INFORMATION SHARING PROTOCOL

COVENTRY AND WARWICKSHIRE HEALTH AND CARE PARTNERSHIP.

Arden GEM Commissioning Support Unit

Coventry and Rugby Clinical Commissioning Group

South Warwickshire Clinical Commissioning Group

Warwickshire North Clinical Commissioning Group

South Warwickshire NHS Foundation Trust

Coventry and Warwickshire Partnership NHS Trust

University Hospital Coventry & Warwickshire NHS Trust

George Eliot Hospital

Warwickshire County Council

Coventry City Council

Coventry and Rugby GP Alliance

South Warwickshire GP Federation

Primary Care Warwickshire

Myton Hospice

CONTENTS

1. Introduction

1.1 This document is an Information Sharing Protocol (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 all Partner Organisations to this Protocol within Coventry and Warwickshire.

1.2 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. This balance between the need to share information to provide quality service and protection of confidentiality is often a difficult one to achieve.

1.3 The legal situation regarding the protection and use of personal information can be unclear. This situation may lead to information not being readily available to those who have a genuine need to know in order for them to do their job properly. See Appendix B for Relevant Legislation.

2. Scope

2.1 This overarching Protocol sets out the principles for information sharing between Partner Organisations (Appendix A).

2.2 This Protocol sets out the rules that all people working for or with the Partner Organisations must follow when using and sharing information including other public sector, private and voluntary organisations.

2.3 The Protocol applies to the following information:

2.3.1 All personal information processed by the Partner Organisations, regardless of format and / or method of processing including electronically (e.g. computer systems, CCTV, Audio etc.), or in manual records. This is a non-exhaustive list.

2.3.2 In relation to anonymised, including aggregated, personal data, the considerations, though less stringent, must take into account factors such as commercial or business, special categories of data, and the effect of many data sets being applied.

2.4 This Protocol will be further extended to include other public sector, private and voluntary organisations working in Partnership to deliver services.

2.5 The specific purpose for use and sharing information will be defined in the Data Sharing Agreements that will be specific to the Partner Organisations sharing information.

3. Aims and Objectives

3.1 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 also provides guidance to ensure the secure transfer of information, and that information shared is for justifiable 'need to know' purposes (see 6.3 and 11.6).

3.2 The objectives are:

a. To guide Partner Organisations on how to share personal information lawfully.

b. To outline the security and confidentiality laws and principles of information sharing.

c. To increase awareness and understanding of the key issues.

d. To emphasise the need to develop and use Data Sharing Agreements.

f. To encourage flows of data between Partner Organisations

g. To protect the Partner Organisations from accusations of wrongful use of Personal Data including Special categories of Personal Data and Criminal Data.

h. To identify the lawful basis for information sharing.

3.3 By becoming a Partner to this Protocol, Partner Organisations are making a commitment to:

a. Apply the Information Commissioner's Code of Practice's 'Fair Processing' and 'Best Practices' Standards;

b. Adhere to or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 2018, GDPR 2016, collectively referred to as the 'Data Protection Legislation'; (See Appendix B).

c. Develop local Data Sharing Agreements that specify transaction details. (See Appendix E for sample template but other templates that adhere to the Information Sharing Protocol may be used for local Information Governance).

d. To apply NHS Caldicott confidentiality standards.

3.4 All Partner Organisations will be expected to promote staff awareness of the major requirements of Information Sharing under this Protocol. This will be supported by the production of appropriate guidelines where required that will be made available to all staff via the Partner Organisations' Intranet sites and/or via other communication media.

4. The Legal Framework

4.1 The principal legislation concerning the protection and use of personal information is listed below and further explained in Appendix B:

- Human Rights Act 1998 (article 8)
- The Freedom of Information Act 2000
- Data Protection Act 2018
- General Data Protection Regulation (GDPR) 2016
- The Common Law Duty of Confidence

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

- The Children Act 1989
- The Children Act 2004
- Education Act 2002
- Education Act 1996
- The Education (Special Educational Needs) (England) (Consolidation) Regulations 2001
- Children (Leaving Care) Act 2000
- Immigration & Asylum Act 1999

- Local Government Act 2000
- Criminal Justice Act 2002
- Crime and Disorder Act 1998
- National Health Service (Consequential Provisions) Act 2006
- The Adoption and Children Act 2002
- Health and Social Care Act 2012
- Care Act 2014

5. Data covered by this Protocol

5.1 All personal and anonymised information as defined in the Data Protection Legislation. **Anonymised data should be used wherever possible.**

5.2 **Personal Information**

5.2.1 The term ‘personal information’ or ‘personal data’ means any information relating to an identified or identifiable natural person who is a living individual (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

5.2.3 The Data Protection Legislation also defines certain classes of personal information as ‘Special Categories of Personal Data' where additional conditions must be met for that information to be used and disclosed lawfully.

5.2.4 An individual may consider certain information about themselves to be particularly ‘sensitive’ and may request other data items to be kept especially confidential e.g. any use of a pseudonym where their true identity needs to be withheld to protect them.

5.2.5 All health data is deemed to be Special Category Personal Data and is held under a duty of confidence.

5.3 **Anonymised Data**

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

5.3.2 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 i.e. when:

- Reference to any data item that could lead to an individual being identified has been removed

- The data cannot be combined with any data sources held by a Partner Organisation to produce personal identifiable data.

6. Purposes for Sharing Information

6.1 Information should only be shared for a specific lawful purpose, basis or where appropriate consent has been obtained.

6.2 Staff should only have access to personal information on a justifiable **need to know** basis, for them to perform their duties in connection with the services they are there to deliver.

6.3 Having this agreement in place does not give license 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.

6.4 Every member of staff has an obligation to protect confidentiality and are responsible to ensure that information is only disclosed to those who have a right to see it.

6.5 All staff should be trained and be fully aware of their responsibilities to maintain the security and confidentiality of personal information. Staff contracts also contain a clause on confidentiality and all employees are bound by this.

6.7 Each Partner Organisation will operate lawfully in accordance with the 6 Data Protection Principles, see Appendix B.

6.8 Clinical/Social Care staff are also bound by their appropriate professional codes of conduct.

7. Restrictions on use of Information Shared

7.1 Information must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant Data Sharing Agreement. 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 the Freedom of Information Act 2000 and any subsidiary regulation.

7.2 Additional Statutory restrictions apply to the disclosure of certain information for example Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection. Information about these will be included in the relevant DSA.

8. Consent

8.1 Consent is not required for information to be shared for direct care purposes, including referrals between organisations. However explicit consent is more likely to be required where:

- The legal basis for sharing the information is less clear;
- An individual would be more likely to object should the data be shared without his or her consent; or
- The sharing is likely to have a significant impact on the individual.

This means that explicit consent is more likely to be required for indirect care or secondary purposes, eg research, population profiling, unless there is another legal basis for the sharing to take place.

All parties of this agreement must have a record of the consent given where this is used as the legal basis for sharing information.

Article 6 GDPR mentions six available lawful bases for processing: consent, contract, legal obligation, vital interest, public task, and legitimate interests.

8.2 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 be informed that such an obligation exists which will usually be done by way of privacy notice unless an exemption applies. However common law duties of confidentiality may still exist.

8.3 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 on the inability to obtain consent from the data subject.

8.4 Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation. Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data. Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly. Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity. Explicit consent must be expressly confirmed in words, rather than by any other positive action. There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate. 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 and explicit 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.

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

8.6 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 (see: Fraser guidelines, and the requirements of the Mental Capacity Act 2005).

9. Organisational Responsibilities

9.1 Each Partner Organisation is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this Protocol.

9.2 Partner Organisations will accept the security levels on information supplied under this Protocol ~~information~~ and handle the information accordingly.

9.3 Partner Organisations accept responsibility for independently or jointly auditing compliance with the Data Sharing Agreements in which they are involved within reasonable time-scales.

9.4 Every Partner Organisation should 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.

9.5 Every Partner Organisation should ensure that their contracts with external service providers abide by their rules and policies in relation to the protection and use of confidential information.

9.6 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 information

9.7 Partner Organisations should apply their policies for retention, and secure waste destruction.

9.8 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 identify areas for improvement.

9.9 Partner Organisations must be aware that a data subject may withdraw consent to processing unless an available exemption applies. 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.

9.10 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.

9.11 The Data Protection Legislation provides individuals the right to have access to information held about them with limited exemptions. Partner Organisations must ensure that appropriate procedures are in place to ensure individuals' rights are met.

10. Individual Responsibilities of Employees and Staff Working at Partner Organisations

10.1 Every individual working for the Partner Organisations listed in this Partnership Agreement is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

10.2 Every individual should know how to obtain, use and share information they legitimately need to do their job.

10.3 Every individual has an obligation to request proof of identity, or takes steps to validate the authorisation of another before disclosing any information.

10.4 Every individual should uphold the general principles of confidentiality follow the rules laid down in this Protocol and seek advice when necessary.

10.5 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.

11. Use of this Information Sharing Protocol

11.1 This Protocol sets out recommended good standards of practice or legal requirements that should be adhered to by all Partner Organisations.

11.2 This Protocol sets the core standards applicable to all Partner Organisations and should form the basis of all Data Sharing Agreements established to secure the flow of personal information with strict adherence to Health and Social Care Information Centre (HSCIC) guidelines.

11.3 This Protocol should be used in conjunction with local service level agreements, contracts or any other formal agreements that exist between the Partner Organisations.

11.4 All Partner Organisations 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.

11.5 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 information.

11.6 The specific purpose for use and sharing information will be defined in the Data Sharing Agreements that will be specific to the Partner Organisations sharing information.

12. Review Arrangements

12.1 This Information Sharing Protocol will be formally reviewed annually by the Information Governance Advisory Group, unless new or revised legislation or national guidance necessitates an earlier review.

12.2 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 – Signatures and Contact Information

Agreement: We the undersigned do hereby agree to implement the terms and conditions of this Protocol .
Contact Information

Organisation	Print Name	Signature	Date	Job Title	Telephone	Email
Arden GEM CSU	Nick Pulman			Caldicott Guardian		n.pulman@nhs.net
Coventry and Rugby CCG	Dr Steve Allen			Caldicott Guardian		
South Warwickshire CCG	Dr Sukhi Dhesi			Caldicott Guardian		
Warwickshire North Clinical CCG	Rebecca Bartholomew			Caldicott Guardian		
South Warwickshire NHS Foundation Trust	Dr Fraser Millard			Caldicott Guardian		
Coventry and Warwickshire Partnership NHS Trust	Sharon Binyon			Caldicott Guardian		
University Hospital Coventry & Warwickshire NHS Trust	Professor Kiran Patel			Caldicott Guardian		

George Eliot Hospital	Dr Catherine Free			Caldicott Guardian		
Warwickshire County Council	Nigel Minns			Caldicott Guardian		
Coventry City Council	Liz Gaulton			Caldicott Guardian		

APPENDIX B - LEGAL CONTEXT

THE DATA PROTECTION LEGISLATION

Data Protection Legislation governs the standards for the processing of personal data including the collection, use of and disclosure of such information. The legislation requires that data controllers meet certain obligations. It also gives individuals or 'data subjects' certain rights with regard to their own personal data. The main standard for processing personal data is compliance with the 6 data protection principles at Article 5 of the GDPR, summarised as follows:

1) the processing of personal data must be lawful and fair
2) personal data must only be processed for a specified, explicit and legitimate purpose
3) personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4) personal data must be accurate, kept up to date; when inaccurate, personal data is erased or rectified without delay
5) personal data must be kept for no longer than is necessary.
6) personal data must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (i.e. protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)

One of the lawful bases from Article 9 of the GDPR must be applied in addition to a lawful basis from Article 6 of the GDPR when processing Special Categories of personal data, with reference to Member State Law in the Data Protection Act 2018.

THE HUMAN RIGHTS ACT 1998

The UK Human Rights Act 1998 gives further effect in domestic law to Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law be compatible with the Convention Articles and places a legal obligation on all public

authorities to act in a manner compatible with the convention. Should a public authority fail to act in such a manner then legal action can be taken under Section 7 of the Act.

Article 8 of the Act states that:

> "Everyone has the right to respect for his private and family life, his home and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law". It is likely that this Sharing of information will be for the purposes of one of the following legitimate aims:

- In the interests of national security.
- Public Safety.
- Economic well-being of the country.
- The prevention of crime and disorder.
- The protection of health or morals.
- The protection of the rights or freedoms of others.

FREEDOM OF INFORMATION ACT 2000

Information held by or on behalf of a public authority may be disclosed to a party requesting it except where a statutory exemption applies. For example, personal data is normally exempt under the Act (but may be disclosable under DPA 2018); as is information provided under a duty of confidence.

LOCAL GOVERNMENT ACT

The main power specific to local authorities is section 2 Local Government Act 2000 - the power of "well-being". This enables LA's to do "anything" to promote social, economic, or social well-being in their area provided the act is not specifically forbidden by other statute (including the Data Protection Act) and that in carrying out the act it gives regard to its own community strategy. For example, all councils are taking measures, including data sharing, to reduce crime in its area in order to promote well-being. In addition S111 Local Government Act 1972 enables local authorities to do anything conducive or incidental to the discharge of any of its functions, providing it has specific statutory authority to carry out those main functions in the first place. The above are general powers available to local authorities. In addition, authorities are granted statutory powers relating to specific activities and these should be referred to as appropriate in the Data Sharing Agreement.

THE CRIME AND DISORDER ACT 1998

Section 115 of the Crime and Disorder Act 1998 confers a power on any 'relevant authority' (which are the police, local authority, health authority and probation service or to any other person acting on behalf of such authority) to sharing that information which is 'necessary' or 'expedient' to help implement the provisions of the Act which includes contributing to local strategies to reduce crime and disorder. The parties to this sharing agreement are relevant authorities for the purposes of this legislation.

Section 17 Crime and Disorder Act 1998 requires that all Local Authorities consider crime and disorder reduction while exercising their duties. Sections 5 and 6 of the Crime and Disorder Act impose a general duty upon local authorities to formulate and implement a strategy for the reduction of crime and disorder in its area.

COMMON LAW DUTY OF CONFIDENCE

The duty of confidence falls within common law as opposed to statutory law and derives from cases considered by the courts. There are generally three categories of exception to the duty of confidence:

- Where there is a legal compulsion to disclose.
- Where there is an overriding duty to the public.
- Where the individual to whom the information relates consented.

Partners should consider which of these conditions are the most relevant ones for the purposes of this Sharing agreement. The guidance from the Information Commissioner states that because such decisions to disclose 'in the public interest' involves the exercise of judgement it is important that they are taken at an appropriate level and that procedures are developed for taking those decisions. The partners to this agreement should document within this agreement how this duty will be maintained, e.g. need to know.

CALDICOTT

Where Health Data is concerned; when sharing information with others, due regard must be given to the Caldicott principles listed below. Ensure that all the conditions are met before sending the data. If unsure then speak to your line manager, or the appropriate Caldicott Guardian.

Caldicott Principles:

- Justify the purpose before sharing information.
- Only use patient identifiable data when absolutely necessary.
- Use the minimum that is required, do not share more data than is necessary, i.e. do not send the whole patient record when the request relates to a recent event.
- Access to the data should be on a strict need to know basis.
- Be aware of your responsibilities in complying with organisational policies relating to confidentiality.
- Understand the law, if uncertain, speak to you line manager.
- The duty to share information can be as important as the duty to protect patient confidentiality.

Where Health Data is concerned Health staff, and others working in partnership with them, should be aware of the concept of Safe Haven**.**

Safe Havens will:

- Provide a secure location restricting access to only authorised staff and will be locked outside normal hours.
- Be staffed by those individuals with authority to access confidential information and who are under contractual and statutory obligations to maintain confidentiality.
- Ensure that no confidential information will be released to parties outside the partner organizations unless it is deemed appropriate. Staff should make reference to the Caldicott Principles listed above and seek advice from the relevant Caldicott guardian where uncertain.
- Ensure that wherever possible the NHS number is present and person identifiable data has been removed

Appendix C - Glossary of Terms

Accessible Record – a health, educational or public record

Aggregated – Data combined from different sources to present a bigger picture

Anonymised data – data where an Organisation does not have the means to identify an individual from the data they hold. If the Data controller has information, which allows the Data Subject to be identified, this is then called **Pseudonymised data**. Data Controller must be able to justify why and how the data is no longer personal.

CCTV – close circuit television.

Consent – The General Data Protection Regulation (GDPR) defines consent in Article 4 (11) as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Data/Information –

a) Information being processed by means of equipment operating automatically or
b) Information recorded with the intention it be processed by such equipment.
c) Recorded as part of a relevant filing system or
d) Not in a, b or c, but forming part of an accessible record.
e) Recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Data Controller – a person or a legal body such as a business or public authority who jointly or alone determines the purposes for which personal data is processed.

Data Sharing Agreement – the local information sharing agreement based on the attached template Appendix E.

Data Flows – the ingoing and outgoing movements of information, both within an organisation and to/from others

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

Data Processor – person or organisation who 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.

European Economic Area (EEA) – this consists of the EU countries and Iceland, Liechtenstein and Norway.

Fair processing – to inform the Data Subject how the data is to be processed before processing occurs

Health Professional – In the Data Protection Act 2018 "health professional" means any of the following who is registered as:

A medical practitioner, dentist, optician, pharmaceutical chemist, nurse, midwife or 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 –The DPA 2018 defines a health record as “a record which consists of data concerning health and has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates.”

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 (including opinion and expression of intention). Examples are: name, contact details, NHS number, date of birth, next of kin details

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

Pseudonymised data – where personal information has been “de-identified” i.e. personal information which directly identifies an individual, e.g. name or date of birth and address used together, has been replaced by non-identifying, artificial data, e.g. NHS number or other code. Pseudonymised data is partially anonymised data and the identification of an individual can be re-established using other available data held by the Data Controller organisation. See also **Anonymised data**

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

Recipient – anyone who receives personal information for the purpose of specific inquiries

Relevant Filing System – two levels of structure, (i) filing system structured by some criteria (ii) each file structured so that particular information is readily accessible.

Special Categories of Personal Data – The Data Protection Legislation defines Special Categories of Personal Data as:

- Racial/ethnic origin
- Political opinions
- Religious/philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex life
- Sexual orientation

Criminal offenses and convictions are processed separately under Article 10 GDPR, with reference to Member State Law under the Data Protection Act 2018

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 prevention of terrorism legislation.

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 (includes Health, Housing, Education, Carers, Voluntary Sector etc. as well as members of the public).**

Appendix D - Confidentiality Statement

To enable the sharing of information between ……and ……. 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. This agreement will be recorded.

This information sharing activity contains confidential patient/ person identifiable information. In order to comply with the law protecting confidentiality the information can only be supplied subject to the following conditions.

1. A senior member of staff in your organisation must take personal responsibility for maintaining confidentiality.

2. The information is stored in a secure environment at all times (e.g. in a locked cupboard, or where stored electronically protected by passwords).

3. Once the task has been completed the original information and all copies will be destroyed or returned to Arden and GEM CSU as soon as possible.

4. Only members of staff legitimately involved in the work should have access to this information in order to carry out the agreed task(s).

5. Members of staff accessing this information are aware of the conditions under which it is supplied, and have signed an honorary contract with this organisation.

6. The information will only be used for the purpose for which it is supplied.

7. Information supplied will not be disclosed to any other organisation or individual.

This agreement must be signed by a member of the organisation with sufficient seniority to ensure that these terms are met.

I have read, understood and agree to abide by these conditions.

Signature……..Date……
…..…

Name…….

Representing…Name and/or Organisation……..

……

Copies of this signed agreement are to be held by the Arden and GEM CSU lead in this work.

Appendix E - Data Sharing Agreement (DSA) Template

NHS England is currently in the process of a Gateway review for publication of their guidance to IG and Data Sharing Agreements. For DSA's they recommend:

A DSA should clearly set out what is the lawful basis for sharing the information that is the subject of the agreement. The DSA should be detailed and specific.

This section provides further information to help you to complete the template which can be found and the end.

A DSA should be published so that it is publicly available to all patients. It will add further information to your fair processing communications strategy – see our guide 'How to inform patients about how their personal information is used'.

A DSA should include:

A clear purpose or purposes for sharing information
The agreement should explain the overall aims and benefits for sharing information in clear and understandable terms.

The organisations involved
All organisations party to the agreement must be clearly identified.

Identify the data controllers and whether they are acting jointly or in common.

Where applicable identify the data processors and the data controller responsible for the contract.

Note: A data processor can be included in the DSA as a signatory party but there must be a separate data processing contract in place to ensure compliance with the law (the DPA).

Names and contact details for key members of staff should be included, specifically the senior person accountable for the Information Sharing Agreement; the Caldicott Guardian and/ or the Information Governance Lead (person responsible for information governance in the organisation).

It should be clear who the central point of contact is within the organisation for any matter concerning the DSA.

The DSA should be signed by a senior accountable person within the organisation who is authorised to commit the organisation to the agreement. For example:

- An Accountable Officer; Senior Responsible Officer, Chief Executive Officer

Governance

Consideration should also be given to who is responsible for leading the development of the DSA and coordinating the review process.

Each organisation signed up to the DSA are joint owners and equally responsible for it.

Where a DSA covers several organisations, a governing group should be established to oversee, support and maintain the secure sharing of information under the agreement.

Each organisation party to the DSA should be represented on the group and actively involved in the decision making process. This can be achieved in various ways, for example, by direct membership of the group or by nominating a member to act on their behalf.

Terms of reference for the governance arrangements should be included in the DSA e.g. as an appendix.

Once the DSA is in place it should be reviewed on a regular basis to ensure that it is effective and kept up-to-date.

In addition to routine matters such as monitoring and review, the terms of reference should include:

- How variations to the DSA will be managed
- Procedure for signing up new partners
- Procedure for terminating the agreement
- Dealing with information governance breaches
- Dealing with disputes

Types of information to be shared

The agreement should set out the types of information that will be shared between the partner organisations, and the parameters for sharing.

Information gathered through the data flow mapping exercise should be used to inform this section. The data flow maps should be attached as an appendix.

This section should be quite detailed.

Basis for sharing

The agreement should clearly explain the legal basis for sharing information.
If consent is the basis for disclosure, explain how this will be obtained, who is responsible for obtaining it and how it will be recorded.

Where personal data is shared under a legal power, explain how patient objections will be managed and how they will be recorded.

Explain how and when you will share data in accordance with the Health and Social Care (Safety and Quality) Act 2015, which establishes a legal duty to share information about a patient when:

- it is likely to facilitate the provision of direct care; and
- in the best interests of the individual patient; and
- they have not raised an objection.

N.B. Implementation guidance is awaited, but for the moment you must ensure patients are adequately informed so they understand how their information is used and what rights they have in order to support compliance statutory duty to share when this becomes law.

State the circumstances and legal basis you will use when it is necessary to override a patient's objection and/ or disclose personal data without consent.

Access and individual's rights

Individuals have a legal right of access to their personal data under the DPA (a subject access request). The Freedom of Information Act 2000 provides a legal right of access to information held by a public body.

Organisations have a legal duty to respond to Subject Access Requests and FOIA requests.

Each organisation is responsible for dealing with requests it receives for access to information they hold on a case by case basis.

The agreement should explain how a request for access to shared data will be managed e.g. discussing responsibility for responding and any necessary co-ordination.

You must consider the legal duty to process personal data fairly and in accordance with the patient's rights. If personal data is pooled into a shared system, then procedures must be established to provide access to that data via a central point of contact.

Obligations on all parties

This section should list all of the prerequisites for information sharing partnership.

For example, all DSA partners should have:

- A recognised accredited standard of information governance e.g. a satisfactory level of compliance with the NHS Data Security and Protection Toolkit or ISO 27001 Information Security Management Standard;
- Common technical and organisational security arrangements in place;
- Procedures to ensure and monitor data quality;

- Systems to ensure confidentiality is included in employment contracts and all staff are trained;
- Sanctions in place to deal with a failure to comply with the agreement or breaches by individual staff;
- Procedures in place to report and deal with information governance breaches.

Obligations on an individual party

Identify and explain individual responsibilities if one organisation takes the lead for any aspect of the DSA, for example, coordinating a review; subject access requests; investigating information governance breaches etc.

Retention and deletion

The rules for retention and deletion of shared data should be set out in the agreement.

Where organisations share personal information, those organisations should agree what to do with the information when they no longer need it.

The fifth DPA principle and NHS Records Management Code of Practice set out the requirement to:

- review the length of time you keep personal data;
- decide whether to retain it and for how long;
- securely archive inactive information; and
- securely delete information when the retention period has expired.

Legal minimum retention periods apply to public sector data, which should be taken into account when setting policy. If data is held electronically in a shared system, you need to agree how that information will be managed during its lifecycle.

Dispute Resolution

You need to agree and specify a procedure for dealing with disputes arising under the Agreement.

Minor disputes can usually be resolved through discussion between the respective organisations' information governance leads. In some circumstances it may be necessary to escalate the issue up to senior managers.

The Governing Group's intervention may be required to decide on unresolved disputes.

Settling disputes by mediation should also be considered.

Data Protection Principles

Each partner organisation is a data controller and legally responsible for ensuring personal data is processed in compliance with the data protection principles. As such they are responsible for their own acts and omissions.

The Information Commissioner's Office (ICO) is the Regulator for the DPA and has powers to take action for non-compliance issues. The powers include monetary penalties for the most severe contraventions.

Liability

Each partner organisation is a data controller and legally responsible for ensuring personal data is processed in compliance with the data protection principles. As such they are responsible for their own acts and omissions.

Termination

Procedures for dealing with the termination of the Agreement, for example if an organisation withdraws, need to be established and documented.

Consideration must be given to the amount of notice the organisation must serve, the management of shared personal data, cancellation of access controls, and notification to other partners.

You also need to consider how you will manage subsequent requests for access to shared data held centrally if the terminated organisation requires it for medico legal purposes or other legal purposes.

****TITLE****

Information Sharing Agreement

THIS AGREEMENT is made on the **xx** day of **Month Year**

B E T W E E N

(1) ****ORGANISATION NAME**** (Data Controller).

(2) ****ORGANISATION NAME**** (Data Controller).

PURPOSE OF SHARING

1.1 The **Organisation Name** will share personal and special categories of personal data with the Data Controller (**Organisation Name**) for the provision of service delivery for the XXXXXXX

1.2 The data shared will identify XXXXXXXXXXXXXXXXXX Schedule
1.3 **Organisation Name** will process the data for the following purposes: -

LEGAL BASIS FOR DATA PROCESSING

2.1 The legal basis for processing personal data is **'GDPR Article 6**
The legislation which provides the statutory function is: -

-

2.2 The legal basis for processing special categories of personal data is **'GDPR Article 9**

WHAT DATA WILL BE SHARED

3.1 **Organisation Name** will share the following categories of data: -

WHEN WILL DATA BE SHARED

4.1 Data will be shared as follows:-

WHO WILL DATA BE SHARED WITH

5.1 Data will be shared with XXXXXXXXXXX.

HOW WILL DATA BE SHARED

6.1 Data will be shared via

XXXXXX@XXXXX

DATA QUALITY

7.1 Prior to sharing data, **Organisation Name** will check the data for accuracy and ensure it is up to date in accordance with their policies and procedures.

DATA SECURITY

8.1 Both parties have a duty to comply with the requirement of the General Data Protection Regulation (GDPR), namely, Article 32 which requires technical and organisational security measures to be implemented to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stores or otherwise processed.

DATA RETENTION AND DESTRUCTION

9.1 The parties will retain the data as part of the patient care record which be retained in accordance with the NHS Records Management Code of Practice for Health and Social Care 2016.

9.2 The parties **have** processes in place to ensure the secure destruction of personal data once it has reached its retention period.

INDIVIDUALS RIGHTS, SUBJECT ACCESS & FOI

10.1 Both parties a duty to comply with the requirement of the General Data Protection Regulation (GDPR), Articles 12 - 22 which requires requests to be responded to within one month.

10.2 Both parties will be responsible for responding to all requests they received regarding the data they hold in accordance with their own organisations policies and procedures.

10.3 Both parties will be responsible for responding to all requests under the Freedom of Information Act in line with their own policies and procedures

DATA BREACHES

11.1 Both parties a duty to comply with the requirement of the General Data Protection Regulation (GDPR), Article 33 which requires organisations to notify the Information Commissioners Office (ICO) of high risk breaches without undue delay and within 72 hours.

11.2 Each party will immediately notify the other upon discovery of data breach during the sharing of personal data.

11.3 The organisation responsible for the data breach will be lead the reporting and investigation in accordance with their own organisations policies and procedures.

REVIEW

12.1 This agreement will be reviewed at least annually by both parties.

SIGNATORIES

13.1 By signing this agreement, all signatories accept and understand their responsibilities for its execution and commit to abide by them.

Signed on behalf of **Organisation Name:**

Name:			
Designation:			
Signature:		**Date:**	

Signed on behalf of **Organisation Name:**

Name:			
Designation:			
Signature:		**Date:**	

Appendix F- Process for Review of a Data Sharing Agreement

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

1 Policy Statements and Purpose of this Data Sharing Agreement

Is the policy statement and the purpose as identified in the DSA still accurate in relation to the present use of the data?

2 Legal Basis for Data Sharing

Do the legal bases in the DSA cover all the parties?

3 What data is it necessary to exchange?

Is the data which is shared by the parties in accordance with the DSA?

4 Who is going to be responsible for exchanging this data and ensuring data is accurate?

Is the contact list up to data and accurate?

5 How will you keep a record of what information has been shared?

How are the parties keeping a record of what information has been shared? Random samples of the data shared could be checked against the source record to see if there is evidence of the data shared

6 How is this information going to be shared?

Is data still being shared in accordance with the DSA?

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 DSA?

8 Timescales

Are any timescales in the DSA being adhered to?

9 How securely does the data need to be stored?

Are all the parties applying the security measures in accordance with the DSA?

10 How long are you going to keep the data?

Are all the parties retaining and destroying the data in accordance with the DSA?

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 DSA 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 have any breaches been dealt with?

13 Indemnity/confidentiality agreements

Is there evidence that any individual who is not covered by an organisation which is a signatory to the DSA has signed a confidentiality agreement and are these held on behalf of the Chair?

14 Freedom of Information Act 2000 (FOIA)

Is this DSA publicly available and also available internally for relevant staff?

15 Requests for Disclosure of Information received under this DSA

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

16 Appropriate Signatories

Is the DSA 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 DSA, any deficiencies should be brought to the attention of the Signatories as appropriate.

Distribution This document has been distributed to:

Name	Title	Date of Issue	Version