Overarching Information Sharing Protocol – Core Principles

A set of agreed principles & standards and a framework for developing information sharing protocols.

Development facilitated by SCW.

If you need further copies of this document or in a different format please email scw.westig-enquiries@nhs.net

May 2018

South, Central & West Commissioning Support Unit		
Document status: **Revised draft**		
Version	**Date**	**Comments**
1.0 - 1.5	February 2002	Issued for sign up to organisations
2.0 - 2.5	March 2003	Reviewed and updated
2.6	May 2003	Comments incorporated from stakeholder consultation
2.7	Jan 2005	Initial revisions following review group - Jan 2005
2.8	March 2005	Incorporating review group comments, prior to signatory (existing & potential) and patient group consultation.
3.0	May 2005	Incorporate comments from wide consultation - issue for organisational sign up
3.1	March 2007	Re-drafting of document along principles discussed by Avon, Gloucestershire, Wiltshire Information Governance Forum
3.2	April 2007	Revised following comments and discussion during stakeholder workshop
3.3	May 2007	Revised following consultation with stakeholders.
4.0	July 2007	Incorporate final stakeholder & representative group comments
4.1	April 2010	Draft revision commenced in 2009 for consultation
5.0	June 2010	Comments from consultation incorporated and issued for organisational sign up.
6.0	August 2012 (issued December 2012)	Regular review - issued for stakeholder consultation in October 2012
7.0	June 2015	Biennial review
8.0	May 2018	Reviewed and updated for Caldicott Review 3 and GDPR.

1 Purpose, overview and management:

Information sharing is a key enabler for the provision of effective services to individuals particularly where a co-ordinated approach across agencies is required. If poorly managed this contributes to a failure to provide effective services, the potential to suffer a damaging loss of data, confidentiality breaches and privacy concerns for individuals.

This was validated by the second Caldicott report (April 2013) establishing a new principle that 'it can be as important to share information as to protect it.'

Information sharing between agencies is often defined in a framework of three levels:

1. A top level shared and documented commitment to key principles, standards and purposes between organisations.
2. A Second level functional agreement defining the information to be shared, how it will be shared and when
3. At the third level, for frontline staff, tools and methods for actual sharing (ref :https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice)

This document[1] sets out the top level commitment by all participating agencies to adhere to the principles, standards and directions defined within it. The commitment covers the sharing of personal information in any form by any method, including verbal, paper, recorded and electronic formats. This document applies to sharing between organisations and professionals. It does not cover communication between professionals and patients/service users, or carers.

The aim is to promote a consistent approach to the sharing of information that will benefit individuals and services whilst protecting the people that information is about.

This protocol will be reviewed every two years, or at the request of any organisation using the document if there is a concern over the document's fitness for purpose, or when there is a change in governing legislation.

The document has been reviewed in line with the second and third Caldicott reports, regulations for processing personal data for commissioning and the General Data Protection Regulations (GDPR).

Organisations will use their own internal Data Protection Impact Assessment processes to support and guide the implementation of information sharing.

[1] This document was originally developed from a core 'sharing agreement' used across the Avon, Gloucestershire and Wiltshire communities since 2003.

2 Information Sharing Key Principles

2.1 Does personal data need to be shared?

Key principle - inclusion of any data that might identify an individual must have a legal basis, be justified and agreed as both necessary and proportionate to achieve the purpose(s).

Any activity to share data must first consider if 'identifying personal information' is required and if so to what degree. Information can generally be put into two categories, depending on what it is being used for.

- Information shared to benefit the individual or others, usually requiring clearly identifiable data. This is mainly related to the delivery of personal healthcare, public health, social care and early help. 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.

- Information shared for the benefit of the public or sections of society. Such information is often used to inform decision making or planning. It may range from completely anonymous statistics to raw datasets that include items of data that relate to a greater or lesser degree to individuals' identities. This is often 'not direct care related' as defined in the Caldicott report as: activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which falls outside the scope of direct care. It covers care services management, preventative medicine and medical research. Examples of activities would include risk stratification, service evaluation, needs assessment and financial audit.

The starting point will be that a 'privacy by default' approach will be adopted by any process for sharing information; therefore the inclusion of any data that might identify an individual must be justified by identifying a valid legal basis and it must be both necessary and proportionate in order to achieve the purpose(s).

2.2 Sharing clearly identifiable data (generally for direct care purposes)

Key principles

- **Data must only be shared if there is a legal duty, an overriding public interest/vital interest of the individual or a legal basis to justify the exchange.**
- **Individuals must be informed about data sharing unless there is a robust reason not to inform them.**

Sharing of personal and special categories of information must be done fairly, lawfully and in a transparent manner. A legal basis for sharing personal information must be

identified and the conditions set out in Data Protection Legislation[2] must be met, common law duty of confidentiality and the Human Rights Act (1998).

Legal duties, robust public interests and vital interests are related to conditions in Data Protection Legislation and are recognised practice in the common law of confidentiality. The General Data Protection Regulations allow processing of special categories of personal data when it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services[3].

In addition sharing must be fair and transparent by ensuring the subject is aware of what is being shared and for what purpose. Only in situations where informing the subject is likely to cause them or others significant harm/distress, or prejudice actions or outcomes of a situation, can this principle be set aside. If an individual lacks the capacity to make a decision, they should still be informed in an appropriate manner if possible.

It is also useful to reference the 7th Caldicott Principle as set out in the second Caldicott report (2013) 'The duty to share information can be as important as the duty to protect it' when considering the basis for sharing data.

Deciding the basis of justification:
Where sharing is to take place a 'Second level' sharing protocol is required in relation to these core principles, this will detail **how information** is to be shared fairly, lawfully and in a transparent manner, by consideration of each of the following options, in order, documenting and justifying the approach to be taken this may include:

1. Reference to specific **legal powers/gateways** relevant to the purposes for sharing, including consistent approaches to justify public or vital interests to sharing. The legal basis for sharing special categories[4] of data for direct care may be provided under GDPR Article 9.

2. Reference to specific legislation which sets a **duty to share**, related to the purposes covered by the specific protocol.

3. **Where it is deemed absolutely necessary to rely on consent**, the reasons to be documented including measures to fully inform subjects of the activity and an agreed process to manage and record consent

'Second level' sharing protocols will detail processes for informing subjects about what is being shared and why. Where necessary they will include potential justifications for not informing subjects. These must be related to appropriate provisions in Data Protection legislation and 'Statutory Instruments/modification orders *'where allowing access would be likely to cause serious harm to the physical or mental health or condition of the subject*

[2] Data Protection Legislation includes: General Data Protection Regulations (2016), Data Protection Act 2018
[3] GDPR Article 9(2)(h)
[4] Under GDPR this is Personal Data revealing a Data Subject's racial/ethnic origin, political opinion, religious/philosophical belief, trade union membership, genetics or biometrics (used to identify them), health, sex life and/or sexual orientation.

or any other person'.

Note - The Data Protection legislation does not apply to information on deceased individuals but general principles of common law and Human Rights should still be applied.

2.3 Sharing for administration, management, planning and developing services where there is a need to include some identity factors

Key principles:

- **Information shared for planning and developing services must only contain identifying items if absolutely required, and only the bare minimum required.**
- **If after removing as much identifying information, one or more identifying factors remains, the principles relating to justifying the sharing of identifiable data (section 2.1) must be adhered to.**
- **Careful attention to regulations governing the control of personal data in health and social care commissioning must be taken into consideration (refer to the current regulations at the time the sharing is proposed).**

Information is classed as 'personal' and subject to the Data Protection legislation if it relates to a living individual who can be identified from those data, or from other information, which is in the possession of, or is likely to come into the possession of the Controllers. A second level sharing protocol which shares statistical information for planning purposes should not include any identifying information such as name, identity number, date of birth and addresses without a robust and documented legal justification for the use of each item of data.

Where information relating to ages of individuals is required, consideration will be given to using age brackets/groups. If age brackets are not appropriate, the smallest amount of data on the date of birth will be used that will satisfy the purpose. Often the year of birth will suffice. Where a purpose requires information on addresses of individuals, a part postcode will be used, unless more accurate location information is required. Full postcodes should only be used where absolutely required and where advice has been taken from Information Governance specialists. Many uses of full postcode when combined with other data make the data set identifiable and some postcodes relate to just one property.

Any extraction of data that includes potentially identifying information and especially where the extraction features small numbers of cases (counts of less than 5 records), should be referred to the Information Governance Leads of the organisations concerned to ensure that the data in either raw or combined state does not identify individuals, or if identification is at all possible, that compliance with data protection legislation is in place.

The National Data Opt[5] out will be respected in all data sharing.

[5] https://digital.nhs.uk/services/national-data-opt-out-programme

2.4 Anonymous/pseudonymised data - shared for planning, developing services

Key principle:

- **If data is truly and permanently anonymised it can be shared provided it relates to the legitimate business of the partner agencies. Whilst legal requirements are not so stringent it is good practice to only share relevant and required information.**
- **Additionally if data has been pseudonymised it can be shared with other agencies who do not have the 'key' to reverse the pseudonyms, however, under the General Data Protection Regulations adequate protections are still required.**

If the data to be exchanged does not in any way identify individuals and cannot be combined with any other data that would lead to the identity of individuals, then, provided the organisations sharing the information are acting within the range of activities they are legally set up to do (their 'vires'), information can be shared. **In situations where data is to be shared on an ongoing basis, especially where the sharing will be relatively frequent, then a specific exchange agreement is required.**

Pseudonymised data is regulated by GDPR, however certain provisions are relaxed. Personal data which have undergone psuedonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person and therefore compliance with the provisions of the GDPR will be required.

3 Justifications and related purposes for sharing information

The table below sets out high level purposes and potential justifications for sharing personal information based around the requirements of the Data Protection legislation. 'Second level' protocols should identify specific provisions of GDPR and the latest Data Protection Act which apply.

If a purpose is not listed it does not mean that information cannot be shared. 'Second level' sharing protocols should add relevant detail of the legal powers organisations have to undertake activities that require sharing of information. In addition the levels described below are starting points for consideration it is possible that in relation to any purpose there could be a situation where a different justification is made. The column for either direct care or secondary use is based on definitions from the NHS Digital:
http://content.digital.nhs.uk/yourinfo

Example justifications for sharing personal and special category information, this is not comprehensive or definitive but provides examples.

Overall purpose(s): The purpose of sharing and processing personal information	**Possible justifications** Legal basis and GDPR Article 6 and 9 conditions; these will change depending on the circumstances	**Initial level of identity** Will data be identifiable?	**Direct Care/ Secondary Use/Public interest** Overall purpose
Delivering routine care and treatment across agencies	GDPR Article 9(2)(h)allows processing of special category information if necessary for the purposes of preventive or occupational medicine. GDPR Article 6 condition also required.	Identifiable data generally required - second level protocol may not be necessary	Direct Care
Safeguarding & protecting vulnerable individuals - including: where emotional, physical, sexual, psychological, financial, material or discriminatory abuse/neglect is suspected, a crime committed or regulations breached.	There may be a legal obligation to share information(e.g. Children's Act 2004; Care Act 2014) Sharing may be in the vital interests of an individual	Identifiable data generally required - second level protocol/document may be required - which may reference national guidance on such matters	Direct Care
Prevention & detection of crime and the apprehension and prosecution of offenders, including terrorism	There is a legal duty to share information in certain circumstances. (e.g. Prevention of Terrorism Act 2005; Road Traffic Act 1988; Female Genital Mutilation Act 2003) The Crime and Disorder Act 1998 also provide a duty in certain circumstances to cooperate with the Police.	Identifiable data generally required - Second level protocol likely to be necessary for regular sharing.	Public interest linked
Assuring and improving the quality of care / treatment	Where sharing is between public authorities involved in health and social care, then this may be based on the existence of a public duty and the management of health or social care systems. This is supported by the Health and Social Care Act 2012 and the activities of the Care Quality Commission In certain cases explicit consent may be required.	Identity should be removed entirely or reduced to an absolute minimum. Specific documentation on the purpose, basis and legal justification required.	Local clinical audit - direct care. Other uses are secondary.
Managing and planning services. Monitoring and protecting public health. Contracting for services.	If any identifiers are required then there must be consideration to GDPR Articles 6 and if required 9. Consent, public task, legal duty or section 251 approval in place to permit the sharing.	Identity should be removed entirely or reduced to an absolute minimum. Specific documentation on the purpose, basis and legal justification required.	Secondary use

Emergency planning & preparedness	Reference to be made to Cabinet office information sharing guidance under the Civil Contingencies Act 2004 and 'Data Protection Sharing guidance for Emergency Planners and responders', Duties to share do not override Data Protection legislation. Consent can be used and should be considered, but may be impractical. Disclosure in the public interest may be necessary and it may also be in the vital interests of individuals.	Limited personal or special categories of personal information may be used in emergency situations. Planning and testing may be possible without identifiable data. Specific sharing documentation at the second level is likely to be required.	Public interest linked

4 Organisational responsibilities (Data Protection Compliance & 'Caldicott Principles'):

All signatories of this Protocol will comply with all relevant legislation guiding and supporting information sharing. All organisations must ensure that they have adequately addressed all of the following responsibilities and be prepared to assure sharing partners of their compliance, when entering into a sharing agreement.

- Organisations must actively inform individuals of how their information may be used and to whom it may be disclosed by provision of appropriate materials in a variety of formats and through contact with staff. It must highlight their rights and provide details of the processes for individuals to invoke them. It must also include the legal basis for processing and meet the requirements of GDPR.
- Organisations must complete and maintain a Data Protection registration with the Information Commissioner's Office detailing all sources, subjects, purposes and disclosures relevant to their business and partnerships under any agreement.
- Organisations will maintain internal records of data processing activities as required under GDPR[6].
- Organisations must maintain the accuracy of data they share. Where necessary, partner organisations will be informed of any changes to the data they have received and also notify the source organisation of any error they discover. A key item for accuracy is use of a consistent shared identifier, such as the NHS number, so that information shared is linked to the correct individual.
- Organisations must ensure that the collection and sharing of information is necessary and proportionate to the purpose(s), and neither excessive or inadequate.
- Organisations must maintain the confidentiality of data in any form, during collection, transmission and storing with appropriate security arrangements and general compliance with ISO27000.
- Specific second level agreements must be in place wherever personal/special category data is shared.
- Second level agreements will detail the security requirements, but as a minimum these will include access by encrypted link, transfer by encrypted email or encrypted removable media/mobile devices (where encrypted email is not possible

[6]GDPR article 30

or sharing is taking place in person).

- Organisations will apply relevant regulations to the retention & disposal of records, only keeping information for as long as is necessary in relation to the original purpose(s) for which it was collected.
- Organisations will ensure all staff are educated to manage information appropriately in line with these principles and organisational policy on the collection and uses of information, supported by contractual terms of employment.
- Organisations should ensure that access to shared information is on a strict 'need to know' basis and is justified either by a clear legal basis for accessing the information. Onward sharing with 3rd parties will also be managed on the 'need to know' and legal justification basis and where possible the original source(s) should be informed.
- Organisations will ensure that any 3rd parties providing a service to them agree and abide by these principles by inclusion in contracts/agreements.
- Where consent is relied upon organisations will have processes/systems in place for recording consent.
- Organisations in receipt of a request that covers personal data provided by another organisation, will discuss the situation with the other organisation prior to disclosure and aim to develop a consensus view on any potential exemptions.

5 Indemnity & non-compliance:

At the level of principles and standards adopted by organisations there will not be any indemnity between organisations relating to actionable situations arising from information sharing. The need for indemnity should be assessed in second level protocols. Organisations will complete a compliance statement (overleaf) that should be provided to any sharing partner on request. Should a partner have concerns over the level of compliance, they should address these with the relevant organisation. The organisational 'data controllers' are responsible for assessing the risk of sharing information with any 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.

6 Second level documentation:

Each service/initiative basing sharing on these principles, is responsible for creating procedure documentation detailing how information will be shared securely, and how the principles have been applied including how sharing can be audited. Where required this will be a specific 'Second level' protocol, with appropriate guidance and process documentation.

When is second level documentation required and what should it look like?
Second level documentation is often required to achieve some (or all) of the following:

- Consistent and agreed approach to the exchange of data with clarity over responsibilities for the confidentiality, quality, security and availability of data
- Agreement on specific legislation, directions, standards and guidance relevant to the subject/initiative.

- Set out specific data items to be exchanged, the frequency, the security requirements and the agreed methods of exchange or access.

Second level documentation can be set out as one of a number of document types, including:

- Shared organisational policy and procedure - for example sharing information on vulnerable adults is best documented as an intrinsic part of an overall cross organisational shared policy and procedures on supporting vulnerable adults.
- Specific information sharing agreement - typically used where an initiative requires specific data to be shared between identified agencies/contacts within a stipulated timeframe and is extracted, compiled and securely transferred. (Data Push)
- System access agreement - typically where the data to be shared is enabled by providing access to it within an information system to partner organisations. This will define how system access controls are to be applied, how users are to be managed and how any issues/incidents will be handled as well as any specific detail required around the sharing.
- Governance arrangements for integrated/shared services - where staff are to formally work together in at least a partially integrated manner, the core governance documentation around such services must reference the relevant information resources and the access and control of them.

Second level documentation will feature the following unless clearly not required:

- The perceived benefits, to any party, related to the purposes for sharing the information. To be described as clear objectives and include processes to review appropriateness or agree further purposes
- Description of the legal basis for sharing relating to the purpose(s) including specific context legislation, noting any duties, powers or obligated controls on information and including Data Protection/GDPR conditions relied upon.
- Clear detail of the level of identity used in the sharing of data (where applicable) and where necessary assessing the level of identity from activity to combine sets of data - where individual data sets may not be identifiable, but become so when combined.
- The level of detail required in the data to be shared, ensuring it is the minimum required for the purpose and a process to determine and agree if more detail becomes necessary.
- How data subjects will be informed of the sharing of data unless legal exemptions are applicable. Where the data sharing is expected, then a privacy notice accessible to individuals may be sufficient. Where it is not expected specific informing activity is likely to be required.
- A commitment to accuracy and completeness of data exchanged, including a process for informing all relevant parties of any inaccuracies identified
- Agreement to the process for exchange, taking account of threats and vulnerabilities in the proposed communication methods and ensuring adequate and agreed safeguards to protect the information during transit and storage are in place, including as a minimum robust encryption of data transferred electronically.
- Agreement to the period of retention of data - with reference to organisational retention schedules.
- Agreed destruction processes relevant to the nature of the information (i.e.

confidential shredding/deletion).
- Description of the timescale and frequency of exchange of data
- A process for managing breaches of security, inappropriate disclosure of data and loss of data

7 Organisational compliance statement

The following activities must be undertaken to comply with responsibilities set out in this document. Each organisation using this document is required to indicate whether relevant activities are in place or in development. In completing the statement, reference should be made to appropriate organisational policy, process and guidance documentation.

Completion should be by the Organisation's nominated Data Protection Officer/Information Governance Lead. Each signatory must store their own statement and be able to provide it to another signatory on request.

Organisational responsibilities:

Responsibility area	In Place? In Progress/target date?
Keeping subjects informed	
■ Active provision of information to patients/service users of the uses to which information about them may be put and to whom it may be disclosed.	
■ Publicise and implement processes to provide access to records to subjects on request and to meet all individuals' rights under GDPR	
Protect information	
■ Have documented processes to check the accuracy and clarity of data both with the subject and on information systems	
■ Protect the confidentiality and security of data in any form, during collection, storage and sharing with appropriate security arrangements (generally compliant with ISO27000 Information Security Management standard) - via relevant policy, process and staff guidance on handling information ■ Have facilities to encrypt data sent via email, placed on removable media, or stored on mobile devices	

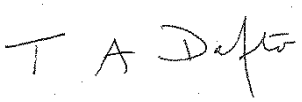
■ Documented policy and process relating to retention and disposal of information & equipment	
■ Ensure contractual arrangements with staff (employment terms), contractors and other suppliers/individuals handling identifiable information contain reference to confidentiality/non-disclosure, secure data handling and destruction	
■ Provide education and training to all staff on the safe handling of personal data including sharing/disclosing information. ■ Control access to shared information on the 'need to know basis'	
■ Complete and maintain a Data Protection registration with the Information Commissioner's Office detailing all sources, subjects, purposes and disclosures relevant to their function and partnerships under any agreement ■ Maintain internal records of processing activities	
Monitoring	
■ Have incident and risk reporting arrangements that incorporate information related issues Audit & assess security of information flows and information systems Perform regular (at least annual) assessments and audits of organisational compliance with legislation and regulation on processing personal information	
GDPR Awareness/ongoing compliance • Make sure your organisation and key people are aware of the changes in data protection legislation and the impact on the processing of personal information. • Develop and implement an action plan to ensure ongoing GDPR compliance	

Organisation Name: Bristol City Council

Contact details: 0117 9037856

Signatory Name & Job Role: Terry Dafter, Director of Adult Social Services

Date: 20 September 2018

Signature: 

Appendix 1: Second level protocol

INFORMATION SHARING: SECOND LEVEL PROTOCOL FOR

BETWEEN…

		AND:	**AND:**
Name			
Address			

Purpose for the sharing Agreed purposes for the use of information and a process for agreeing further purposes if necessary	To identify and provide missing NHS numbers.
Roles of Partners Definition of who is the controller/processor	Bristol City Council and NHS
Legal Basis The legal basis for sharing information, in relation to the initiative, based on legal justifications for sharing.	Section 47 of the Children Act 1989 (http://www.legislation.gov.uk/ukpga/1989/41/section/47) Section 22 of the Children Act 1989 (http://www.legislation.gov.uk/ukpga/1989/41/section/22)
Data Description Who are the Data Subjects? What Level of identity will be shared? What fields of data will be shared? What is the source of the data? Will multiple datasets be linked?	LCS ID; Date of Birth; Name; Gender; Address
Date of Sharing When will sharing commence/cease? How frequently will information be shared?	Start 22/11/2018 Periodically if NHS number need identifying.
Transparency and Rights How individuals will be informed of the sharing and use of data where required? How will individuals' information rights be upheld?	Covered under the Children's Services Privacy Notice
Security - Physical Security - Electronic security (access control, secure transfer, encryption levels)	Data will be transferred using GCSX secure email

QUALITY A commitment to accuracy and completeness of data exchanged, including a process for informing all relevant parties of any inaccuracies identified	Data extracted from LCS will be checked by Bristol City Council
Retention Agreement to the period of retention of data with reference to organisational retention schedules and the longest applicable period, unless there is reason for destruction of copies of data.	Following provision of NHS numbers to Bristol City Council, the data files provided will be destroyed once matching completed
Training Additional/specialist training needs	N/A
Monitoring and Review Who will monitor that the processes above are taking place and are effective? What checks will be made? How often will this agreement be reviewed? Who will ensure that the review takes place?	One off process
Incident Management How will any breaches of principles be reported and managed? What will be the procedure to update this protocol in the light of any findings?	One off process

DATE	
SIGNATURE	
JOB TITLE For and on behalf of: **ORGANISATION**	
DATE	
SIGNATURE	
JOB TITLE For and on behalf of: **ORGANISATION**	

Copy to SCW Information Governance Team scwcsu.westig-enquiries@nhs.net