TOLSON CARE PARTNERSHIP
INTER-AGENCY INFORMATION SHARING PROTOCOL

DOCUMENT CONTROL

Author	**Information Sharing Protocol Review Group**
Contributors	**All signatory agencies**
Version	**Version 16**
Date of Production	**April 2018**
Date due for revision	**November 2019**
Post responsible for revision	**Information Sharing Protocol Review Group**
Primary Circulation list	**All Signatory Organisations**
Number of document	**N/A**
Restrictions	**None**

Contents Page

INTER-AGENCY INFORMATION SHARING PROTOCOL

1. Purpose of the Protocol

Local organisations are increasingly working together. To work together effectively organisations need to be able to share data about the services they provide and the people they provide these services to.

This protocol covers the sharing of person-identifiable confidential data, with the individual's express consent, unless a legal or statutory requirement applies for the following purposes:

- Provision of appropriate care services
- Improving the health of the population
- Protecting people and communities
- Supporting people in need
- Supporting legal and statutory requirements
- Managing and planning services (where data has been suitably anonymised)
- Commissioning and contracting services (where data has been suitably anonymised)
- Developing inter-agency strategies
- Performance management and audit
- Research (subject to the Research Governance Framework)
- Investigating serious incidents or Inter Agency complaints
- Reducing risk to individuals, service providers and the public as a whole
- Clinical Audit
- Monitoring and protecting public health
- Common Assessment Framework
- Staff management and protection
- In the interests of National Security
- The prevention of disorder or crime
- To fulfil requirements within the Data Security and protection Toolkit (DSPT)
- To fulfil responsibilities in law such as- Data Protection Legislation (GDPR/DPA 2018) in May 2018, Human Rights Act (1998), Common Law, Crime and Disorder Act (1998), Mental Health Act (1983), Fertilisation and Embryology Act (1990), NHS (Venereal Diseases) 1974 Regulations and the Children Act (2004).

This is not intended to be an exhaustive list. If, as a result of policy changes or other developments, additional data sharing requirements arise these will be added to the protocol.

This protocol does not give carte blanche licence for the wholesale sharing of data.

Data sharing must take place within the constraints of the law and relevant guidance and service specific requirements.

This protocol will be underpinned by service specific operational agreements that are designed to meet the specific data sharing needs of that service.

The purpose of this protocol is:

- To provide the basis for an agreement between both local organisations and other associated organisations, to facilitate and govern the effective and efficient sharing of data. Such data sharing is necessary to ensure that individuals, and the population as a whole, can and do receive the care, protection and support they may require.

- To identify the purposes for which data may be shared. This document is supported by local operational policies and procedures within each organisation that underpin the secure and confidential sharing of such data

- To promote and establish a consistent approach between the organisations to the development and implementation of data sharing agreements and procedures.

A further purpose of the protocol is to establish arrangements for the sharing of large datasets between organisations. Following, the recent publication by the ICO of the Data Sharing Checklists and the Data Sharing Code of Practice
https://ico.org.uk/
and as part of the Service Transformation Plans, a cross-government programme has been established with the aim of overcoming barriers to data sharing within the public sector.

In delivering the Interagency Information Sharing Protocol, the focus and challenges are in the effective, timely and secure data sharing with trusted partners. Appropriate district wide governance structures need to be in place to consider and apply the recommendations from Dame Fiona Caldicott's independent review of how information about individuals is shared across the health and care system published on 26th April 2013.

Caldicott Report 1997 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1769982/
And the Caldicott 2 Review 2013 - https://www.gov.uk/government/publications/the-information-governance-review

Please see Appendix 1 "Summary of Key Legislation and Guidance" for further detail

The key areas where data sharing could be beneficial include:

1. Sharing for the purposes of law enforcement and public protection

2. Sharing to provide or improve services in the public, private and voluntary sectors

3. Sharing to facilitate statistical analysis and research.

Consent to share should be sought through agreements at the point of data collections. Data-sharing practices and schemes should be published and maintained as required under the Freedom of Information Act. Organisations should publish and regularly update a list of those organisations with which they share and exchange personal data.

A Data Sharing Agreement would cover the purposes, accountability, restrictions imposed and secure transfer arrangements where data has been shared and each occasion of data sharing of this type will need its own Data Sharing Agreement.

Requests to share datasets must relate to one or more of the three key areas identified above and should contain only demographic details, such as a geographical reference, age, gender and possible ethnicity data.

As such this document:

- **Informs** about the reasons why data may need to be shared and how this sharing will be managed and controlled by the organisations concerned.

- **Identifies the local organisations** that are party to this protocol.

- **Sets out the principles** that underpin the exchange of data between organisations.

- **Defines the purposes** for which organisations have agreed to share data.

- **Describes the policies and procedures** that support the sharing of data between organisations and will ensure that such sharing is in line with legal, statutory and common law responsibilities.

- **Promotes a standard approach** to the development of data sharing agreements and procedures.

- **Sets out the process** for the implementation, monitoring and review of the protocol.

2. Background

2.1 Legislative context and national guidance documentation

All organisations are subject to a variety of legal, statutory and other guidance in relation to the sharing of person- identifiable or anonymised data.

For all organisations the key legislation and guidance affecting the sharing and disclosure of data includes (but is not necessarily an exhaustive list): -

Legislation:

- Access to Health Records 1990
- The Children Act 2004
- Civil Contingencies Act 2004
- Common Law Duty of Confidentiality
- Crime and Disorder Act 1998
- Criminal Justice Act 2003
- Criminal Procedures and Investigations Act 1996
- Data Protection Legislation (GDPR/DPA 2018)Education Act 2002
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- Homelessness Act 2002
- Human Rights Act 1998
- Local Government Act 2000
- Mental Capacity Act 2005
- Mental Health Act 1983
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006

Appendix II provides summary details of some of the above-mentioned, and related, legislation and guidance.

2.2 Local Context

All organisations face similar requirements with regards to the development of data sharing agreements with their local partners. While the requirements remain similar the number of partners with which an organisation must have such agreements differs. This number is dependent on the geographical area covered by an organisation and the nature of its work.

This protocol is a recognition that consistent data sharing agreements now need to exist across boundaries.

The intention of this protocol is to support and build on existing agreements in order to provide a common process for the development and implementation of future data sharing agreements across the patch.

The protocol is aimed at the data sharing agreements required between organisations and provides a framework within which organisations can share data.

3. Principles guiding the sharing of information

The following key principles guide the sharing of data between the organisations:

3.1 Organisations endorse, support and promote the accurate, timely, secure and confidential sharing of both person identifiable and anonymised data where such data sharing is essential for the provision of effective and efficient services to the local population.

3.2 Organisations are fully committed to ensuring that if they share data it is in accordance with their legal, statutory and common law duties, and, that it meets the requirements of any additional guidance.

3.3 All organisations must have in place policies and procedures to meet the national requirements for Data Protection, Data Security and Confidentiality - https://ico.org.uk/for-organisations/guide-to-data-protection/ . The existence of, and adherence to, such policies provides all organisations with confidence that data shared will be transferred, received, used, held and disposed of appropriately.

3.4 Organisations acknowledge their 'Duty of Confidentiality' to the people they serve. In requesting release and disclosure of data from other organisations employees and contracted volunteers will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that data is not disclosed illegally or inappropriately. This responsibility also extends to third party disclosures; any proposed subsequent re-use of data which is sourced from another organisation should be approved by the source organisation.

3.5 An individual's personal data must be complete and up to date and will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary. For all other purposes data should be anonymised. ICO Anonymisation Code of Practice - https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

3.6 Where it is agreed that the sharing of data is necessary, only that which is needed, relevant and appropriate will be shared and that would only be on a "need to know" basis.

3.7 When disclosing data about individual, organisations will clearly state whether the data being supplied is fact, opinion, or a combination of the two.

3.8 There will be occasions when it is legal and necessary for organisations to request that data supplied by them be kept confidential from the person concerned. Decisions of this kind will only be taken on statutory grounds and must be linked to a detrimental effect on the physical or mental wellbeing of that individual or other parties involved with that individual. The outcome of such requests and the reasons for taking such decision will be recorded.

3.9 Careful consideration will be given to the disclosure of data concerning a deceased person, and if necessary, further advice should be sought before such data is released.

3.10 All staff will be made aware that disclosure of personal data, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action.

3.11 Organisations are responsible for putting into place effective procedures to address complaints relating to the disclosure of data, and information about these procedures should be made available to service users.

4. Consent

4.1 Data is provided in confidence when it appears reasonable to assume that the provider of the data believed that this would be the case, or where a person receiving the data knows, or ought to know, that the data is being given in confidence. It is generally accepted that most (if not all) data provided by service users is confidential in nature. All organisations, which are party to this protocol accept the duty of confidentiality and will not disclose such data without the consent of the person concerned, unless there are statutory grounds or an overriding justification for doing so. In requesting release and disclosure of information from members of partner organisations, staff in all organisations will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that data is not disclosed illegally or inappropriately, this includes third party disclosures.

4.2 Organisations are fully committed to ensuring that they share data in accordance with their statutory duties. They are required to put in place procedures that will ensure that the principles of the Data Protection Legislation (GDPR/DPA 2018) and requirements of other relevant legislation are adhered to and underpin the sharing of data between their organisations.

4.3 As is required by the fair processing requirements of the Data Protection Legislation (GDPR/DPA 2018) individuals in contact with organisations will be fully informed about data that is to be obtained, held or disclosed about them. The individual has the right to request that processing of their data cease. .

4.4 As a **minimum**, individuals will be informed that data may be shared and the circumstances in which this could happen unless this poses a risk of harm or danger. Fair processing notices should always be in place. Consent can often be inferred from the circumstances in which data was given. However, it is always important that the person giving consent understands who will see their data and the purpose to which it will be put. If there is any doubt as to whether a disclosure is supported by a legal, statutory requirement or an immediate serious risk explicit consent should be sought. Where an organisation has consent forms the service user should be

requested to sign one. Consent can be given verbally and should be recorded and managed correctly. That it should be a positive opt in and that the methods to withdraw to consent should be given at the time consent was given. Consent should be as easy to withdraw as it was to give. Data Controllers can evidence how they comply with this

4.5 The individual's right to confidentiality are not absolute and may be overridden if evidence that disclosure for specific purposes is necessary in exceptional circumstances. Such as;

- Where it is required by statute
- Where not to share the data poses a public health risk
- Where there is a risk of harm to any person
- Where sharing is required to prevent serious crime. (This is not an exhaustive list)
    - *Treason*
    - *Murder*
    - *Manslaughter*
    - *Rape*
    - *Acts of Terror*
    - *Kidnapping*
    - *Indecent assault constituting gross indecency*
    - *Causing an explosion likely to endanger life or property*
    - *Certain offences under the Firearms Act 1968*
    - *Causing death by dangerous driving*
    - *Hostage taking*
    - *Torture*
    - *Many drug-related offences*
    - *Ship hijacking and Channel Tunnel train hijacking*
    - *Taking indecent photographs of children*
    - *Publication of obscene matter etc.*

Where the individual chooses to exercise their right not to provide express consent for data sharing, they must be advised of any constraints that this will put upon the service that can be provided, however the individuals wishes must be respected unless there is a statutory requirement or a significant risk of harm to an individual to override those wishes as indicated above.

4.6 Where the individual is unable to provide express consent due to incapacity, the professional concerned must take decisions about the use of data. This must take into consideration the individual's best interests and any previously expressed wishes, or the wishes of anyone who is authorised to act on behalf of the individual. Data must only be disclosed that is in the individuals best interest, and only as much data as is needed to support their care.

4.7 Where the individual to whom the data relates is a child, (under the age of 13), and it is determined that the individual has the competency to make decisions regarding the sharing of data they have provided in confidence, their wishes must be respected. Except in cases where the child has suffered, or is suffering abuse or neglect, when there is a legal duty to share data with Children's Social Care (CSC) and/or the Police. In other cases where the individual does not have the capacity to consent, express consent must be sought from the individual with parental responsibility (parent or guardian).

Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidentiality as adults

4.8 Safeguarding Children and Adults

Principles

- Safeguarding children and adults is everyone's responsibility
- Abuse and neglect of children and adults is never acceptable
- Sharing data is crucial to protecting the child (even when the child or young person does not agree) and vulnerable adults
- Failure to share appropriate data places children and adults at greater risk

Where the safety or welfare of a child is in doubt, staff must share data with the statutory agencies which can provide protection (Children's Social Care and Police). This is irrespective of whether the child and/or their parents or carers have given permission for the data to be shared. This is a legal duty under the Children Act 2004. Failure to share relevant data places a child in danger, and leaves the staff vulnerable to both professional misconduct and disciplinary consequences.

All Adults and young people over the age of 16 are assumed to have capacity to consent unless it is proven otherwise (Mental Capacity Act 2005).

- A person who lacks capacity at a certain time may be able to make that decision at a later date. Consideration should be given to whether the data needs to be shared now, or could wait until a time when the person is able to consent to the data being shared.
- The 5 Key Principles in the Mental Capacity Act should be taken into account in coming to a decision about a person's capacity.
- Where it is considered that a person does not have capacity, a record should be made of this decision and the steps taken by the professional to reach a decision about whether data should be shared

The capacity to be able to give consent can be assessed by considering:

- has the person got the capacity to make this particular decision,
- have they got the capacity to understand and retain the information relevant to the decision,
- will they be able to understand the reasonably foreseeable consequences of deciding one way or the other,
- will they have the capacity to communicate the decision they have come to

4.9 Where professionals request that data supplied by them be kept confidential from the people who use services the outcome of this request and the reasons for taking the decision will be recorded. Decisions of this kind will only be taken on statutory grounds.

4.10 Emergency Planning and Response

In the event of the need to respond to an emergency involving any or all organisations, it is recognised that organisations may need to share sensitive personal data to respond to the emergency situation, where explicit consent has not been given, and where the emergency circumstances are incompatible with the initial purposes for which the personal data was originally collected.
As is the case for sharing personal data about children to prevent or detect a serious crime, it may be entirely proportionate for local and regional emergency responders to share personal data to save life or prevent the possibility of serious harm.

The absence of data sharing agreements should not prevent organisations from sharing data when responding to an actual emergency, and agencies take on board the lessons identified in previous Government reports relating to data sharing at the time of emergency response: *"There has been a culture of risk averseness among senior decision-makers or information managers in the emergency community surrounding data protection issues."*

The Data Protection and Sharing Guidance for Emergency Planners and Responders - https://www.gov.uk/government/publications/data-protection-and-sharing-guidance-for-emergency-planners-and-responders gives more detail and guidance to assist regional emergency planners and responders in decision making about sharing information in the event of a large-scale emergency

5. Supporting Policies, Procedures and Guidance

5.1 Supporting policies

For members of the public and staff from different organisations to have confidence that data sharing takes place legally, securely and within relevant guidance all organisations have in place policies which meet the requirements for:

- Data Protection
- Confidentiality
- Information Security

These policies must cover manual, verbal and computer-based data.
Processes must be in place within organisations to regularly monitor and improve the effectiveness of these policies.

5.2 Access and Security Procedures

All organisations will look to implementing secure solutions to support the safe transfer of data. Risk assessments will be carried out before the transfer of data is carried out and all reasonable steps to mitigate any risks identified will be taken Supporting documentation relating to the secure transfer, receipt, access to, storage and disposal of shared data should be made available to staff.

Each organisation will keep a log of all requests for data sharing received.

Each organisation will instigate a system of reporting back to the originator of data where actions have been taken on the basis of the data shared.

Organisations should put into place policies, procedures or guidelines covering:

- Communication by fax
- Communication by phone
- Electronic communication
- Verbal communication
- Written communication
- Use of personal data for purposes other than that agreed
- Access arrangements to shared records and databases
- Secure storage and disposal of confidential data

These policies, procedures or guidelines should be subject to regular monitoring and all organisations, as data controllers, should evidence that they have checked that their data shared with 3rd party data processors is being kept and processed correctly.

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. The Information Commissioner has the statutory power to impose a financial penalty on an organisation if satisfied that there has been a serious breach of one or more of the Data Protection principles and the breach was likely to cause substantial damage or distress. There are two levels of fines. The first is up to €10 million or 2% of the company's annual turnover of the previous financial year which ever is the higher. The second is up to €20 Million or 4% of the company's global annual turnover for the previous financial year whichever is the higher.

5.3 Data security and protection Toolkit

The Data security and protection Toolkit (DSPT) is an online tool that enables organisations to measure their performance against the information governance requirements.

1. To provide organisations with a means of self- assessing performance against key aspects of information governance, the toolkit contains a set of six initiatives or work areas as described below.

    - Information Governance Management
    - Confidentiality and Data Protection Assurance
    - Information Security Assurance
    - Clinical Information Assurance
    - Secondary Uses Assurance
    - Corporate Information Assurance

Within: General Practices, Commercial Third Parties, NHS Business Partners, Social Care Organisations, Pharmacies and all other NHS Organisations.

Note: V15 of the DSP Toolkit is very different in look, content and requirement and is expected to be released in June 2018

5.4 Induction and continuing education

To support the implementation of the above-mentioned policies and procedures appropriate staff induction, training programmes and awareness raising sessions are mandatory for all staff within the organisation. All training must include all aspects of Data protection, information security and safe data transfers.

5.5 Data Quality

Shared data needs to be of sufficient quality for its intended purpose; this is an essential requirement to all data users and underpins the timely and effective delivery of services to those in need. Several characteristics of good data quality have been identified and in summary they are:

Accuracy – Data should be accurate so as to present a fair picture of circumstances and enable informed decision-making at all appropriate levels. Definitions for data should be specific and unambiguous.

Validity – Data should represent clearly and appropriately the intended result and should be used in accordance with the correct application of any rules or definitions.

Reliability – Data should reflect stable and consistent data collection processes that need to be fit for purpose and incorporate controls and verification procedures.

Timeliness – Data input should occur on a regular ongoing basis rather than being stored to be input later. Verification procedures should be as close to the point of input as possible. Data must not be retained for longer than is necessary.

Relevance – Data collected should comprise the specific items of interest only. Sometimes definitions need to be modified to reflect changing circumstances in services and practices, to ensure that only relevant data of value to users is collected, analysed and used.

Completeness – All the relevant data must be recorded. Missing or invalid data can lead to incorrect judgement and poor decision-making.

6. Approval, implementation and review

6.1 Agreeing the protocol

This Protocol proposes a consistent approach to the development of data sharing agreements. Appendix III provides outline of the formal agreement format.

6.2 Implementation -Following approval of the protocol organisations will need to take action, either individually or jointly, on the following issues:

Organisation	Actions
All organisations	• Promoting ownership of responsibilities associated with the protocol • Ensuring dissemination and appropriate implementation • Reviewing existing support policies, procedures and guidance. • Agreeing training and awareness programmes • Auditing and monitoring the implementation and compliance of existing agreements • Establishing review processes • Joint work to develop standard service specific agreements • Ensuring amendments to existing agreements • Agreeing audit processes • Maintaining local registers of agreements.
Chief Officers/Boards of each organisation or department/Caldicott Guardians	• Reviewed every 3 years

6.3 Monitoring and review processes

Where not already in place, processes will be set up in each agency to adopt a risk management approach to breaches/problems in relation to the implementation of this agreement. Formal review of the protocol should be held at three yearly intervals unless legislative changes require immediate action.

Prior to the review date, agencies should submit feedback on the use of the protocol and propose options for addressing problems or amending procedures.

It is proposed that reviews would, in the first instance, be co-ordinated through the Data Sharing Protocol Review Group.

7. Conclusion

All organisations are in the position of having to balance the conflicting demands of the need and requirement to share information with other organisations with the responsibility to maintain the highest level of confidentiality.

This protocol acknowledges these competing demands and provides a means whereby members of the public, staff and the agencies can be confident that where data is shared it is done so appropriately and securely

Appendix 1 - Glossary of Terms

Agency - A business or organisation providing a particular service on behalf of another business, person or group

Anonymised Data - This is data which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.

Caldicott Guardian - A Caldicott Guardian is a senior person in the NHS responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

Data - Within this Protocol data could include personal and/or special category data

Data Controller - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

Data Processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller

Data Protection Officer - A designated person within an organisation who is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements and other Data Protection Laws.

Data Recipient - in relation to personal data, means any person to whom the data are disclosed

Data Source – The source the data was originally obtained from

Data Subject - means an individual who is the subject of personal data

Disclosure - The divulging or provision of access to data.

Explicit Consent - This means articulated agreement and relates to a clear and voluntary indication of preference of choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

Implied Consent - This means agreement that has been signalled by the behaviour of an individual with whom a discussion has been held about the issues and therefore understands the implications of the disclosure of data.

Information Commissioner - The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals https://ico.org.uk

Data Security and protection Toolkit
Is an online system which allows NHS and Social Care organisations and partners to assess themselves against Department of Health Information Governance policies and standards. It also allows members of the public to view participating organisations' DSP Toolkit assessments.

Information Sharing Protocol - Is the high level document setting out the general reasons and principles for sharing data. The protocol will show that all signatory organisations are committed to maintaining agreed standards on handling data and will publish a list of senior signatories. It should be underpinned by data sharing agreements between the organisations who are actually sharing the data.

Information Sharing Agreement - Is a more detailed document the intention of which is to spell out how the organisations involved will operate the approach to data sharing. Agreements will be produced where organisations specifically identify a purpose to share data across organisational boundaries. The agreement should state whether partners are obliged to, or are merely enabled to, share data.

Organisations - Used in the context of this document to relate to the organisations specified within appendix IV which details the organisations that are signatories to this protocol.

Special Category Personal Data – A full description is available at the ICO's web site - https://ico.org.uk/for-organisations/guide-to-data-protection**Pseudonymisation** - "Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified

Senior Information Risk Owner (SIRO) – Is an NHS Senior Management Board Member who will take overall ownership of the Organisation's Information Risk Policy and act as champion for information risk on the Board.

APPENDIX II

SUMMARY OF KEY LEGISLATION AND GUIDANCE

(Detailed guidance should be available in all agencies for staff)

Access to Health Records Act 1990 - http://www.legislation.gov.uk/ukpga/1990/23/contents

This Act provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements. The Data Protection Act 2017 supersedes the Access to Health Records Act 1990 apart from the sections dealing with access to information about the deceased

Data Protection Legislation (GDPR/DPA 2018)- https://ico.org.uk/ -

The key legislation governing the protection and use of identifiable patient/client data (Personal Data) is the Data Protection Legislation (GDPR/DPA 2018). The Act does not apply to data relating to the deceased.

The Act stipulates that anyone processing personal data comply with eight principles of good practice. These principles are legally enforceable.

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) 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;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) 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;
e) 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
f) 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."

Detailed information for staff about the requirements of the Act in relation to information sharing is available in each organisation.

Crime and Disorder Act 1998 - http://www.legislation.gov.uk/ukpga/1998/37/contents

The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area. Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power but only where it is necessary and expedient for the purposes of the Act. However, whilst all organisations have the power to disclose, Section 115 does not

impose a requirement on them to exchange information and responsibility for the disclosure remains with the organisation that holds the data. It should be noted, however, that this does not exempt the provider from the requirements of the 2nd Data Protection principle.

Human Rights Act 1998 - http://www.legislation.gov.uk/ukpga/1998/42/contents

Article 8.1 of the Human Rights Act 1998 provides that "everyone has the right to respect for his private and family life, his home and his correspondence". This is however, a qualified right i.e., there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights and Article 8.2 provides "there shall be no interference by a public authority with the exercise of this right as it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others".

The Act also requires public bodies to read and give effect to other legislation in a way that is compatible with these rights and makes it unlawful to act incompatibly with them. As a result these rights still need to be considered, even when there are special statutory powers to share information.

Common Law duty of Confidentiality -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

All staff working in both the public and private sector are aware that they are subject to a common law Duty of Confidentiality and must abide by this. The duty of confidence only applies to identifiable information and not to aggregate data derived from such information or to information that has otherwise been effectively anonymised i.e., it is not possible for anyone to link the information to a specified individual.

The Duty of Confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g., to protect others from harm). Whilst it is not entirely clear under law whether or not a common law Duty of Confidence extends to the deceased, the Department of Health and professional bodies responsible for setting ethical standards for health professionals accept that this is the case.

All organisations are subject to their own codes or standards relating to confidentiality.

Caldicott Report 1997 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1769982/
and the Caldicott 2 Review 2013 - https://www.gov.uk/government/publications/the-information-governance-review

In December 2011 the Government announced that it wanted to allow patients' records and other NHS data to be shared with private life science companies, to make it easier for them to develop and test new drugs and treatments. Concerns were raised about what that might mean for patient confidentiality. This and other issues prompted the instigation of Caldicott 2, in which Dame Fiona was asked to review information issues across the health and social care system.

Dame Fiona first investigated issues surrounding confidentiality when she chaired a similar review in 1996-7 on the use of patient data in the NHS. That review recommended that the NHS adopt six principles (see below) for the protection of confidentiality, which became known as the

"Caldicott principles". The review also recommended that NHS organisations appoint someone to take responsibility for ensuring the security of confidential information. These people became known as "Caldicott Guardians".

The reach of Caldicott 2 is far wider than the 1997 report. Its recommendations affect all organisations working in the health and social care sector – including local authorities. Its recommendations, if adopted, will have a significant impact on the way that local authorities operate.

1. **Justify the purpose(s) for using confidential information**

2. **Only transfer/use patient-identifiable information when absolutely necessary**
3. **Use the minimum identifiable information that is required**

4. **Access should be on a strict need to know basis**

5. **Everyone with access to identifiable information must understand his or her responsibilities**

6. **Understand and comply with the law**

7. **The duty to share personal confidential data can be as important as the duty to respect service user confidentiality.**

Only the NHS and Social Care are required to apply these principles and to nominate a senior person to act as a **Caldicott Guardian** responsible for safeguarding the confidentiality of patient information.

Freedom of Information Act 2000 - https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

This Act provides clear statutory rights for those requesting information together with a strong enforcement regime. Under the terms of the Act, any member of the public will be able to apply for access to information held by bodies across the public sector. The release of personal information remains protected by the Data Protection Legislation (GDPR/DPA 2018).

The Children Act 2004 - http://www.legislation.gov.uk/ukpga/2004/31/contents

The Act provides a legislative spine for the wider strategy to improve children's lives. This covers the universal services which every child accesses, and more targeted services for those with additional needs. The overall aim is to encourage integrated planning, commissioning and delivery of services as well as improve multi-disciplinary working, remove duplication and increase accountability. There is a duty to cooperate between relevant partners in the making of arrangements to improve the wellbeing of children.

Data Protection Bill

https://ico.org.uk/for-organisations/data-protection-bill/

Data Protection Legislation (GDPR/DPA 2018)
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Health and Social Care Act 2012 -
http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted

The Health and Social Care Act 2012 underpins wide ranging reforms of the NHS since it was founded in 1948. Changes include the establishment of a National Health Service Commissioning Board and Clinical Commissioning Groups, as well as Health and Wellbeing Boards. The changes became operational on 1st April 2013. The Act sets out provision relating to public health in the United Kingdom; public involvement in health and social care matters; scrutiny of health matters by local authorities and co-operation between local authorities and commissioners of health care services. The Act establishes a National Institute for Health and Care Excellence, and establishes the provision for health and social care.

The clinical commissioning organisations established by the Act must have a secure legal basis for every specific purpose for which they wish to use identifiable patient data. Where there is no such statutory legal basis either the consent of the patient is required to process personal confidential data or the data must be fully pseudonymised.

Care Act 2014 -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/365345/Making_Sure_the_Care_Act_Works_EASY_READ.pdf

This Act incorporates a wide range of provisions relating to adult social care, including Safeguarding and most provisions come into force on 1 April 2014.

The sections with most relevance to information sharing are:

Ss 6&7: Duties to cooperate with other persons in the exercise of functions relating to adults with needs for care and support, and to carers.

S37: Duty to notify receiving LA when an adult receiving care and support moves.

S45: Duty to comply with request for information by Safeguarding Adults Board to enable or assist the SAB to exercise its functions. This could include information about individuals.

S67: Involvement of independent advocate in assessments, plans etc.

Statutory guidance is available on all parts of this Act.

National Data Guardian for Health and Care consultation: Review of Data Security, Consent and Opt-Outs

Both the National Data Guardian Consultation Notice and the Information Commissioners response

https://ico.org.uk/about-the-ico/consultations/national-data-guardian-for-health-and-care-consultation-review-of-data-security-consent-and-opt-outs/

Other relevant legislation

- Civil Contingencies Act 2004
- Criminal Justice Act 2003
- Criminal Procedures and Investigations Act 1996
- Education Act 2002
- Homelessness Act 2002
- Local Government Act 2000
- Mental Capacity Act 2005
- Mental Health Act 1983

- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006

There are statutory restrictions on passing on information linked to:
NHS (Venereal Disease) Regulations 1974
Human Fertilisation and Embryology Act 1990
Abortion Regulations 1991

Further Guidance
HM Government Publications:
Information Sharing: Guidance for practitioners and managers
Information Sharing: Pocket Guide
Available at www.education.gov.uk/publications to download

ICO Publications - Fors a full index of the ICO's data protection and privacy and electronic communications guidance for organisations**- https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/**

Anonymisation
Data Processing
Data Protection
Data Sharing
Notification
Personal Data
Privacy Notices
Security
Subject Access

Appendix III

DATA SHARING AGREEMENT

This agreement is to be used in conjunction with the Inter Agency Information Sharing Protocol and complies with all the guidance therein.

1. Parties to this agreement

Organisations Name	The Whitehouse Centre
Address	Princess Royal Health Centre, Greenhead Rd, Huddersfield HD1 4EW
Responsible Manager	Helen Jones, Assisant Director of Operations, Locala CIC
Contact Details	030 3003 4459
Authorised Signatory (Partner, Caldicott Guardian, etc.)	
Date:	8 July 2019

Organisations Name	Dalton Surgery
Address	364a Wakefield Road, Dalton, Huddersfield, HD5 8DY
Responsible Manager	Dawn Whincup
Contact Details	01484 530068
Authorised Signatory (Partner, Caldicott Guardian, etc.)	Dr S Khokhar
Date:	09/07/2019

Organisations Name	The Waterloo Practice
Address	Wakefield Road, Waterloo, Huddersfield, HD5 9XP
Responsible Manager	Brigid Collinge
Contact Details	01484 505283 brigid.collinge@gp-b85024.nhs.uk
Authorised Signatory (Partner, Caldicott Guardian, etc.)	Dr Farooq Hameed
Date:	4.7.19

Organisations Name	The Junction Surgery
Address	Birkhouse Lane, Moldgreen, Huddersfield, HD5 8BE
Responsible Manager	Julie Sunderland
Contact Details	01484 411827
Authorised Signatory (Partner, Caldicott Guardian, etc.)	Julie Sunderland – Practice Manager
Date:	08.07.19

Organisations Name	Almondbury Surgery
Address	Longcroft, Almondbury, Huddersfield, HD5 8XN
Responsible Manager	Gillian Ellis
Contact Details	01484 514555
Authorised Signatory (Partner, Caldicott Guardian, etc.)	Gillian Ellis
Date:	09.08.2019

Organisations Name	Rose Medical Practice
Address	140 Fitzwilliam Street, Huddersfield, HD1 5PU
Responsible Manager	Sally Oldbury
Contact Details	Sally.oldbury@nhs.net 01484 500921
Authorised Signatory (Partner, Caldicott Guardian, etc.)	 Dr Satpal Singh
Date:	05.07.2019

Organisations Name	Greenhead Family Doctors
Address	15 Wentworth Street, Huddersfield, HD1 5PX
Responsible Manager	Josephine Anderson
Contact Details	01484 530834
Authorised Signatory (Partner, Caldicott Guardian, etc.)	Dr R Edara
Date:	05/07/2019

Organisations Name	The University Health Centre
Address	12 Sand Street, Huddersfield, HD1 3AL
Responsible Manager	Nicola Kelly/Nicola Toner
Contact Details	01484 430386
Authorised Signatory (Partner, Caldicott Guardian, etc.)	Dr J Thomas – GP Partner
Date:	08/07/19

Organisations Name	My Health Huddersfield GP Federation
Address	Oaklands Health Centre, Huddersfield Road, Holmfirth, HD9 3TP
Responsible Manager	Claire Sibbald – Business Development Manager
Contact Details	01484 689111 ext 1216 Claire.sibbald@myhealthhuddersfield.co.uk
Authorised Signatory (Partner, Caldicott Guardian, etc.)	Claire Sibbald
Date:	23/07/19

Date of Agreement	09 August 2019

2. Specific purpose(s) for which the data sharing is required (all intended purposes should be described, it may be appropriate to describe each one on a separate pro forma)

To provide Extended Hours clinical services in order to deliver the requirements of the NHS England commissioned Primary Care Networks contract DES

3. Type and status of data shared

Is the data 'person identifiable'?	**Yes**
Has explicit consent been given and recorded?	**Yes**
Has implied consent been recorded?	**Yes**
Is the subject aware that sharing will take place?	**Yes**
Is the data anonymised?	**No**

4. Legal basis for sharing where no consent is given

Where the patient is at risk from harm

5. Data Items shared

This list must be comprehensive and include ALL data items that are to be shared. All data items to be shared must be justifiable as necessary for the purpose. The service user/staff member should be aware that the information will be shared and have consented to it. For the purpose of delivering care implied consent is sufficient. You should tailor this section to suit your organisations specific needs.

Service User Data	**Yes/No**	**Comment**
Name, address, Date of Birth, Gender, GP	**Yes**	**Recorded as standard so clinician can identify patient**
Identifying numbers (NHS No. etc.)	**Yes**	**Standard element of record**
Next of Kin, Emergency Contact, Carer Details	**Only if recorded within record, may not be included**	
Clinical Details (Clinical details should only be shared where there is a justifiable purpose)	**Yes**	**Clinicians will require access to information in order to provide appropriate advice/prescribing**
Basic Clinical Details (Condition and relevant care requirements)	**Yes**	
Full Clinical Details (May include medical history, test results, clinical letters, reports etc.)	**Yes**	**May be relevant to reason appointment required and will ensure appropriate advice/prescribing**
Other (Should only be shared where there is a justifiable purpose)	**Yes**	**Only if applicable to consultation**
Risk Factors		
Other (Please Explain)		
Staff Information	**Yes/No**	**Comment**
Name, Job Title, Work Base, Work Team, Line Manager	**No**	**N/A**
Identifiers Such As Payroll No. NI Number	**No**	**N/A**
Home Address, Date of Birth and Next of Kin	**No**	**N/A**

Full Employment Record	**No**	**N/A**

6. Protective Marking

Is Protective marking/Classification relevant to this information?	**No**
If yes please use the system relevant to your Organisation	

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

7. Data Transfer Method

All parties to this agreement are responsible for ensuring that appropriate security and confidentiality procedures are in place to protect the transfer, storage and use of the shared, person identifiable data.

Regular flow (specify frequency)	**Data will be shared via SystmOne and so will remain within clinical record**
Ad hoc	

More than 21 items per flow	
Less than 21 items per flow	

Give full details of how the transfer will be made and what security measures will be in place e.g. encryption, business secure mail or recorded signed for etc.

Face to face	
Telephone	
Safe haven fax (or faxed following procedure)	
Electronically (state method)	
Secure E Mail	**If additional information is required to support a complaint/patient query this will be requested and transferred via person specific NHS net email.**
Secure Mail	
Secure Courier	
Encrypted Removable Media	
Other	

Has a risk assessment been carried out on the chosen methods of transfer?	**No – standard process for sharing of patient data with Health Care organisations. Already in place in GP practices and Local Care Direct**

What are the identified risks?	

8. Audit and Review

Organisations Name	
Address	
Responsible Manager	
Contact number	
Review Date	

INCIDENTS
Any incidents occurring as a result of this agreement should be reported to the signatories of all affected organisations. They will then pass on the information in accordance with incident reporting procedures within their own organisation if appropriate. Organisations will agree to share information in order to help investigate any such incidents

9.

Subject Access Requests Will Be Directed To	The Practice Manager
Special Arrangements For Subject Access Requests	

10.

Retention Period For Data	
Disposal Method For Data	

APPENDIX IV

INTER-AGENCY INFORMATION SHARING PROTOCOL

MEMORANDUM OF AGREEMENT

The signatory organisations to this agreement endorse the vital importance of the sharing of data between the organisations to support the provision of effective and efficient services to the populations of the local area.

The signatory organisations are committed to working in partnership on this and future data sharing activities and recognise that without such sharing the increasing amount of initiatives requiring a multi-agency approach cannot be fully achieved.

The signatory organisations accept and support the principles and processes identified in the Inter-Agency Information Sharing Protocol.

The signatory organisations are committed to ensuring that their organisations have in place the appropriate policies, procedures and training to maintain the security and confidentiality of shared data.

The signatory organisations are committed to the monitoring and review of the data sharing processes arising from this protocol.

The signatory should be the Caldicott Guardian, SIRO, Chief Executive or a Director of the organisation.

INTER-AGENCY INFORMATION SHARING PROTOCOL

I …….. (Name of signatory)

On behalf of …….. (Name of organisation)

Hereby agree to the following:

- To subscribe to the principles contained within the Protocol
- To work to the principles contained within the Protocol
- To ensure that the Protocol is fully implemented within the organisation/authority and all relevant staff are trained in the principles and legal requirements
- To contribute to the development of trust between the signatory organisations by working within the framework of the Protocol

Signature …….. Name …….

Position …… Date ……..
(Chief Executive, SIRO, Caldicott Guardian, Director etc.)

Please complete and sign this page and return by email or post to,
Kathryn.wise@this.nhs.uk
Kathryn Wise Information Governance Officer, THIS, Oak House, Woodvale Office Park, Woodvale Road, Brighouse, HD6 4AB

Appendix V

Signatories as at July 2019

The Whitehouse Centre
Dalton Surgery
The Junction Surgery
Rose Medical Practice
The Waterloo Practice
Almondbury Surgery
Greenhead Family Doctors
The University Health Centre
My Health Huddersfield GP Federation