SOMERSET OVERARCHING INFORMATION SHARING PROTOCOL (SOISP)

Supporting the Somerset Sustainability and Transformation Plan (STP) for safety, health and well-being

Version:	2.4 Final
Ratified by:	STP Information Governance Working Group
Date Ratified:	
Name of Originator/Author:	Peter Grogan
Name of Responsible Committee/Individual:	STP Digital Steering Group
Date issued:	January 2018
Review date:	
Target audience:	NHS Trusts, Somerset CC providers of NHS Services and Independent Contractors

SOMERSET OVERARCHING INFORMATION SHARING PROTOCOL

CONTENTS

SOMERSET OVERARCHING INFORMATION SHARING PROTOCOL

VERSION CONTROL

Number assigned to document:

Document Status:	Final
Version:	2.4

DOCUMENT CHANGE HISTORY		
Version	**Date**	**Comments**
1.0	09.03.2017	Initial Draft
1.2	09.05.2017	Second Draft
1.3	17.05.2017	Third Draft
1.4	12.07.2017	Fourth Draft
1.5	01.12.2017	Fifth Draft
2.0	27.12.2017	Final
2.2	27.01.2018	SIRO & Caldicott comments
2.3	01.03.2018	Updates to appendices
2.4	09.03.18	Further updates to appendices
Sponsoring Director:		**Peter Lewis** - Deputy Chief Executive, Taunton and Somerset NHS FT and STP SRO for System Performance and Enablers (Chair)
Author(s):		Peter Osbourne (IG Manager Somerset CCG), Louise Coppin (IG Manager Taunton and Somerset NHS FT), Peter Grogan (IG Manager SCC), Kevin Caldwell (IG Officer Somerset CCG),
Document Reference:		

SOMERSET INFORMATION SHARING PROTOCOL

1. INTRODUCTION

1.1 The organisation of Health and Social Care services in Somerset is evolving rapidly. The adoption of the Sustainability and Transformation Plan (STP), the new EU General Data Protection Regulation (GDPR) and updated Caldicott guidance, mean that as the County enters 2018 new ways of working and information sharing will have to be adopted.

1.2 This protocol sets key principles and standards for sharing personal data as defined by the EU GDPR and information in any recorded form including paper, electronic, audio and visual, in order to establish a framework for sharing of information across the health and social care community for the benefit of the people of Somerset. This will ensure there is high level governance for all participating agencies to refer to when establishing information sharing protocols for specific initiatives and activities.

1.3 Organisations, from the public, private and third sector, who provide services to the people of Somerset, are invited to adopt these principles and standards as their baseline approach to sharing personal information.

1.4 The aim is to promote a consistent approach to the sharing of personal information that will respect the privacy of individuals, benefit those to whom services are provided, support the commissioning of services by providers and inform research designed to improve service delivery.

1.5 Whilst it is vital for the provision of services, to an individual, that partners are able to share personal information, it is also important that individuals can trust the agencies involved to only share personal data based on a principle of "need to know".

1.6 The Health and Care report from the National Data Guardian (Dame Caldicott) in December 2017 has emphasised three principles:

a) To encourage sharing of information in the interests of providing direct care to an individual.
b) There should be no surprises to citizens and they should have choice about the use of their data.
c) There must be dialogue with the public, helping to increase their knowledge and choices about how data is used to improve health and care.

This ISP is designed to meet the statutory requirements and enshrine all three principles to support secure, effective and efficient sharing of personal information.

2. JOINT DATA CONTROLLERS

2.1 Chapter IV, section 1, Article 26 of the GDPR details the responsibilities of data controllers when sharing the responsibility for personal data.

2.2 When data is transferred from one organisation to another, and they do so on the understanding that both organisations will be using that data for a shared purpose as defined in Article 26, they are acting as Joint data Controllers.

> *"Where two or more controllers jointly determine the purposes and means of processing, they shall be joint data controllers. They shall in a transparent manner determine their respective responsibilities for compliance under this Regulation, in particular as regards the exercising the rights of the data subject and their respective duties to provide information referred to in Articles 13 and 14* ***by means of an arrangement between them..".***

2.3 This "arrangement" – protocol – is designed to facilitate a Joint Controller relationship with each of the parties sharing personal data, understanding the legitimising conditions for the processing and purposes for which the data is to be used.

2.4 When personal data is shared, organisations take joint responsibility for any personal information they share including: organisational and technical controls, breach reporting to the ICO, informing data subjects of a breach.

2.5 As described in Article 26.3, data subjects can exercise their rights against either of the respective joint data controllers.

3. LEGAL AUTHORITY FOR SHARING INFORMATION

3.1 Sharing personal information must always be within the legitimate activities undertaken by an organisation in providing a service to the public, set out in their legal powers (intra vires). This first tier Information Sharing Protocol (ISP) outlines the overarching principles and the legislation under which this will be done.

3.2 'Second tier' Information Sharing Agreements (ISA's) should add relevant detail of any specific legal powers organisations have to undertake sharing of personal data for identified purposes.

3.3 The Care Act 2014 – this legislation provides a clear duty on all public bodies to co-operate and provide a person-centred approach to the provision of health and social care services in the interests of the well-being of a person.

3.4 The Second Caldicott Report defined Direct Care as follows:

> *"A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of an identified individual. 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 (identified patient safety), the management of untoward or adverse incidents."*

3.5 The EU-GDPR in Article 6 "Lawfulness of processing" provides six lawful purposes for the processing of personal data:

a) the data subject has given consent
b) necessary for the performance of a contract
c) compliance with a legal obligation to which the controller is subject
d) necessary to protect the vital interests of the data subject
e) performance of a task carried out in the public interest
f) necessary to pursue a legitimate interest of the data controller (not applicable to public bodies)

The ICO guidance on this aspect of the GDPR is clear that public authorities in a position of power over the data subject should not rely on consent as a "fair" purpose for processing personal data and should seek another purpose.

3.6 The EU-GDPR Article 9 "Processing of Special Categories of Personal Data" stipulates that the processing of such data including that from health and social care can rely on one of ten exemptions to allow processing. Those relevant here included processing:

a) for which data subject has given explicit consent
b) is compliant with a legal obligation to which the controller is subject
c) is necessary to protect the vital interests of the data subject
d) by a not-for-profit organisation to pursue their legitimate activities
e) of personal data made public by the data subject
f) is necessary for legal claims by the courts
g) necessary for reasons of substantial public interest
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
i) processing is necessary for reasons of public interest in the area of public health
j) is necessary for archiving purposes in the public interest

3.7 The underlying legitimising for Health and Social care purposes under GDPR and the UK Data Protection Act 2018are summarised in this table.

Overall Purpose(s)	**Legitimising Condition under Article 9** **EU-GDPR**	**Common Law Duty of Confidentiality**	**Required Identification of individuals**
Delivering routine direct care and treatment across partner agencies. Somerset uses the definition of Direct Care defined by Caldicott 2 *"A clinical, social or public health activity….."*	9 (h) information can be shared on the basis of "the provision of health or social care treatment" 9 (i) information can be shared in the public interest to protect from serious cross border health issues.	Implied Consent is appropriate where it complies with the reasonable expectations	Identifiable data required

Overall Purpose(s)	Legitimising Condition under Article 9 EU-GDPR	Common Law Duty of Confidentiality	Required Identification of individuals
Safeguarding - Where emotional, physical, sexual, psychological, financial, material or discriminatory abuse/neglect is suspected, a crime committed or regulations breached	9 (b) Information can be shared to meet a legal duty or obligation that applies in social protection law. 9(c) Information can be shared on the basis of 'vital interests' of the individual(s)	Legal obligation or duty will over-ride any expectation of confidentiality	Identifiable data required
Prevention & detection of crime and the apprehension and prosecution of offenders, including terrorism	9 (a) Consent may be applicable, unless agreed by parties that informing and consenting may be reasonably expected to prejudice the situation 9 (b) A legal duty or obligation will apply in cases of terrorism and road traffic incidents European Crime Directive / UK Data Protection Act 2017	Legal obligation or duty will over-ride any expectation of confidentiality Where consent is obtained it must be "explicit" and managed in accordance with GDPR	Identifiable data required
Assuring and improving the quality of care / treatment, to include Symphony database.	9 (h) information can be shared on the basis of "the management of health or social care systems and services"	Implied Consent is appropriate where it complies with the reasonable expectations	Identity must be pseudonymised, reduced to an absolute minimum
Emergencies and Civil Contingency events	9(c) Information can be shared on the basis of 'vital interests' of the individual(s) 9 (g) Information can be shared for reasons of substantial public interest 9 (h) information can be shared on the basis of "the provision of health or social care treatment"	Implied Consent is appropriate where it complies with the reasonable expectations	Identifiable data required
Defence of Legal Claims or responding to Court requests	9 (e) Information can be shared on the basis of disclosure or Court Orders	Legal obligation or duty will over-ride any expectation of confidentiality	Identifiable data required
Managing and planning services Statistical monitoring of public health Commissioning and Contracting for services	This data ceases to be personal information when it is anonymised.	Caldicott opt-out will apply	All identifiers must be removed including the ability to reverse "pseudonymised" data. Identity must be removed entirely

Overall Purpose(s)	Legitimising Condition under Article 9 EU-GDPR	Common Law Duty of Confidentiality	Required Identification of individuals
Targeted Research purposes into an individual's medical condition	9 (a) Explicit Consent	Explicit Consent must be obtained to include an individual in a research programme Caldicott opt-out will apply	Identifiable data required

3.8 Common Law Duty of Confidentiality and professional secrecy.

Article 9.3 of the GDPR identified the need to accommodate the "professional obligations of secrecy". For the purposes of this agreement this is interpreted as the Common Law of Confidentiality between patient and health / social care professional. This ISP recognises that there is an implicit requirement that information should only be shared in the Health / Care pathway in a manner which the person might reasonably expect in the course of their treatment / care.

This must not be seen as a barrier to information sharing in the implementation of Better Care Models under STP integration of Health and social Care, as these models will clearly define the care pathway and the expectation of the person undergoing direct care.

3.9 Dame Caldicott has emphasised Caldicott principles 2, the duty to share personal data when dealing with the closer integration of health and social care and the need to ensure that perceived barriers to information sharing do not result in preventable harm or even fatalities as in recent Serious Case Reviews.

4. THE ORGANISATIONS

4.1 This protocol is designed to incorporate all organisations who share personal data, this includes:

a) public sector organisations
b) private sector providers under contract to the public sector
c) 3rd sector providers under contract to the public sector

Described by organisation type this would include Local Authorities, NHS Trusts, the Police, Fire and Rescue Services, GP Practices, Education providers, Housing Associations, Private sector and 3rd sector providers of services whose operations require the sharing of personal information. A complete list, at time of publication, is included in **Appendix A**.

4.2 The specific arrangements for any specific information sharing will be defined in either a 2nd Tier ISA, or a binding contract depending on the legal relationship between the parties involved.

4.3 The decision about whether or not it is appropriate to share personal information with another organisation or agency always rests with the data controller responsible for that data.

5. POLICIES AND GUIDANCE

5.1 This Information Sharing Protocol should be read in conjunction with ICO guidance on information sharing, Department of Health policy and guidance, the relevant organisation's data protection and information governance policies. A list of relevant national policy and guidance is available in **Appendix B.**

5.2 The Article 29 Working party (WP187) opinion on consent has now been codified into the EU-GDPR. This guidance makes clear that a public authority processing personal data based on a statutory requirement does not need consent and should not seek to obtain it. Consent to permit data processing is not consent to receive services and support.

5.3 The UK Government will in due course issue National Derogations and statute that will sit alongside the EU-GDPR. All organisations will need to ensure that these are complied with as required.

5.4 Local policies and guidance are issued by the organisations signed up to this Protocol, please refer to those organisations for their most up do date documentation

6. PURPOSE OF THIS PROTOCOL

6.1 In accordance with the requirements of law and "best practice" guidance, this protocol provides a formal agreement between public sector agencies and their partners and contractors to share information to safeguard and promote the well-being of our service users, wherever they reside.

6.2 This protocol will seek to promote the most effective and efficient methods of information sharing whilst recognising our duty of confidentiality and the right to privacy in respect of their personal information.

6.3 This protocol needs to be set alongside other documents within Somerset, which address the sharing of information between agencies for specific objectives.

6.4 The principles within this protocol should underpin any additional service specific ISAs, formal guidance and agreements that are felt to be necessary for the provision of services.

7. SIGNATORIES

7.1 It is intended that this protocol will be approved by the Caldicott Guardian and Data Protection Officers and signed by Chief Executive from each organisation and such representatives will endorse the whole of this protocol and abide by it. It is anticipated that organisations will join and may leave this Protocol and this will be reflected in amendments made to the list of signatories available in **Appendix A**.

8. LEGAL FRAMEWORK

8.1 All organisations must make themselves aware of the Acts of Parliament and other guidance. This Protocol recognises that we must comply with the legislation and directives. This list is not exhaustive and is subject to change and is included in **Appendix C**.

8.2 The EU-GDPR 2018 defines the rights of data subjects and the obligations placed on organisations as data controllers and data processors, these are detailed in **Appendix D**.

8.3 There must be transparency in the process of information sharing both within and between agencies and with service users by the use of Fair Processing Notices (FPNs).

8.4 Organisations will always seek a legal gateway for sharing personal data as defined by Article 9 of the GDPR. Consent of the data subject will only be sought if no other practicable way can be found to provide the required service.

8.5 Organisations must fully inform their data subjects as to what information is required, for what purpose, with whom will it be shared, how long will it be retained, how and when will it be destroyed.

8.6 Organisations must make provision for data subjects to object to the processing of their personal data and inform them of any implications of doing so relating to access or provision of services.

8.7 Organisations must inform the data subjects of their rights of access to the personal data held by the data controllers.

8.8 Information shared will be adequate, relevant and not excessive to fulfill the purpose. Evidence within each organisation's records will confirm that information has been shared in line with the principles contained within the EU-GDPR and relevant national and local guidance.

9. INFORMATION COMMISSIONER'S OFFICE (ICO)

9.1 The ICO are the statutory body with responsibility for the protection of personal data in England and Wales. They produce guidance documentation relating to interpretation of the law and on best practice. A list of relevant material can be found on the **ICO website**.

10. CALDICOTT PRINCIPLES

10.1 Dame Caldicott is the National Data Guardian and as such provides detailed guidance on the use of personal data in the field of Health and Social Care. Details of her principles recommendations are listed in are available in **Appendix E**.

11. PSEUDONYMISATION AND ANONYMISATION

11.1 Sensitive personal data will not be shared unless absolutely required by the request and legally justified. Data Controllers must have robust gateway controls over such data to ensure it cannot leave their organisation without agreement from a suitably senior officer.

11.2 Where pseudonymisation is applied to personal data it must be sufficiently altered to prevent the re-identification of individuals from the data shared. This can include a "manufactured ID" that will allow the originating organisation to re-identify an individual should that be required, but the recipient organisation must never be allowed access to the "key" to the manufactured IDs.

11.3 Each organisation is responsible for ensuring their de-identification process is sufficiently robust to prevent re-identification without the "key".

11.4 Where no re-identification is required and data is only required for statistical purposes the information should be anonymised, it must be sufficiently altered to prevent the re-identification of individuals by any party. At this point the information ceases to be personal data as defined by the EU-GDPR.

11.5 Where there is debate between sharing partners about pseudonymisation or anonymisation, reference will be made to the Anonymisation Code of Practice set out by the ICO.

11.6 **Confidential Patient data** - When sharing health information reference may also be needed to regulations controlling the use of patient confidential data between healthcare providers and commissioners. Unless a CCG is established as an 'accredited safe haven' (ASH), then patient confidential data cannot be received by the organisation, without a robust legal justification.

12. SHARING CLEARLY IDENTIFIABLE PERSONAL INFORMATION

12.1 The justification for sharing identifiable personal data can be done for the following reasons:-

- delivery of effective personal care, treatment and advice
- assuring and improving the quality of care, treatment and advice
- to safeguard children and vulnerable adults from harm
- individual's risk management
- to avoid duplication of information gathering
- investigating complaints or actual/potential legal claims
- teaching / staff development
- research – specific to data subjects

12.2 Sharing of personal/sensitive information must be done 'legally' and 'fairly'. The legal basis for sharing is set out in the EU-GDPR (2018), common law duty of confidentiality and the Human Rights Act (1998).

12.3 The legal framework is laid out in section 2 of this document. Data Controllers must ensure they engage an express legal obligation, act in the vital interests of the data subject, or they obtain explicit consent.

12.4 To share information fairly they must ensure the data subject is fully informed as detailed in section 6. Each organisation must ensure they provide details of the information sharing to the public when they make contact with them when services are delivered, on their web-sites, in public places etc.

13. SHARING PSEUDONYMISED PERSONAL INFORMATION

13.1 Pseudonymised information is defined by the GDPR as Personal Identifiable Data (PID) as it can still be re-identified by the originator who holds the original key.

13.2 The sharing of pseudonymised information can overlap with that of sharing identifiable data, but there are some specific additional reasons which despite removing the PID still may require the re-identification of individuals by the data controller:-

- monitoring and protecting public health, safety and well being
- Commissioning and planning services
- risk management
- auditing of accounts, care and performance
- statistical analysis and analytics

13.3 Where data is claimed to be pseudonymised it will need to conform to the ICO Anonymisation Code of Practice.

14. SHARING ANONYMISED PERSONAL INFORMATION

14.1 Anonymised personal data is not recognised by the GDPR as PID and as such does not require any legal basis for processing.

14.2 The sharing of anonymised information would be used in situations where the 3rd party does not need to know the identities of the individuals aggregated in the statistics:-

- monitoring and protecting public health, safety and well being
- commissioning and planning services
- risk management
- auditing of accounts, care and performance
- statistical analysis and analytics

14.3 Where data is claimed to be anonymised it will need to conform to the ICO Anonymisation Code of Practice

15. SECOND TIER INFORMATION SHARING AGREEMENTS (ISAs)

15.1 'Second Level' sharing protocols for the sharing of personal data for specific purposes developed in relation to these core principles, will detail how information is to be shared 'fairly and lawfully' by consideration of each of the following options, documenting and justifying the approach to be taken:-

- reference to specific legalisation which sets a duty to share, related to the purposes covered by the specific protocol Article 9 2 (h)
- reference to specific legal powers relevant to the purposes for sharing, including consistent approaches to justify public or vital interests Article 9 2 (b) (c)
- use of explicit consent (Article 9 2 (a) where specific legislation or legal powers are not applicable

15.2 'Second Level' sharing protocols should detail the processes for informing subjects about what is being shared and why:

- 'Actively informed' if the sharing is deemed to be potentially unexpected or objectionable
- 'Passively informed' can be used where the activity is reasonably expected and not objectionable

15.3 If necessary in specific situations, second level protocols will include potential justifications for not informing subjects. These must be related to appropriate provisions in GDPR such as 'Crime & Disorder exemptions' and 'Statutory Instrument/modification orders where allowing access would be likely to cause serious harm to the physical or mental health or condition of the subject or any other person'.

15.4 A list of current 2nd Tier ISAs is included in **Appendix F.**

15.5 Any second level sharing protocol sharing pseudonymised healthcare or Police information for commissioning or planning purposes should not include any identifying information such as name, identity number, date of birth and addresses without clearly documented justification for each item of data in the protocol. Such justifications must be based on the requirements of:

a) the 'Guide to confidentiality in Health & Social Care' (HSCIC Sept 2008)
b) recommendations of the Caldicott review (2013 – Information to share or not to share?)

16. EXPLICIT CONSENT

16.1 Explicit Consent is a legal basis for sharing under GDPR (Article 9 2 (a)). However given the complexities in obtaining, monitoring and managing consent in the complexities of the health-care arena the GDPR no longer requires this for the processing of special categories of data for the purposes of health and social care (Article 9 2 (h)).

16.2 Explicit consent should therefore only be used when no other legal basis for processing is available. This approach is supported by the ICO in their March 2017 guidance.

Example – the Police approach a data controller for personal data to establish if the person might be an unreliable witness. As there is no justification for disclosure under the prevention or detection of crime the data controller should establish that the data subject has given their consent for the processing.

17. DECEASED INDIVIDUALS

17.1 Information about deceased individuals will be treated as confidential, subject to the prevailing legislation concerning its use and disclosure, e.g. Access to Health Records Act 1990 and the decision notice by the ICO / Information Tribunal and provision of information to HM Coroner. (Note Tribunal ruling in case of 'Bluck' that section 41 exemptions under Freedom of Information Act 2000 apply to the deceased).

18. OBLIGATIONS FOR ORGANISATIONS

18.1 **Employee Confidentiality** - All employees have an obligation to safeguard the confidentiality of personal information. It is an offence to knowingly or recklessly obtain or disclose personal data without the consent of the organisation in control of the personal data, or without lawful excuse. This is governed by law, contracts of employment, professional codes of conduct and organisational policies. All staff must be made aware of their obligations through training and job induction procedures. All staff should understand the consequences to both the individual and themselves resulting from a breach of confidentiality.

18.2 **Information Security** – all organisations signed up to this protocol must ensure the following are in a place appropriate to the sensitivity of the information they are processing:

a) all personal information must be kept in a secure environment, where access is controlled, and security measures are in place aligned to best practice (ISO27000) for collection, transmission, storage and destruction of personal data such as encryption of email and mobile devices
b) they have appropriate policies covering the security, storage, retention and destruction of personal information
c) all employees are suitably screened and vetted prior to employment
d) that employees receive appropriate induction and annual refresher training in the safe and secure handing of confidential information

e) that employees are only allowed access to personal data on a "need to know" basis to do their job
f) that the data controllers are informed of all proposals for onward sharing to all contractors and sub-contractors whose terms must include all data protection and confidentiality clauses in original contracts

19. RESEARCH

19.1 Under Article 6.1 of the GDPR there is specific provision for tasks carried out in the Public Interest (6.1 (e)). This protocol will endeavor wherever possible to use the flexibility in A.6(2) to create a dedicated public interest legal basis for scientific research for the named organisations in this protocol, if such basis does not already exist that fulfils the requirements of Recital 41 and A.89(1). This will ensure there is a clear legal basis to support research.

19.2 If the sharing of specific person identifiable information, for research purposes, requires explicit consent on the part of the research participant (patient or member of staff), this would be in addition to any other conditions previously notified to the service user for information sharing between statutory/ partner organisations for the purpose of providing care.

19.3 Each organisation will have an appropriate protocol for research governance, including the approval of the information governance arrangements in relation to research projects.

19.4 Under Recital 45 the UK Government is expected to issue specific guidelines on the use of special categories of data for tasks carried out in the public interest.

> **EXTRACT** "It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association."

20. MONITORING THE PROTOCOL

20.1 Each organisation will have in place a governance structure appropriate to the sensitivity and volume of personal data it is processing. This may include:

- Information Governance / Management Board
- Data Protection Officer (DPO) as required by GDPR
- Senior Information Risk Owner (SIRO)
- Caldicott Guardian (Health / Social Care)
- Information Governance Manager

20.2 The following activities must be undertaken by each organisation to comply with the GDPR responsibilities to data subjects subject to the restrictions / exemptions laid out in Article 23 and Recital 73.

Provision of Data Subject Rights under GDPR

- Transparent and accessible information concerning the processing of personal data by the data controller
- Fully inform data subjects about data collected by the data controller in accordance with Article 13 and Recitals 60-61
- Fully inform data subjects about data collected from 3rd parties in accordance with Article 14 and Recitals 61-62
- Provide access to a data subject's personal data in accordance with Article 15 and Recitals 63-64
- Provide appropriate rights to rectification in accordance with Article 16 and Recital 65
- Provide appropriate rights to erasure in accordance with Article 17 and Recitals 65-66
- Provide appropriate rights to restriction of processing in accordance with Article 18 and Recital 67
- Provide appropriate rights with regard to notification relating to rectification, erasure and restriction in accordance with Article 19
- Provide appropriate rights to data portability in accordance with Article 20 and Recital 68
- Provide appropriate rights to allow objection to automated processing in decision making in accordance with Article 21 and Recitals 69-70
- Provide appropriate rights to allow objection processing in accordance with Article 21 and Recitals 69-70
- Provide appropriate rights to allow objection to automated processing in decision making in accordance with Article 22 and Recitals 71-72

21. New signatories to this Protocol

21.1 Any other providers of Services from whom services are commissioned in the future who wish to share personal data will need to sign this protocol as part of the contracting process. This will be reviewed in line with Information Governance tool kit and / or relevant procedures which will provide evidence to demonstrate assurance of compliance. See **Appendix G** for the signatories.

22. Termination of the Protocol

22.1 Where an organisation (or in the case of independent contractors, their lead organisation or commissioner) finds it is necessary to withdraw from the agreement to abide by this Protocol:

- they will, in writing, notify all other signatories to the Protocol of their intention to withdraw
- they will agree an exit strategy from the agreement such that the data holdings of the parties concerned can be secured to reflect the absence of their participation in the Protocol
- on agreement of an exit strategy from participation in the Protocol they will ensure that all staff are informed of the changed arrangements

22.2 Where an organisation has agreed an exit strategy from agreement to abide by the protocol all other organisations are responsible for ensuring that their staff are fully informed of the changing arrangements and the effect on normal working practices.

23. Review of this Protocol

23.1 This document should be subject to review when any of the following conditions are met:

a) the adoption of the protocol highlights errors and omissions in its content
b) where other standards / guidance issued by any participating agency conflicts with the information contained
c) where good practice evolves to the extent that revision would bring about improvement
d) 2 years from the date of approval of the current version

24. Indemnity and Non-Compliance

24.1 Information Sharing Protocols and Agreements are not binding legal contracts. As such there is no enforceable indemnity or legal action that can be taken in event of non-compliance or breach.

24.2 Those organisations listed in **Appendix A** who are under contract to service providers will still be subject to any indemnity or liability contract clauses. The SOISP is designed to facilitate information sharing but does not remove those contractual obligations.

24.3 The GDPR does states in the articles in Chapter IV, Section 1 that there must be formal recognition of e a relationship as either Joint Controllers or a Controller / Processor arrangement. For the purposes of this Protocol all organisations become joint data controllers responsible for the data they share and the purposes it is used for.

24.4 Organisations must complete a relevant compliance statement that must be provided to any sharing partner on request. This statement must include the:

a) legitimising condition for processing
b) purpose for data sharing
c) responsibilities for the partners in relation to data subject rights

Should a partner have concerns over the level of compliance, they should address these with the relevant organisation.

24.5 The organisational ‘data controllers’ are responsible for assessing the risk of sharing information with any other organisation where compliance is limited. This assessment should be based on the risk to information from sharing compared with the risk to the fulfilment and quality of the purpose information is to be shared for. Any serious disputes should be referred to the office of the Information Commissioner.

25. ORGANISATIONS - Appendix A

Public sector

- Taunton and Somerset NHS Foundation Trust
- Yeovil District Hospital NHS Foundation Trust
- Somerset Clinical Commissioning Group (CCG)
- Somerset Partnership NHS Foundation Trust
- South West Ambulance Service NHS Foundation Trust
- Somerset GP Practices
- Somerset County Council
- Somerset County Council Schools and Colleges (Compact Agreement)
- NHS England
- NHS Digital
- South Central and West Commissioning Support Unit
- Weston Area Health NHS Trust
- Royal United Hospitals NHS Foundation Trust

Private sector

- Care UK
- Nuffield Hospital
- Circle Bath
- Spire Bristol
- BMI Healthcare
- Marie Stopes
- British Pregnancy Advisory Service
- Somerset Care
- Somerset Doctors Urgent Care
- Devon Doctors Limited
- Somerset Primary Healthcare Ltd
- Independent Contractors for General Practice, Dentistry, Optometry and Pharmacy
- BUPA Home Healthcare
- BBraun

Third sector Voluntary and Charities

- Change Grow Live
- Turning Point
- St Margaret's Somerset Hospice
- Weston Hospicecare
- Children's Hospice South West
- Dorothy House Hospice
- Way Ahead Care

26. POLICIES AND GUIDANCE - Appendix B

- Caldicott Reviews (1997,2013 & 2017)
- Information Governance Toolkit (most recent)
- NHS Constitution
- Relevant Professional Codes of Conduct
- Information Commissioners Office Data Sharing Code of Practice 2011
- Memorandum of Agreement with the Police, Information Sharing Protocol, Safeguarding Adults Sharing Protocol
- Department for Education – 'Information Sharing for practitioners and managers' (Oct 2008)

27. LEGAL FRAMEWORK - Appendix C

- Access to Medical Reports Act 1988
- Caldicott Committee Report 1997
- Caldicott 2 Report 2013
- Carers (Recognition and Services) Act 1995
- Children Act 1989
- Children Act 2004 (Safeguarding Children)
- Children's and Families Act 2014
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- UK Data Protection Act 2017 / 2018
- EU-GDPR 2018
- Family Law Reform Act 1969
- Freedom of Information Act 2000
- NHS Act 2006
- Human Rights Act 1998
- Mental Health Act 2006
- Mental Capacity Act 2005
- NHS and Community Care Act 1990
- Confidentiality: NHS Code of Practice
- Patient Care Record Guarantee
- DFE Information Sharing for practitioners & managers 2008 (incorporating Every Child Matters and No Secrets)

28. EU GDPR Principles (UK Data Protection Act 2017) - Appendix D

GDPR - Article 5

Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5 (2)

- the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

29. CALDICOTT PRINCIPLES and GUIDANCE - Appendix E

- **Caldicott Report 1 1997**
- **Caldicott Report – To share or not to Share 2013**
- **Caldicott Report Data Security and Opt Outs 2017**

Extract from Caldicott 2 report 2013 – The Principles

There was widespread support for the original Caldicott principles, which are as relevant and appropriate for the health and social care system today as they were for the NHS in 1997. However, evidence received during the Review persuaded the Panel of the need for some updating, and inclusion of an additional principle. The revised list of Caldicott principles therefore reads:

1. **Justify the purpose(s)** Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian

2. **Don't use personal confidential data unless it is necessary** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data** Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to personal confidential data should be on a strict need-to-know basis** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities** Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Comply with the law** Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality.** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

These principles should underpin information governance across the health and social care services.

30.2ND TIER INFORMATION SHARING PROTOCOLS – Appendix F

Somerset CCG

Learning Disabilities	Somerset CCG Somerset County Council Somerset Partnership NHS FT Taunton and Somerset NHS FT Yeovil District Hospital NHS FT
EMIS Viewer	Somerset CCG Somerset GP practices Taunton and Somerset NHS FT Yeovil District Hospital NHS FT
EMIS Viewer	Somerset CCG Somerset GP practices Taunton and Somerset NHS FT Yeovil District Hospital NHS FT
RIO (SomPar)	Somerset Partnership NHS FT Somerset CCG
Caretrack	Somerset CCG CHS Healthcare Ltd
DARS	SCWCS Somerset CCG
GP Extended Hours	Somerset CCG Somerset GP practices
My Diabetes Phase 1	Somerset CCG Preston Grove Surgery My Diabetes My Health

- NHS Somerset, Avon Information Management and Technology Consortium (AIMTC) and Somerset Clinical Commissioning Group
- Somerset Partnership NHS Foundation Trust, Somerset Clinical Commissioning Group, Somerset Health Informatics
- Somerset Partnership Intelligence Unit and NHS Somerset Information and Performance Team
- Graphnet
- Bridgwater Federation of General Practices Enhanced Care Hub (ECH)

Taunton NHS Trust

SCCG EMIS Viewer
CHWL_Somerset_2Tier_v102 v2
LD 2nd tier ISA v7
ISA with TST Dec14 - SCC Death Notifications
Somerset ISP v1 14 July 2014
Somerset Data Sharing Agreement 2014
OISP Somerset May 2017 v1.2
Data Sharing Agreement Taunton and Yeovil Orthopaedic Hip and Knee Access to EPRO
EPRO Access for St Marg's Hospice
EPRO Access for Community Tissue Viability Nurses
Offshore and Internet Connection Addendum - IEP Data Sharing Agreement v1.3
ETMC_Taunton and Somerset NHS - Information Sharing Agreement - 04082016
Image Sharing Agreement 0 6
N3 Data Sharing Agreement V2 0 March 2013
Nuffield PACS Data Sharing Agreement - Taunton doc v2
Alliance Medical Limited for CT Scanning
ReStart - Taunton Somerset Data Processing Agreement FINAL
Data Sharing Agreement - MobiMed Smart (Monitoring ePCR) v1 (mb)
BEACON signed Information Processing Agreement Aug 17 Andrew Morgan
ISA Alliance Medical Ltd re primary care MRI scans
Free D Path
Free D Path
Free D Path
HSCIC CP-IS
Questback
DeepMind Health
IMS MAXIMS
Bluewire (EPRO)
Equiniti

Yeovil NHS Trust

- NHS

Somerset Partnership Trust

- NHS

Somerset County Council

- Somerset Partnership NHS Trust - Mental Health
- Somerset Partnership NHS Trust – Community Health Visitors

Taunton NHS Trust, Yeovil NHS Trust,

- Somerset Partnership NHS Trust – Special Educational Needs & Disability (SEND).

Second Tier ISA Templates

Generic 2nd Tier ISA v1.doc

31. SIGNATORIES - Appendix G

Organisation	Role (CEO / SIRO / Caldicott / DPO)	Print Name	Signature	Date
Somerset CCG				
Taunton NHS Trust				
Yeovil NHS Trust				
Somerset Partnership Trust				
Somerset County Council				