Herefordshire Council

NHS
Herefordshire
Clinical Commissioning Group

West Mercia POLICE

NHS
Herefordshire and Worcestershire
Health and Care
NHS Trust

Wye Valley NHS
NHS Trust

Hoople
innovation in business

National Probation Service

HEREFORD & WORCESTER
HWFR
FIRE AND RESCUE SERVICE

TURNING POINT
inspired by possibility
www.turning-point.co.uk

# HEREFORDSHIRE and WORCESTERSHIRE

# INFORMATION SHARING PROTOCOL

| | |
|---|---|
| *Date issued* | |
| *Version* | **3.1** |
| *Last revised* | **January 2023** |
| *Category* | **Information Assurance** |
| *Owners* | **Data Protection Officers / Information Governance Leads** |
| *Target audience* | **All staff** |

## Document Control

This is a CONTROLLED document and updates or changes to this document are authorized and then advised by email to the relevant document holders.

It is UNCONTROLLED when printed. You should verify that you have the most current issue.

### Author(s)

| Names | Role |
|---|---|
| Helen Worth | Information Governance Manager |

### Document Log

| Version | Status | Date Issued | Description of Change | Pages affected |
|---|---|---|---|---|
| V0.01 | Draft | 30/12/2009 | - | Newly created document |
| V1.0 | Final | 28/05/10 | Final, agreed by CEO of HHT, HC and NHSH | |
| V1.01 | 2nd Draft | | Updated to reflect organisational changes | All |
| V2 | Final | 28/01/15 | Reviewed by Herefordshire Council Legal Services | |
| V2.01 | Draft | 02/01/18 | Review and update to reflect new data protection legislation | |
| V3 | Final | 20/04/22 | Updated to include new providers | |
| V3.1 | Final | 01/02/23 | Reviewed for updates and to include Worcestershire SAB and providers | 2, 3, 9 |

# Contents

## 1 Memorandum of Understanding and Signatories

The partner organisations agree to:

- Appoint lead officers, such as their Caldicott Guardian, Safeguarding Lead or Data Protection Officer, to ensure compliance with the terms of the Herefordshire and Worcestershire Information Sharing Protocol and all associated agreements and procedures, together with the law, whilst adhering to best established practice.

- Review requirements for staff training, and ensuring the provision of adequate training to all their employees to ensure that employees are aware of their duties with regard to the sharing of information.

- Map the flow of information that is being shared and ensuring that confidentiality safeguards are implemented at each stage of the movement of that information, including use of safe havens. A safe haven refers to both a physical location and to an agreed set of administrative arrangements to ensure the safety and secure handling of confidential person identifiable information.

- Ensure that relevant standards of information security, data quality and records management are met.

- Implement adequate arrangements to test compliance with the Herefordshire and Worcestershire Information Sharing Protocol.

- Ensure that material is made available to members of the public explaining their rights under information legislation; how records of their personal data will be recorded and stored; who will see these records; the circumstances under which personal information may be shared with or without consent and the choices they have to limit sharing; the procedures for accessing their records; and the complaints procedure. This material must be made available in another language or format such as Braille or large print on request.

…….

Herefordshire Council

…….

Wye Valley NHS Trust

…….

CCG

…….

Herefordshire and Worcestershire Health Care Trust

……

West Mercia Police

……

National Probation Service

……

Turning Point

……

Youth Offending Service

……

Hereford & Worcester Fire and Rescue Service

…….

Hoople

## 2 Introduction

This document is an information sharing protocol (for the purpose of this protocol, the terms data and information are synonymous). The aim of this document is to facilitate sharing of information between the public, private and voluntary sectors so that members of the public receive the services they need whilst maintaining their confidentiality.

Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected. The balance between the need to share information to provide a quality service and protection of confidentiality is often difficult to achieve.

The legal situation regarding the protection and use of personal information can be complex. In these situations this type of information may not be readily available to those who have a genuine need to know, which could obstruct their ability to undertake their duties. See the accompanying document Information Sharing – Relevant Legislation Guidance for further information.

## 3 Purpose

This is an overarching protocol that provides a framework which must be followed when sharing information. Data exchange agreements must be agreed by the Caldicott Guardian, Safeguarding Lead, Data Protection Officer or person responsible for data protection matters for the provider and recipient organisations who are party to the Agreement.

**In all circumstances having a protocol and a data exchange agreement in place does not in itself make the sharing of personal and sensitive personal information lawful, a legal basis for that sharing must be identified prior to the sharing taking place.**

## 4 Scope

The protocol applies to the following information:

- All personal information processed by the organisations including electronically (e.g. computer systems, CCTV [only systems which fall within the scope of the Data Controller], audio etc.), or in manual records.
- All information relating to deceased patients including that processed electronically, or in manual records.
- Anonymised (including aggregated) and pseudonimised personal data. The considerations must take into account factors such as the effect of many data sets being applied with the risk of data being linked to identify an individual, and low numbers of data being released only if they are truly anonymous and therefore not personal data.
- Commercially sensitive information, information given in confidence and legal advice where this applies to joint teams working within public authority services in Herefordshire or Worcestershire.

This overarching protocol sets out the principles for information sharing between partner organisations, setting out the rules that all people working for, or with, the partner organisations must follow when using and sharing information.

The specific purpose for use and sharing of information will be defined in the data exchange agreements that will be specific to the partner organisations sharing information.

## 5 Aims and Objectives

The aim of this protocol is to provide a framework for the partner organisations and to establish and regulate working practices between partner organisations. The protocol will aid information sharing with all partner organisations.

The protocol also provides guidance to ensure the secure transfer of information, and that personal and sensitive personal information is shared for justifiable 'need to know' purposes. In order to reduce the potential for duplication of effort and increase the re-use of currently held information, non-personal and anonymised / pseudonimised information already held should be shared wherever possible, unless it is commercially sensitive or if it would be withheld under a Freedom of Information Act exemption or Environmental Information Regulations exception.

**Care must be taken to ensure that individuals cannot be identified using anonymised / pseudonimised information shared, in conjunction with other information which is already in the possession of, or may come into the possession of the intended recipient.**

These aims include:

- To ensure that mechanisms are in place for information sharing where public protection issues arise.
- To guide partner organisations on how to share personal information lawfully.
- To ensure that the information necessary for decision making is available.
- To explain the security and confidentiality laws and principles of information sharing.
- To increase awareness and understanding of the key issues.
- To emphasise the need to develop and use data exchange agreements
- To manage the risks associated with information being shared and mitigate those risks.
- To encourage flows of data.
- To encourage the recording of data flows.
- To ensure that the partner organisations are sharing information to a standard that is lawful and appropriate and will therefore protect them from accusations of inappropriate use of data.
- To identify the lawful basis for information sharing.
- To identify the resources for training, awareness and provision of advice.

By becoming a partner to this protocol, partner organisations are making a commitment to:

- Adhere to, or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 2018 (See Information Sharing – Relevant Legislation Guidance)
- Apply the Information Commissioner's guidance on data protection and the Code of Practice for Sharing Personal Information.
- Develop local data exchange agreements that specify transaction details for each information flow identified. (See APPENDIX for template)
- To apply NHS and Social Care Caldicott confidentiality principles to personal and sensitive personal information as required.

All partners will be expected to promote staff awareness of the major requirements of information sharing. This will be supported by the production of appropriate guidelines where required, consistent to all partners that will be made available to all staff via the partners' Intranet sites and/or via other communication media.

## 6 Legal Framework

The principal legislation concerning the protection and use of personal information is listed below and further explained in the associated document Information Sharing – Relevant Legislation Guidance, this is not an exhaustive list:

- Data Protection Act 2018
- The Freedom of Information Act 2000
- Human Rights Act 1998 (Article 8)

Other legislation may be relevant when sharing specific information. For example, the sharing of information relating to children or adults may involve (but is not limited to) consideration of any of the following:

- The Children Act 1989 and 2004
- Education Act 1996 and 2002
- Learning & Skills Act 2000
- Education (SEN) Regulations 2001
- Children (Leaving Care) Act 2000
- Mental Capacity Act 2005
- Protection of Children Act 1999
- Immigration and Asylum Act 1999
- Local Government Act 2000
- Criminal Justice Act 2003
- Crime and Disorder Act 1998
- National Health Service Act 1997 and 2006
- Health and Social Care Act 2003
- The Adoption and Children Act 2002
- Health and Social Care Act 2012
- Anti-Social Behaviour, Crime and Policing Act 2014
- Children and Families Act 2014
- Care Act 2014

## 7 Data Covered by this Protocol

All personal and anonymised information as defined in the Data Protection Act 2018 (DPA) and as amended by the Freedom of Information Act 2000 (Section 68).

### *Personal Information*

The terms 'personal information' refers to **any** information held as either manual or electronic records, or records held by means of audio and / or visual technology, about an individual who can be personally identified from that information (see Appendix APPENDIX – Information Sharing Decision Tree).

Consideration should also be given to relevant case law that has defined personal data such as the Durant ruling.

The DPA also defines certain classes of personal information as special categories of data (See APPENDIX ) where certain conditions must be met for that information to be used and disclosed lawfully.

All medical data is deemed to be a special category of personal data (see APPENDIX - Information Sharing Decision Tree) and is held under a duty of confidence.

The Data Protection Act deals with criminal offence data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.

### *Anonymised and Pseudonimised Data*

Partners must ensure anonymised or pseudonimised data, especially when combined with other information from different agencies, **does not** identify an individual, either directly or by summation.

Anonymised data about an individual can be shared without consent (subject to certain restrictions regarding health/social care records), in a form where the identity of the individual cannot be recognised for example, when:

- Reference to any data item that could lead to an individual being identified has been removed, examples could include postcode, date of birth etc.
- The data cannot be combined with any data sources held by a Partner to produce personal identifiable data.

### *Aggregated Data*

Aggregated data can be shared without consent unless they identify an individual.

### *Rights of the Data Subject*

The person about whom the information is held (the Data Subject) has various rights under the Act including the right to be informed about what personal data is being processed, the right to request access to that information, the right to request that inaccuracies or incomplete data are rectified, and the right to have personal data erased and to prevent or restrict processing in specific circumstances. Individuals also have the right to object to processing based on the performance of a task in the public interest / exercise of official authority (including profiling), direct marketing (including profiling); and processing for the purposes of scientific/historical research and statistics. There are also rights concerning automated decision making (including profiling) and data portability.

## 8 Purposes for Sharing Information

- Information should only be shared for a specific lawful purpose, such as where appropriate consent has been obtained.
- Staff should only have access to personal information on a justifiable **need to know** basis, in order for them to perform their duties in connection with the services they are responsible for delivering.
- Having this protocol or any data sharing agreement in place does not give licence for unrestricted access to information another partner organisation may hold. It lays the parameters for the safe and secure sharing of information for a justifiable **need to know** purpose.
- Every member of staff has an obligation to protect confidentiality and is responsible for ensuring that information is only disclosed to those who have a right to see it.
- All staff should be trained and be fully aware of their responsibilities to maintain the security and confidentiality of personal information and any other confidential information. Staff contracts must contain a clause on confidentiality and all employees are bound by this.
- All staff must follow the procedures and standards that have been agreed and incorporated within this protocol and any associated data exchange agreements.
- Each partner organisation will operate lawfully in accordance with the 6 Data Protection Principles; see Information Sharing – Relevant Legislation Guidance.
- Clinical and Social Care staff are also bound by their appropriate professional codes of conduct.

## 9 Restrictions on the Use of Information Shared

Information must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant data exchange agreement (DEA). It is a condition of access that it must not be used for any other purpose without the permission of the Data Controller who supplied the data, unless an exemption applies within the Data Protection Act 2018 or the information is required to be provided under the terms of legislation such as the Freedom of Information Act 2000 or the Environmental Information Regulations 2004.

Additional Statutory restrictions apply to the disclosure of certain information, for example, criminal records, HIV and AIDS, assisted conception and abortion, and child protection. Information about these will be included in the relevant DEA.

## 10 Consent

Consent is not the only means by which data can be disclosed. Under the Data Protection Act 2018, in order to disclose personal information, certain conditions must be met. See Information Sharing – Relevant Legislation Guidance (Data Protection Principles) and Glossary for explanation (APPENDIX )

Where there is evidence of, or reasonable cause to believe, that a child is suffering, or at risk of suffering significant harm; or an adult is suffering or at risk of suffering serious harm, or where the sharing of information is intended to prevent significant harm to children or serious harm to adults, information may be shared without consent. In all cases the decision making process underpinning the decision to share must be documented. Even where the sharing of medical information is considered inappropriate, it may be proportionate for the clinician to share the fact that they have concerns about a child or an adult.

Practitioners must always consider referring concerns to social care or the police where there are concerns about significant or serious harm. In all circumstances the individual's safety and well-being must be kept as the overriding consideration in making any decision about sharing information in these circumstances. If staff are unsure they should seek advice from their Information Governance Team, Legal Services, Caldicott Guardian, Safeguarding Lead or Data Protection Officer.

**In an emergency situation, where there is an identified risk of harm, timeliness is essential, it may not therefore be appropriate to seek consent, if this will result in a delay.** If this is the case, you need to decide how much information needs to be shared in order to fulfil the purpose and the most suitable way in which to share the information given the circumstances. Security applied must be appropriate to the sensitivity of the information being shared and the urgency of the situation. Decisions to share and the reasons for them must be documented.

Where a partner organisation has a statutory obligation to disclose personal information, then the consent of the data subject is not required; but the data subject should normally be informed that such an obligation exists. However, common law duties of confidentiality may still exist.

If a partner organisation decides not to disclose some or all of the personal information, the requesting authority must be informed. For example, the partner organisation may be relying on an exemption or the inability to obtain consent from the data subject.

Consent has to be signified by some communication between the organisation and the data subject. If the data subject does not respond, this cannot be assumed as implied consent. Explicit informed consent must be obtained, subject to any existing exemptions. In such cases the data subject's consent must be clear and cover items such as the specific details of processing, the data to be processed and the purpose for processing.

If consent is used as a form of justification for disclosure, the data subject must have the right to withdraw consent at any time.

Specific procedures will apply where the data subject is either under the age of 16, or where the data subject does not have the capacity to give informed consent. In these circumstances, the relevant policy of the partner organisation should be referred to. Consideration should also be given to other case law, for example, *Gillick v West Norfolk & Wisbeck Area Health Authority and Department of Health & Social Security [1985] 3 All ER 402* (HL) and the requirements of the Mental Capacity Act 2005.

All partner organisations must ensure the roles of Caldicott Guardian, Safeguarding Lead and Data Protection Officer are appropriately filled where applicable and staff are aware who is responsible for compliance in these areas.

## 11 Organisational Responsibilities

- Each partner organisation is responsible for ensuring that appropriate organisational and technical measures are in place to protect the information shared under this protocol and ensure that it is only used for specified lawful purposes.
- Partner organisations will accept the security levels on supplied information and handle the information accordingly.
- Partner organisations accept responsibility for independently or jointly auditing compliance with the data exchange agreements in which they are involved within reasonable timescales.
- Every organisation must make it a condition of employment that employees will abide by their agreed rules and policies in relation to the protection and use of confidential information. This condition should be written into employment contracts and any failure by an individual to follow the policy should be dealt with in accordance with that organisation's disciplinary procedures.
- Every organisation must ensure that staff, volunteers, contractors and temporary staff attend an appropriate level of information handling training; the training should include confidentiality, information security, records management responsibilities etc.
- Every organisation must ensure that contracts with external service providers include information assurance clauses to ensure that confidential information is protected in accordance with the requirements of the organisation originally supplying it. This may include that it is only shared with sub-contractors where prior consent has been obtained from the organisation originally supplying

the information and that the organisation contracting the service has the right to audit the provider's processes to obtain the necessary assurance that confidential information is being handled appropriately.

- The partner organisation originally supplying the information should be notified of any breach of confidentiality, or incident involving a risk or breach of the security of the information, as soon as it is discovered; this should be via the organisation's Data Protection Officer, Information Governance Team, Safeguarding Lead or Caldicott Guardian as appropriate.
- Partner organisations should have documented policies for information security, records management policies covering retention, maintenance and secure destruction of records.
- Partner organisations should be committed to having procedures in place to ensure the quality of information. It is suggested that they consider having a data quality strategy. A strategy will secure and ensure the maintenance of good quality standards and areas for improvement.
- Partner organisations must be aware that a data subject may withdraw consent to processing at any time. Where the partner organisations rely on consent as the condition for processing, then withdrawal means that the condition for processing will no longer apply. Any such withdrawal of consent should be communicated to partner organisations and processing cease as soon as possible unless an exemption (such as risk of harm or prevention or detection of crime) applies.
- Partner organisations must be committed to having procedures in place to address complaints relating to inappropriate disclosure or failure to disclose personal information. Individuals must be provided with information about these procedures.
- Individuals have the right to have access to information held about them with limited exemptions. Partner organisations must ensure that only appropriate access to information is granted, therefore appropriate procedures must be in place to ensure individuals' rights are met.
- It is important to ensure that lessons learned from both Safeguarding Adults Reviews and Child Safeguarding Practice Reviews are shared appropriately, both to ensure that they are adequate and fit for purpose and that action can be taken at an early stage to improve processes in line with those lessons learned in order to reduce the potential for future incidents of a similar nature to occur. Ofsted, the Care Quality Commission, HMI Constabulary and HMI Probation (where appropriate) should have access to full reports to enable them to prepare for local inspections of children's or adults services, health, police and probation where appropriate. It will also ensure that inspectorates are able to adequately assess whether recommendations made are appropriately implemented. There should be a timely sharing of the Reports Executive Summaries between Local Authorities, the Association of Chief Police Officers, and Strategic Health Authorities.

## 12 Individual Responsibilities

- Every individual working for the organisations listed in this protocol is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.
- Every individual should know how to obtain, use and share information they legitimately need to do their job.
- Every individual should uphold the general principles of confidentiality, follow the rules laid down in this protocol and seek advice when necessary.
- Every individual should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal. Criminal proceedings might also be brought against that individual.

## 13 General Principles

- The principles outlined within this protocol are based on legal requirements and recommended good standards of practice, which should be adhered to by all partner organisations.
- This protocol sets the core standards applicable to all partner organisations and should form the basis of all data exchange agreements established to secure the flow of personal information.

- This protocol should be used in conjunction with local service level agreements, contracts, or any other formal agreements that exist between the partner organisations.
- All parties signed up to this protocol are responsible for ensuring that organisational measures are in place to protect the security and integrity of personal information and that their staff are properly trained to understand their responsibilities and comply with the law.
- This protocol has been written to set out clear and consistent principles that satisfy the requirements of the law that all staff must follow when using and sharing personal and other confidential information.
- The specific purpose for use and sharing information will be defined in the data exchange agreements that will be specific to the partner organisations sharing information.

## 14 Implementation

### *Information Flow Mapping*

In order to ensure that data exchange agreements can be developed which accurately reflect the information flowing into, out of and around the organisation, it is necessary to initially identify the internal and external flows of information. It is also necessary to identify areas of risk relating to each flow in order that these can be addressed within the DEA.

Partner organisations should implement a programme to identify and map their internal and external flows of personal, sensitive personal and commercially confidential information.

All flows should be documented and risk assessed in order to ensure that they are appropriate, lawful and that appropriate organisational and technical measures have been implemented to protect the information being mapped.

Where risks are identified, these should be addressed in accordance with the organisation's risk management policy and procedures.

Information flows should be refreshed whenever there is a change to a previous system, process, or procedure.

Information flow mapping should be conducted on all new information flows introduced following the initial flow mapping exercise, these should then be refreshed in accordance with the refresh requirements outlined above.

### *Data Protection Impact Assessments*

A data protection impact assessment should be completed where high risk processing is likely to occur, such as within:

- Projects to develop a system, database, program, application, service, scheme or process.
- Enhancements to any systems, databases, programs, applications, services, schemes or processes.
- New Initiatives, proposals or reviews

This will identify and address privacy, data protection and human rights issues which may arise from changes to or new implementations of processes, procedures, and systems.

### *Privacy Notices*

Partner organisations should ensure that privacy notices are developed which provide data subjects with information about why their personal is collected, what it will be used for, the legal basis for processing, who it will be shared with, how long it will be retained, and their data privacy rights. Privacy notices should be drawn up in accordance with the Information Commissioner's guidance on

privacy notices and should be available through all communication channels. Privacy notices should be approved by the Data Protection Officer or Information Governance Team as appropriate.

### *Recording Information Sharing*

Partner organisations should implement a method of recording instances of information sharing which will document where appropriate what information is being shared, with whom it is being shared, when it was shared, the legal basis for sharing, who approved the sharing and the data exchange agreement and other documentation associated with the shared information.

### *Training and Awareness*

Partner organisations should provide initial information sharing training to staff within their organisation, followed by annual refresher training. Training should cover the following areas:

- Data Protection
- Confidentiality
- Caldicott (if appropriate)
- Information Security
- Records Management
- Information Sharing

Training can be provided on a face-to-face basis, via e-learning or a mixture of both, although it is preferable that an element of face-to-face training is included. Partner organisations should ensure that an appropriate assessment mechanism is included in the training to ensure that staff have understood the subject area and its application within the workplace.

Staff should be provided with awareness materials disseminated through appropriate communication channels, including team meetings and corporate communications. Partner organisations should conduct an annual staff survey to identify any areas of concern with regard to the understanding of responsibilities relating to information sharing.

### *Advice and Assistance*

Partner organisations should provide a contact point for staff to obtain advice and assistance in the application of this protocol.

### *Board and Chief Executive Endorsement*

A communication should be sent to all staff making them aware of the protocol and associated training provision, outlining staff responsibilities with regard to information sharing and identifying a contact point for staff queries, advice and assistance.

Support should be given for the information flow mapping process to be rolled out across the organisation; this may involve additional human resources, particularly where information flows have not previously been mapped.

## 15 Monitoring

Performance against this policy will be monitored through assessment of reported incidents, review of data exchange agreements, information sharing logs, information flow mapping refreshes and feedback from staff within training sessions and staff surveys. Monitoring of the policy will be undertaken by the Data Protection Officer or Information Governance Team at each partner organisation and fed back through the partnership organisation's Information Governance Group.

## 16 Evaluation

Effectiveness of this protocol will be evaluated annually by each partner organisation:

- a review of the information being shared and the reasons for sharing.
- feedback from staff with regard to the benefits realised and issues which have arisen as a result of the protocol's implementation.
- feedback from staff via staff awareness surveys to identify whether staff awareness of information sharing issues has improved.
- feedback from partner organisation with regard to benefits realised and issues which have arisen as a result of the protocol's implementation.

## 17 Audit

An annual audit of compliance with this protocol should be undertaken by each partner organisation.

## 18 Cross References to Other Related Policies and Procedures

Associated policies and procedures can be found on partner organisation's Intranet sites, staff should make themselves aware of policies and procedures relating to Data Protection, confidentiality, information security, and records management.

## 19 Non-Compliance

The consequences of non-compliance with this protocol may be:

- a breach of the law.
- a breach of professional codes of conduct.
- a breach of contract.
- damage to personal and organisational reputation.
- damage and distress to an individual.
- damage to public confidence in partner organisations' abilities to handle personal, sensitive personal and other confidential information appropriately.

Non-compliance with this protocol and associated policies and procedures may result in legal or disciplinary action being taken against individuals. Any disciplinary action taken will be in accordance with Human Resources policies and procedures of the employing organisation.

Any actions taken against partner organisations and third party contractors will be in line with the procedures agreed in the contractual agreements or data exchange agreements.

## 20 Review Arrangements

This protocol will remain in place until any changes in legislation are identified or national guidance necessitates a review.

Any of the signatories can request an extraordinary review at any time where a joint discussion or decision is necessary to address local service developments.

## APPENDIX A – Indemnity Agreement

1.1 In consideration of the provision of information, the signatory organisations undertake to indemnify any of those partners included in this information sharing protocol against any liability which may be incurred by one of the partners as a result of the provision of such information.

1.2 In respect of every disclosure, the receiving party undertakes to indemnify the disclosing party against all actions, claims, demands and civil proceedings and all damages, costs and expenses incurred in connection therewith made or brought against the other party by any person in respect of any loss or distress to that person by the loss, unauthorised destruction, or disclosure of any personal data by the party which has been disclosed to them in confidence by the other. "Disclosure of any personal data" also includes "any disclosure found to be in contravention of the Data Protection Act 2018".

1.3 Provided that this indemnity shall not apply where the liability arises from the information supplied which is shown to have been incomplete or incorrect (ie, where the information does not comply with the fourth data protection principle) unless the partner claiming the benefit of this indemnity establishes that the error did not result from any wilful wrongdoing or negligence on its part.

1.4 The partner claiming the benefit of this indemnity shall notify the granting partner as soon as possible when they receive notice or warning that may give rise to any action, claim, or demand, permits the granting partner to deal with the action, claim or demand by settlement or otherwise and renders the granting partner all reasonable assistance in so doing.

1.5 This indemnity shall not apply to the extent that the partner claiming the benefit of the indemnity makes any admission which may be prejudicial to the defence of the action, claim, or demand. By signing this protocol, partners agree that they have read, understood and agree to abide by the terms and conditions of this Protocol. In addition:

- All information received under this protocol will only be used for the purposes defined and listed in the protocol and subsequent data exchange agreements.
- Information received under this protocol will not be disclosed to another organisation without the agreement of the organisation that provided the information in the first place.
- Information will be retained no longer than is necessary and will be protected by the security measures such as those of a standard of ISO 27001.

## APPENDIX B – Glossary of Terms

**Aggregated** – collated information in tabular format.

**Anonymous Data** – anonymous data is where an organisation does not have the means to identify an individual from the data they hold. The Data Controller must be able to justify why and how the data is no longer personal.

**CCTV** – close circuit television.

**Consent** – The Information Commissioner's legal guidance to the Data Protection Act 2018 is to refer to the Directive, which defines consent as "... any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (3.1.5).

**Data Controller** – a person or a legal body, such as a business or public authority who jointly or alone determines the purpose(s) for which personal data is processed.

**Data exchange agreement** – the local information sharing agreement, based on the template in APPENDIX . A data exchange agreement should be completed for regular flows of information and for one-off flows of information.

**Data Flows** – the movement of information internally and externally, both within and between organisations.

**Data Processing** – any operation performed on data. The main examples are collection, retention, deletion, use and disclosure.

**Data Processor** – operates on behalf of the Data Controller.

**Data Set** – a defined group of information.

**Data subject** – an individual who is the subject of personal information.

**Disclosure** – the passing of information from the Data Controller to another organisation/individual.

**Duty of Confidentiality** – everyone has a duty under common law to safeguard personal information.

**Fully informed implied consent** – in order to comply with the Data Protection Act, to validate implied consent if necessary to satisfy moral obligations, the sender must always strive to fully inform the Data subject wherever possible of the uses to which their information will be put, what disclosures could be envisaged and what the consequences of the processing are. All parties must strive to be open and transparent.

**Health Professional** –any of the following who is registered as:

- A medical practitioner, dentist, optician, pharmaceutical chemist, nurse, midwife of health visitor and osteopaths.

*And;*

- Any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 currently extends to, clinical psychologists, child

psychotherapists and speech therapist, music therapist employed by a health service body and scientist employed by such a body as head of department.

**Health Record** – any information relating to health, produced by a health professional.

**Need to know** – to access and supply the minimum amount of information required for the defined purpose.

**Personal Data** – means data relating to a living individual who can be identified from those data.

**Portability** – data in a useable format that can be electronically transmitted

**Processing** – any operation performed on data. Main examples are collect, retain, use, disclosure and retention.

**Privacy Notice** – a method for informing people why their information is being collected, what it will be used for, who it will be shared with, how long it will be kept for, how they can access their information and a contact name and number for the organisation collecting their information in order that they can raise any objections or queries about how they information is handled.

**Purpose** – the use/reason for which information is stored or processed.

**Recipient** – anyone who receives personal information for the purpose of specific enquiries.

**Serious Crime** – there is no absolute definition of "serious" crime, but Section 116 of the Police and Criminal Evidence Act 1984 identifies some "serious arrestable offences".
These include:

- Treason
- Murder
- Manslaughter
- Rape
- Kidnapping
- Certain sexual offences
- Causing an explosion
- Certain firearms offences
- Taking of hostages
- Hijacking
- Causing death by reckless driving
- Offences under the prevention of terrorism legislation (disclosures now covered by the Prevention of Terrorism Act 1989)

**Subject Access** – the individual's right to obtain a copy of information held about themselves.

**Third Party** – any person who is not the data subject, the Data Controller, the Data Processor.

## APPENDIX C – Confidentiality Statement

***Suggested wording for meetings where confidential information is shared***

To enable the exchange of information between attendees at this meeting to be carried out in accordance with the Data Protection Act 2018, the Human Rights Act 1998 and the Common Law Duty of Confidentiality, all attendees are asked to agree to the following statements. This agreement will be recorded in the minutes.

1) Information can be exchanged within this meeting for the purpose of identifying any action that can be taken by any of the agencies or departments attending this meeting to resolve the problem under discussion.
2) A disclosure of information outside the meeting, beyond that agreed at the meeting, will be considered a breach of the data subject's confidentiality and a breach of the confidentiality of the agencies involved.
3) All documents exchanged should be marked in accordance with the protective marking scheme of the relevant organisation. All minutes, documents and notes of disclosed information should be kept in a secure location to prevent unauthorised access.
4) If further action is identified, the agency(ies) who will proceed with this action(s) should then make formal requests to any other agencies holding such personal information as may be required to progress this action quoting their legal basis for requesting such information. Information exchanged during the course of this meeting must not be used for such action.
5) If the consent to disclose is felt to be urgent, permission should be sought from the Chair of the meeting who will take appropriate guidance on the lawfulness of the disclosure such as the prevention or detection of crime, apprehension or prosecution of offenders, or where it is required to prevent injury or damage to the health of any person.

This confidentiality agreement is in relation to the _____

_____ meeting(s).

Signature _____ Date _____

Name _____

Representing _____

Name and/or Organisation _____

---

**Copies of this signed agreement are to be held by the Chair.**

## APPENDIX D – Data Exchange Agreement (DEA) Template

All wording in bold should be included in your Data exchange agreement and sections 1-3 need to be completed.

**What is the Purpose of this Data Exchange Agreement?**

<Set out why you need to share the data>

**What is the Legal Basis for Data Exchange?**

*It is important to ensure that any partner/individual who provides or receives information (and then holds and processes it) is able to identify the necessary requirement for processing in the Data Protection Act to ensure that the sharing is fair and lawful.*

*The lawful grounds for processing set out in the Data Protection Act include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract to which the data subject is a party, for the compliance with a legal obligation to which the data controller is subject, the processing is necessary to protect the vital interests of the data subject or the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.*

*When sensitive personal data is being processed (now known as "special categories of personal data"), additional conditions must be met.*

*If consent is the lawful basis for processing, partners must ensure that the appropriate privacy notices are in place, and that the consent gained is informed, explicit consent recorded in such a way as to be able later to identify that consent was gained for specific processing. If consent is withdrawn mechanisms must be in place to stop processing of the personal data across all partner organisations.*

<Set out the legal basis for sharing, referring to the Relevant Legal Guidance document as necessary, and explaining which of the lawful grounds for processing under the Data Protection Act is met. If consent is being relied on, expand on how consent will be captured and recorded, and include a copy of the privacy notice as an appendix.>

| **What data is it necessary to exchange?** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Data Set** | **Who from** | **Who to** | **Why** | **Which Organisation owns the information** | **Frequency of sharing** | **How will information be exchanged** | **How long will data be held for by recipient organisation** |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

If any further data is required over and above that included in this Data exchange agreement, contact should be made with the Data Protection Officer or Information Governance Officer of the sending organisation prior to the release of any information.
Ensure that all data items to be exchanged are listed with a clear 'data definition'. All parties to the agreement should have a common understanding of the information to be provided/received.

a. **Who is going to be responsible for exchanging this data and ensuring data is accurate?**

b. **How will you keep a record of what information has been exchanged?**

c. **How is this information going to be exchanged?**

d. **Who will have access to this data and what they may use if for?**

e. **How long will access be granted for?**

f. **How securely does the data need to be stored?**

g. **How long are you going to keep the data?**

h. **Further Use of Data – Will it be shared with another party?**

## 2 Breach of Confidentiality

In the event that this agreement is breached by either partner or any named third party who has received data under this agreement the appropriate lead officer should be notified immediately and in any case, no later than within 24 hours.

Depending upon the seriousness of the breach this may be reported to the Information Commissioners Office within the legal requirement of 72 hours of discovery of the breach and where criminal action is involved the Police may also be informed.

Where staff have failed to comply with organisational policies and procedures disciplinary action will be taken against them and in the case of a criminal offence legal proceedings may be taken against those responsible for the breach.

## 3 Complaints Procedures

*Each partner must be committed to having procedures in place to address complaints relating to inappropriate disclosure or failure to disclose personal information. Individuals must be provided with information about these procedures.*

<Include details of how complaints will be handled here>

## 4 Access to Information

*The Data Protection Act provides individuals the right to have access to information held about them with limited exemptions. It is necessary to ensure that only appropriate access to information is granted, therefore the agreement must detail the responsibilities of each organisation to ensure individuals' rights are met appropriately.*

*Individuals also have a number of rights under data protection legislation, including the right to restrict processing, the right to erasure, the right to object to processing, the right to rectification of inaccurate data, and the right to receive personal data concerning the data subject in a commonly used format (known as data portability) and transferred to another controller without hindrance.*

<Include details of the processes for handling requests from individuals to view information about themselves, and requests concerning their other rights>

## 5 Closure/Termination of Agreement

Any partner organisation can suspend this Data Exchange Agreement for 45 days if security has been seriously breached. This should be in writing and be evidenced.

Any suspension will be subject to a Risk Assessment and Resolution meeting, the panel of which will be made up of the Signatories of this agreement, or their nominated representative. This meeting to take place within 14 days of any suspension.

Termination of this Data Exchange Agreement should be in writing to Partner Organisations, giving at least 30 days' notice.

## 6 Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIR) and Re-Use of Public Sector Information Regulations 2015

As well as data protection legislation, all recorded information held by public sector agencies is subject to the provisions of the Freedom of Information Act 2000, the Environmental Information Regulations 2004, and the Re-Use of Public Sector Information Regulations 2015. Whilst there is no requirement to consult with third parties under this legislation, the parties to this Agreement will consult the party from whom the information originated and will consider their views to inform the decision making process. All decisions to disclose must be recorded by the disclosing organisation.

*Information requested under information legislation shall only be withheld where the information would be exempt from disclosure and if applicable the public interest lie in favour of withholding. Personal data is one type of information likely to be exempt under FOIA and EIR. Public sector information is usually licensed under the open government licence by the organisation that owns the information.*

<Include the process for answering requests for information under FOI / EIR, and requests for re-use of data>

## 7 Appropriate Signatories

Name _____

Signature _____

Organisation_____

Date_____

Name _____

Signature _____

Organisation _____

Date _____

**One copy of the Agreement must be sent to each partner organisation's Data Protection Officer or Information Governance Team, and the original signed copy must be retained within the lead team involved in the sharing of information**

## APPENDIX E – Process for Review of a Data exchange agreement

The aim of a review is to ensure that the DEA is achieving its purpose and that the actual process of exchanging data is operating efficiently.

**1 Policy Statements and Purpose of this Data exchange agreement**
Is the policy statement and the purpose as identified in the DEA still accurate in relation to the present use of the data?

**2 Legal Basis for Data Exchange**
Do the legal bases in the DEA cover all the parties?

**3 What data is it necessary to exchange?**
Is the data which is exchanged by the parties in accordance with the DEA.

**4 Who is going to be responsible for exchanging this data and ensuring data is accurate?**
Is the contact list up to date and accurate?

**5 How will you keep a record of what information has been exchanged?**
How are the parties keeping a record of what information has been exchanged? Random samples of the data exchanged could be checked against the source record to see if there is evidence of the data exchange.

**6 How is this information going to be exchanged?**
Is data still being exchanged in accordance with the DEA?

**7 Who will have access to this data and what may they use it for?**
What use of the data is made by the parties receiving data and is access restricted in accordance with the DEA.

**8 Timescales**
Are any timescales in the DEA being adhered to?

**9 How securely does the data need to be stored?**
Are all parties applying the security measures in accordance with the DEA?

**10 How long are you going to keep the data?**
Are all the parties retaining and destroying the data in accordance with the DEA?

**11 Further Use of Data**
Is there any evidence that data is being used by any party for purposes other than in accordance with the DEA without consent from the originator?

**12 Breach of Confidentiality**
Have there been any breaches of confidentiality which have not been reported to the other parties? How may any breaches been dealt with?

**13 Indemnity/confidentiality agreements**
Is there evidence that any individual who is not covered by an organisation which is signatory to the DEA has signed a confidentiality agreement?

**14 Freedom of Information Act 2000 (FOIA)**
Is this DEA publicly available and also available internally for relevant staff?

**15 Requests for Disclosure of Information Received under this DEA**

Have there been any instances where a party has disclosed information received under this DEA without consulting the originating party?

**16 Appropriate Signatories**

Is the DEA signed by appropriate staff?

**Review was carried out by:**

Name _____

Signature _____

Organisation _____

Date _____

Name _____

Signature _____

Organisation _____

Date _____

**A copy of this review should be stored with the DEA, any deficiencies should be brought to the attention of the Signatories as appropriate.**

## APPENDIX F – Seven Golden Rules for Information Sharing

1 **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.

2 **Be open and honest** with the person (and/or their family, where appropriate) from the outset about why, what, and how the information will be used and with whom information will be shared, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3 **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

4 **Share with consent where appropriate** and, where possible respect the wishes of those who did not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5 **Consider safety and well-being:** Base your information sharing decisions on consideration of the safety and well-being of the person and others who may be affected by their actions.

6 **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purposes for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7 **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

## APPENDIX G – Information Sharing Decision Tree

## Acknowledgements:

Herefordshire Council and its partners acknowledge the work that Leicestershire County Council DSP Review Group and subsequently Dudley Beacon and Castle PCT and Dudley MBC undertook to produce the Protocol on which this document is based.

This high level document has been jointly further developed by public sector organisations in Herefordshire, to facilitate the sharing of information amongst key organisations and to incorporate revised guidance from HM Government, Every Child Matters, Department of Health, the Laming Review, Information Commissioner's Office, GMC, National Patient Safety Agency, Nursing and Midwifery Council, Royal College of Psychiatrists and many others.