principles of the Act.		This is how they will be met.
1	Processed fairly, lawfully and in a transparent manner	Please insert how this will be met. Examples include: • Whether there is a legal basis for processing • Has the data subject been informed who has the information • Is a privacy notice available Who has been given access to the information

2	Collected for specified, explicit and legitimate purposes and not further processed for other purposes	Please insert how this will be met. Examples include: • The purpose the information will be used by each organisation Whether the information is shared elsewhere & if so, what precautions have been taken.
3	Adequate, relevant and limited to what is necessary in relation to the purposes	Please insert how this will be met. Examples include: • How the information will be limited to what is stated in this agreement • Whether information is merged with any other Whether additional information is collected, and is so what it is used for
4	Accurate and up to date	Please insert how this will be met. Examples include: • How information is checked. • How inaccuracies are corrected or updated and when Who is told about changes
5	Kept no longer than necessary	Please insert how this will be met. Examples include: • The retention that is applied How information is disposed of
6	Appropriate security measures	Please insert how this will be met. Examples include: • Hard copies stored securely • How electronic copies are secured folder on local computer drive. How Computer is security patched and virus protected

Special Categories of Data

Any information shared as part of this agreement, which is classed as Special Categories of Data is subject to schedule 1 of the Data Protection Act. Additional safeguards need to be applied to meet Part 4 of Schedule 1.

These are requirements which apply to satisfy Schedule 1:		
1	Employment, social security and social protection	Please delete as necessary.
2	Health and social care	Please delete as necessary.
3	Public health	Please delete as necessary.
4	Archiving, research and statistics	Please delete as necessary.
5	Substantial public interest	Please delete as necessary, or specify which public interest criteria is met.
6	Conditions relating to criminal convictions	Please delete as necessary, or specify

		which public interest criteria is met.

Additional safeguards for Special Categories of Data

Additional safeguards which apply to satisfy Schedule 1 Part 4:		
1	Appropriate policy document	Please specify how this will be met public interest criteria is met.
2	Record of processing	Which condition is relied on, (b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing)

The Parties will ensure this agreement and the manner in which information is shared adheres in all respects to the principles of the Data Protection Act.

No information will be forwarded on to a third party or sub-contractor without the express written permission of the Data Controller of the disclosing party.

Each party hereby undertakes to apply appropriate security measures to all information it processes under this agreement.

Information requests

Requests may be received under the Data Protection Act, the Freedom of Information Act 2000 or the Environmental Information Regulations. When a request for information which has been shared under this Information Sharing Agreement is received, the party which receives the request will inform the other and request its views about the disclosure or otherwise of the information.

Information retention

The information covered by this agreement will be stored for an agreed time. This retention period is set out in the table below.

Organisation name	Period Information retained	Disposal Date
Data Processor	Retention period	Date for Disposal

Information Disposal

All information subject to this agreement must be disposed of securely at the end of the retention period. Electronic forms of the information must be disposed of securely using a security accredited method of deletion. This includes any copies of the data which has been backed up or copied off site.

All paper forms of the information must be securely shredded. The costs of disposal will be met by the data processor.

Agreement Compliance

It is the duty of each party to this Information Sharing Agreement to ensure compliance with this agreement within their respective organisations.

Agreement Breaches

If any information which is shared under this agreement is lost, stolen, or disclosed to anyone who should not have had access to it, this should be treated as an information governance breach. The Data Controller for the breaching party must notify the other party of any breach as soon as it becomes aware. If there is suspicion of a breach, this also must be notified immediately. Investigation into the breach will be conducted by the Data Controller for the breaching party, with relevant escalation.

Peninsula Information Sharing Agreement Declaration

Partners/signatories

Partners that have signed up to this data sharing agreement are listed on University Hospitals Plymouth NHS Trust website.

If you would like your organisation to sign up to this agreement then identify the responsible signatory which will typically be the Senior Information Risk Owner and ask them to fill out this form. Once completed please email it to: informationgovernancepht@nhs.net

I am the Senior Information Risk Owner for the organisation below and confirm that my organisation is party to this agreement.	
Name:	
Job Title:	
Email Address:	
Phone Number:	
Organisation:	