INFORMATION SHARING PROTOCOL GENERAL PRACTICES.

CONTENTS

1. Introduction

1.1 This document is a Data 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 GPs and Partner organisations so that members of the public receive the services they need.

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.it can also be a risk when sharing much information, which can in itself lead to a breach and misuse. 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.

2.3 The Protocol applies to the following information:

2.3.1 All personal information processed by the organisations including electronically (e.g. computer systems, CCTV, Audio etc), or in manual records.

2.3.2 Anonymised, including aggregated, personal data. The considerations, though less stringent, must take into account factors such as commercial or business, sensitive 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 Exchange 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 These aims include:

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

b. To explain 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 Exchange Agreements.

e. To support a process, this will monitor and review all data flows.

f. To encourage appropriate flows of data.

g. To protect the Partner Organisations from accusations of wrongful use of sensitive personal 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 1998; (See Appendix B).

c. Develop local Data Exchange Agreements that specify transaction details. (See Appendix E for template).

d. To apply appropriate clinical governance principles, for example NHS Caldicott 2 Principles.

3.4 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 that will be made available to all staff via the Partners' 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 1998
- 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 limited to) consideration of any of the following:

- The Children Act 1989
- The Children Act 2004
- Education Act 2002
- Education Act 1996
- Learning & Skills Act 2000
- Education (SEN) Regulations 2001
- Children (Leaving Care) Act 2000
- Protection of Children Act 1999
- Immigration & Asylum Act 1999
- Local Government Act 2000

- Criminal Justice Act 2002
- Crime and Disorder Act 1998
- National Health Service Act 1977
- Access to Health Records Act 1990
- Health Act 1999
- The Adoption and Children Act 2002
- Health and Social Care Act 2012

5. Data covered by this Protocol

5.1 All personal and anonymised information as defined in the Data Protection Act 1998 (DPA) and as amended by the Freedom of Information Act 2000 (Section 68). **Anonymous data should be used wherever possible.**

5.2 **Personal Information**

5.2.1 The term '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.

5.2.2 The term is further defined in the DPA as:

- Data relating to a living individual who can be identified from those data, or

- Any other information which is in the possession of, or is likely to come into the possession of the data controller (person or organisation collecting that information).

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

5.2.3 The DPA also defines certain classes of personal information as 'sensitive 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 medical data is deemed to be sensitive 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 to produce personal identifiable data including rare medical conditions and unique identifiers such as a single post code.

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, in order 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.

6.6 All staff should follow the procedures and standards that have been agreed and incorporated within this Information Sharing Protocol and any associated Data Exchange Agreements.

6.7 Each Partner Organisation will operate lawfully in accordance with the 8 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 Exchange 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 1998 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 DEA.

8. Consent

8.1 Consent is not the only means by which data can be disclosed. Under the Data Protection Act 1998 in order to disclose personal information at least one condition in schedule two must be met. In order to disclose sensitive personal information at least one condition in both schedules two and three must be met. See Appendix B and Glossary for explanation (Appendix C).

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. 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 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. When using sensitive data, 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, such as Fraser, 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 supplied information and handle the information accordingly.

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

9.4 Every 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 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 have documented policies for retention, weeding 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 (i.e. Section 10 DPA) 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 sixth principle of the Data Protection Act 1998 provides individuals the right to have access to information held about them with limited exemptions. For health these are described within the Data Protection (Subject Access Modification) (Health) Order 2000. Partner Organisations must ensure that only appropriate access to information is granted therefore appropriate procedures must be in place to ensure

individual's rights are met.

10. Individual Responsibilities

10.1 Every individual working for the 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. General Principles

11.1 The principles outlined in this Protocol are 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 Exchange 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 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.

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 Exchange Agreements that will be specific to the Partner Organisations sharing information.

12. Review Arrangements

12.1 This overarching Agreement will be formally reviewed annually by South Warwickshire GP federation, 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

M number	Practice Name	Lead GP (PRINT)	Signature	Date
M84036	Abbey Medical Centre	Dr Prosser (Susan Elizabeth)		
M84049	Alcester Health Centre	Dr Wallis (Andrew James)		
M84617	Arden Medical Centre	Dr Wood (Nigel Charles)		
M84060	Arrow Surgery	Dr Lambert (Richard Anthony)		
M84010	Avonside Health Centre	Dr Carter (John Christopher)		
M84018	Bidford Health Centre	Dr Edwards (Deborah)		
M84014	Bridge House Medical Centre	Dr Allwood (Ian Justin)		
M84069	Budbrooke Medical Centre	Dr White (Henry)		
M84038	Cape Road Surgery	Dr Meadon (Richard William)		
M84013	Castle Medical Centre	Dr Rapley (David Michael)		
M84017	Clarendon Lodge Medical Practice	Dr Fullbrook (John Edward)		
M84015	Croft Medical Centre	Dr Warner (Andrew Phillip)		
M84029	Cubbington Road Surgery	Dr Collins		
M84009	Fenny Compton Surgery	Dr Sharples (Thomas) & Dr Taylor (Jan)		
M84044	Harbury Surgery	Dr Snowdon (Colin Maxwell)		
M84030	Hasting House Surgery	Dr Gunton (Helen)		
M84024	Henley-in-Arden Medical Centre	Dr Taylor (Catherine Mary)		
M84062	Kineton Surgery (Vale of Red Horse)	Dr Kanwar & Dr Layton-Henry (Jenny)		
M84620	Lapworth Surgery	Dr Rowland (Gareth David)		
M84603	Lisle Court Medical Centre	Dr Madagan (Nigel George)		
M84066	Meon Medical Centre	Dr Clarke (Karen Louise)		

M number	Practice Name	Lead GP (PRINT)	Signature	Date
M84002	Pool Medical Centre	Dr Walter (Stephen)		
M84028	Priory Medical Centre	Dr Box (Mark Jolyon)		
M84021	Rother House Medical Centre	Dr Crook (Timothy George Alfred)		
M84040	Sherbourne Medical Centre	Dr Ainsworth (Paul)		
M84025	Shipston Medical Centre	Dr Gilder (Jane)		
M84026	Southam Surgery	Dr Wright (Michael John Andrew)		
M84059	Spa Medical Centre	Dr Pandya (Kirit Kashinath)		
M84608	Studley Health Centre	Dr Buckley (Margaret Patricia)		
M84047	Tanworth in Arden Medical Centre	Dr Green (Keith Nicholas)		
M84063	The New Dispensary	Dr Vara (Nilesh)		
M84043	Trinity Court Surgery	Dr Buckley (David)		
M84070	Warwick Gates Family Health Clinic	Dr Campbell (Francis Stephen)		
M84032	Waterside Medical Centre	Dr Wilkinson (Yvonne)		
M84064	Whitnash Medical Centre	Dr Holtby (Kate Elizabeth)		

APPENDIX B - LEGAL CONTEXT.

THE DATA PROTECTION ACT 1998

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 give individuals or 'data subjects' certain rights with regard to their own personal data. The main standard for processing personal data is compliance with the eight data protection principles summarised as follows:

i) All personal data will be obtained and processed fairly and lawfully.

ii) Personal data will be held only for the purposes specified.

iii) Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held.

iv) Personal data are accurate and where necessary, kept up to date.

v) Personal data will be held for no longer than is necessary.

vi) Personal Data will be processed in accordance with the Rights of the Data Subject.

vii) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

viii) Personal data shall not be transferred to countries outside the European Economic area except in limited circumstances

The first principle states that personal data shall be processed fairly and lawfully and shall not be processed unless at least one Schedule 2 condition and in the case of 'sensitive personal data', at least one Schedule 3 condition is also met.

The type of information being disclosed for the purposes of this exchange agreement may constitute 'sensitive personal data' which means that at least one of both Schedule 2 *and* Schedule 3 conditions must be satisfied.

Even in the event that the *prevention and detection of crime* exemption (Section 29 Data Protection Act) is being relied upon, or other power such as S.115 Crime and Disorder Act, Schedules 2 and 3 conditions must still be satisfied.

Data Protection Act 1998 (Principle 1) Schedules 2 and 3.

The most relevant schedules are:

- The processing is however likely **to be necessary for compliance with any legal obligation** (3), such as the Police Acts and the Local Government Act 2000.
- It is likely that the most relevant condition will be that the processing **is necessary for the exercise of any other functions of a public nature exercised in the public interest by any person (5)(d).**
- The **legitimate interests (6)** condition *may* be appropriate but cases are likely to arise whereby a service user could clearly challenge this, depending upon the circumstances.

The most relevant conditions in Schedule 3 are s3 and s7.

Section 3. The processing is necessary

(a) in order to protect the **vital interests of the data subject, or another person**, in a case where:

(i) consent cannot be given by, or
(ii) on behalf of the data subject, or the data controller cannot

reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on
behalf of the data subject has been unreasonably withheld.

Section 7. (1) Processing is necessary:

(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under an enactment.

Although the aforementioned conditions are likely to apply to any or all of the variable circumstances, it is likely that for the purposes of this exchange agreement one of the additional conditions specified in secondary legislation, for example: S.I No 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000 and (Draft) The Data Protection (Processing of Sensitive Personal Data) Order 2006, may apply.

S.I 417 Data Protection (Processing of Sensitive Personal Data) Order 2000

The Order lists additional circumstances in which sensitive personal data may be processed. For example, it covers processing for the purposes of the prevention or detection of any unlawful act, where seeking the consent of the data subject would prejudice those purposes. It also covers processing required to discharge functions involving the provision of services such as confidential counselling and advice where the subject's consent has not been obtained.

In each of the examples above processing would have to be "in the substantial public interest". This could mean, for example, that processing is necessary to protect public safety or to protect vulnerable people.

Draft S.I Data Protection (Processing of Sensitive Personal Data) Order 2006

The Order specifies that information about a criminal conviction or caution may be processed for the purpose of administering an account relating to the payment card used in the commissioning of one of the listed offences relating to indecent images of children.

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 exchange 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 1998); 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 Exchange Agreement.

POLICE ACT 1996

The Police Act 1996 gives a Constable certain powers. Section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales and Section 30(5) defines these powers as powers under any enactment when ever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the Chief Constable can delegate certain powers to police staff.

In addition, the Code of Practice on the Management of Police Information 2005 defines the policing purpose as:-

- protecting life and property,
- preserving order,
- preventing the commission of offences,
- bringing offenders to justice,
- any duty or responsibility arising from common or statute law

The policing purpose set out in the Code does not replace or supersede any existing duty or power defined by statute or common law. In addition, this does not define every policing activity and does not mean that there is no legal basis for performing such activities. For example, roads policing, public order, counter-terrorism or protection of children or other vulnerable groups while not referred to explicitly are non the less legitimate policing functions.

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 exchange 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 exchange 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 imposes 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 exchange 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 only 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.

Appendix C - Glossary of Terms

Accessible Record – unstructured personal information usually in manual form relating to health, education, social work and housing.

Agent – acts on behalf of the data subject.

Aggregated – collated information in a tabular format.

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, regardless of whether or not they intend to identify the individual is immaterial - in the eyes of the Information Commissioner this is not anonymous data – see **Pseudonymised data**. 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 1998 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/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 or 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 Exchange Agreement – the local information sharing agreement based on the attached template Appendix E.

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

Appendix C: Glossary of Terms Continued…

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

Data Processor – operates on behalf of the Data Controller. Not staff.

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 fifteen EU members together with Iceland, Liechtenstein and Norway.

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

Fully informed implied consent - In order to comply with the Data Protection Act, to validate implied consent if necessary and to satisfy moral obligations, the sender must always strive to fully inform the 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 – In the Data Protection Act 1998 "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 – 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 (including opinion and expression of intention).

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. 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.

Sensitive Personal Data – The DPA defines sensitive personal data as:

(a) the racial or ethnic origin of the data subject;

(b) his/ her political opinions;

(c) his/ her religious beliefs or other beliefs of a similar nature;

(d) whether he/ she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);

(e) his/ her physical or mental health or condition;

(f) his/ her sexual life;

(g) the commission or alleged commission by him/ her of any offence; or

(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Serious Crime – There is no absolute definition of "serious" crime, but section 116 of the Police and Criminal Evidence Act 1984 identifies some "serious arrest-able offences".

Appendix C: Glossary of Terms Continued…

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

Appendix D - Confidentiality Statement

To enable the exchange of information between the constituent practices as detailed in Appendix A and South Warwickshire GP Federation (SWGP Ltd. to be carried out in accordance with the Data Protection Act 1998, 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. Only appropriate information is shared.

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

4. Once the task has been completed the original information and all copies will be destroyed or returned to the GP practice as soon as possible.

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

6. 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.

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

8. 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…….

…….

Copies of this signed agreement are to be held by South Warwickshire GP Federation.

Appendix E Data Exchange Agreement (DEA)
EMIS Enterprise Search & Reports

1. Policy Statements and Purpose of this Data Exchange Agreement

Under this agreement the GP Practices identified in this agreement (refer to signature sheet) agree to share information with South Warwickshire GP Federation (SWGP). This will facilitate the reporting of GP Practice and Federation level activity to support the monitoring of enhanced service contracts and other mutually agreed initiatives where federation level data is deemed beneficial.

Information provided by the Practices shall only be used for the purposes outlined in this Section 1 and will be anonymised, aggregate data, unless explicit consent has been sought and confirmed in writing by all the Parties.

2. Legal Basis for Data Exchange

2.1 The principal legislation concerning the protection and use of information, including Personal Data is:

- The Human Rights Act (1998)
- The Data Protection Act (1998)
- The Freedom of Information Act (2000)
- The Common Law Duty of Confidence.

2.2 The main legal basis upon which information will be shared under the Agreement is:

- Schedule 2 of the Data Protection Act, 1998 (DPA)
  The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

2.3 In performing their respective obligations under the Agreement, the Parties shall comply with the requirements of the DPA and all subordinate and related legislation in force from time to time together with any appropriate guidance published in accordance with the same.

2.4 The Parties shall ensure that all Personal Data which it obtains in the course of performing the obligations under the Agreement is obtained fairly and lawfully, and those individuals or other third party individuals to whom the Personal Data relates are provided with all Fair Processing Information in accordance with the DPA.

2.5 Personal Data will only be processed to the extent, and in such a manner, as is necessary to meet the obligations under the Agreement or as is required by Law.

2.6 The Parties shall ensure that all staff required in the processing of the information obtained and processed under the Agreement are informed of their obligations under the Agreement with regard to the security and protection of the information and that the Parties shall ensure these obligations are complied with within its own organisation.

2.7 The Agreement has been developed to achieve the objectives as set out in Section1. It is the intention that all aspects of information exchange and disclosure relating to the Agreement shall comply with legislation that protects Personal Data.

3. Data

3.1 What data is it necessary to exchange?

READ coded anonymised patient reports split by GP practice that serve the purpose of this agreement outlined in Section 1.

3.2 Staff responsible for exchanging this data

We the undersigned do hereby agree to implement the terms and conditions of this Data Exchange Agreement.
See sign off sheet at foot of document.

3.3 How will you keep a record of what is exchanged?

The SWGP folder within EMIS Population reporting will list all the reports developed as part of this agreement. For each of the reports the GP practice will see the data extracted and the schedule for this extraction.

3.4 How is the information going to be exchanged?

The information will be exchanged via the Search and Reports functionality within EMIS. GP Practices as well as signing this agreement will be required to activate the corresponding data sharing agreement within the EMIS clinical system. This can be activated / deactivated at any point.

3.5 Who will have access to this information and what may they use it for?

- The parties shall ensure that only authorised staff has access to the information shared under this agreement, and shall as appropriate, ensure the reliability of such staff.

- The parties shall ensure that staff only have access to information shared under this agreement or in connection with this agreement, on a justifiable, need to know basis and only to the extent that it is necessary for them to perform their duties in connection with this agreement.

- All information shared under or in connection with the agreement shall be treated as confidential and not disclosed (without prior approval) or used by any staff other than the agreed purposes of this agreement.

3.6 Timescales

The data will be shared as required and will be reviewed annually.

3.7 How is the data securely stored?

- All parties will comply with the seventh principle of the DPA 1998, implementing appropriate technical and organisational measures to protect the information shared under this agreement , against accidental loss, destruction, alteration or disclosure
  These measures shall be appropriate to the harm which might result from any unauthorised access or unlawful processing, accidental loss, destruction or damage to the information and having due regard to the nature of the information that is to be protected.

- Each party signing the agreement agrees to adhere to the agreed standards of security. If there is a security breach in which the data is compromised the Practice will be notified at the earliest opportunity, through the post holder identified in sign off sheet.

3.8 How long are you going to keep the data?

The information will be securely stored within the EMIS system and no patient identifiable data will be kept by SWGP. Anonymous and aggregate data will only be kept for as long as is necessary to support practices with service delivery.

3.9 Further Use of Data

The data and information shall only be used for the purposes outlined in this agreement and for no other purpose unless mutually agreed in writing by all parties.

4 Breach of confidentiality

- The parties shall immediately notify each other of any security breach in relation to the information being obtained or shared in the performance of this agreement and shall keep a record of such breaches.

- The party where the breach has occurred will use its best endeavours to recover such information however it may be recorded.

- The party where the breach has occurred shall conduct a full investigation of the breach and the findings of the investigation will be shared with the other parties.

- All parties shall co-operate fully in any investigation that another party considers necessary to undertake as a result of any breach.

5 Complaints procedures

- Each Party shall have policies and procedures in place to address complaints relating to the inappropriate disclosure or failure to disclose information, including Personal Data. Individuals must be provided with information about these policies and procedures where appropriate.

- The Parties shall provide the other Parties with full co-operation and assistance in relation to any complaint or request made, including, without limitation:

- Providing full details to the other Parties (as appropriate) of the complaint or request

- Complying with data access requests within the relevant timescales set out in the DPA

- Providing the other Parties (as appropriate) with any information that may help in responding to, or resolving the complaint or request.

6 Access to Information

The sixth principle of the DPA provides individuals with the right to access information held about them with limited exceptions.

- The Parties shall ensure that only appropriate access to information is granted.

7 Indemnity

Each partner will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner of any data obtained in connection with this agreement.

8 Review of Data Exchange Agreement

This agreement will be reviewed annually or prior to this if a breach occurs.

9 Closure/termination of agreement

Any partner organisation can suspend this DEA 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 is to take place within 14 days of any suspension.

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

10 Appropriate Signatories

IN WITNESS WHEREOF the Parties have signed this Agreement on the date shown below

Name of Party	Caldicott Signature	Name of Signatory	Position of Signatory	Date
South Warwickshire GP Federation		**Dr Francis Campbell**	**Chair / SIRO**	

Staff responsible for exchanging this data

M number	Practice Name	Lead GP (PRINT)	Signature	Date
M84036	Abbey Medical Centre	Dr Prosser (Susan Elizabeth)		
M84049	Alcester Health Centre	Dr Wallis (Andrew James)		
M84617	Arden Medical Centre	Dr Wood (Nigel Charles)		
M84060	Arrow Surgery	Dr Lambert (Richard Anthony)		

M number	Practice Name	Lead GP (PRINT)	Signature	Date
M84010	Avonside Health Centre	Dr Carter (John Christopher)		
M84018	Bidford Health Centre	Dr Edwards (Deborah)		
M84014	Bridge House Medical Centre	Dr Allwood (Ian Justin)		
M84069	Budbrooke Medical Centre	Dr White (Henry)		
M84038	Cape Road Surgery	Dr Meadon (Richard William)		
M84013	Castle Medical Centre	Dr Rapley (David Michael)		
M84017	Clarendon Lodge Medical Practice	Dr Fullbrook (John)		
M84015	Croft Medical Centre	Dr Warner (Andrew)		
M84029	Cubbington Road Surgery	Dr Collins		
M84009	Fenny Compton Surgery	Dr Sharples (Thomas) & Dr Taylor (Jan)		
M84044	Harbury Surgery	Dr Snowdon (Colin)		
M84030	Hasting House Surgery	Dr Gunton (Helen)		
M84024	Henley-in-Arden Medical Centre	Dr Taylor (Catherine Mary)		
M84062	Kineton Surgery (Vale of Red Horse)	Dr Kanwar & Dr Layton-Henry (Jenny)		
M84620	Lapworth Surgery	Dr Rowland (Gareth David)		
M84603	Lisle Court Medical Centre	Dr Madagan (Nigel George)		
M84066	Meon Medical Centre	Dr Clarke (Karen Louise)		
M84002	Pool Medical Centre	Dr Walter (Stephen)		
M84028	Priory Medical Centre	Dr Box (Mark Jolyon)		
M84021	Rother House Medical Centre	Dr Crook (Timothy George Alfred)		
M84040	Sherbourne Medical Centre	Dr Ainsworth (Paul)		
M84025	Shipston Medical Centre	Dr Gilder (Jane)		
M84026	Southam Surgery	Dr Wright (Michael)		
M84059	Spa Medical Centre	Dr Pandya (Kirit)		
M84608	Studley Health Centre	Dr Buckley (Margaret)		
M84047	Tanworth in Arden Medical Centre	Dr Green (Keith Nicholas)		
M84063	The New Dispensary	Dr Vara (Nilesh)		
M84043	Trinity Court Surgery	Dr Buckley (David)		
M84070	Warwick Gates Family Health Clinic	Dr Campbell (Francis Stephen)		
M84032	Waterside Medical Centre	Dr Wilkinson (Yvonne)		
M84064	Whitnash Medical Centre	Dr Holtby (Kate)		

11. Freedom of Information Act 2000 (FOIA)

"Each Partner Organisation (PO) shall publish this DEA on its website and refer to it within its Publication Scheme. If a PO wishes to withhold all or part of the DEA from publication it shall inform the other PO's as soon as reasonably possible. Partner Organisations shall then endeavour to reach a collective decision as to whether information is to be withheld from publication or not. Information shall only be withheld where, should an application for that information be made under FOIA 2000 it is likely that the information would be exempt from disclosure and the public interest lie in favour of withholding. However, nothing in this paragraph shall prevent the individual Partner Organisations from exercising its obligations and responsibilities under FOIA 2000 as it sees fit.

12. Requests for Disclosure of Information received under this DEA

All recorded information held by public sector agencies is subject to the provisions of the Freedom of Information Act 2000 and the Data Protection Act 1998. While there is no requirement to consult with third parties under FOIA, the parties to this DEA 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.

13. Financial Implications

Any costs in requesting, reviewing, agreeing and managing any DEA will be reviewed and agreed by all signatories.

14 Appropriate Signatories

Each Partner should identify who is the most appropriate post holder within their agency to sign the DEA having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their organisation to the indemnity. It is the responsibility of the individuals identified at 3.2 to ensure that copies of the DEA are made available as necessary to ensure adherence to the DEA.

I confirm that this DEA has been prepared in consultation with the Data Information Governance Team/ Caldicott Guardian (delete as appropriate) **for each signatory.**

South Warwickshire NHS
NHS Foundation Trust

Appendix E Data Exchange Agreement (DEA)

GP record viewing to be available in Emergency Department, Nicholas Ward and Frail ambulatory care area.

1. Policy Statements and Purpose of this Data Exchange Agreement

Under this agreement the GP Practices identified in this agreement (refer to signature sheet) agree to share information with South Warwickshire NHS Foundation Trust (SWFT). This sharing will allow for improving the care and continuing treatment provided by SWFT's Frailty Team to relevant frail patients (over 75's) within the Practices.

Information provided by the Practices relating to individuals shall only be used for the purposes outlined in this Section 1, unless consent has been sought and confirmed in writing by all the Parties.

4. Legal Basis for Data Exchange

2.8 The principal legislation concerning the protection and use of information, including Personal Data is:

- The Human Rights Act (1998)
- The Data Protection Act (1998)
- The Freedom of Information Act (2000)
- The Common Law Duty of Confidence.

2.9 The main legal basis upon which information will be shared under the Agreement is:

- Schedule 2 of the Data Protection Act, 1998 (DPA)
  The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

- Schedule 3 of the DPA
  The processing is necessary for medical purposes and is undertaken by: A health professional

  *A **person** who in the circumstances owes a duty of confidentiality, which is equivalent to that which would arise if that person were a health professional.*

In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

2.10 In performing their respective obligations under the Agreement, the Parties shall comply with the requirements of the DPA and all subordinate and related legislation in force from time to time together with any appropriate guidance published in accordance with the same.

2.11 The Parties shall ensure that all Personal Data which it obtains in the course of performing the obligations under the Agreement is obtained fairly and lawfully, and those individuals or other third party individuals to whom the Personal Data relates are provided with all Fair Processing Information in accordance with the DPA.

2.12 Personal Data will only be processed to the extent, and in such a manner, as is necessary to meet the obligations under the Agreement or as is required by Law.

2.13 The Parties shall ensure that all staff required in the processing of the information obtained and processed under the Agreement are informed of their obligations under the Agreement with regard to the security and protection of the information and that the Parties shall ensure these obligations are complied with within its own organisation.

2.14 The Agreement has been developed to achieve the objectives as set out in Section1. It is the intention that all aspects of information exchange and disclosure relating to the Agreement shall comply with legislation that protects Personal Data.

2.8 With the exception of performance monitoring and evaluation information, the data to be shared will need to be personal confidential data. The information will only be viewed by clinicians directly involved in the patient's care.

2.9 Explicit consent will be asked from the patient (or their authorised representatives) at the point of care to ensure that the sharing of personal data and subsequent processing is fair and lawful. The record will only be opened if the clinician clicks to confirm that the patient has consented, and where there is a need to waive consent e.g. in the case that the patient is unconscious and therefore unable to gain consent, the reason for over-ride will be recorded within the audit record associated with the patient's record.

5. Data

5.1 What data is it necessary to exchange?

The data items to be exchanged are:

Care Record Sharing Details
NHS Number, Date of Birth, Full name, patient demographics
Care Record Summary, including Problems, Medication, Allergies, Alerts, Recent Activity including Appointments and Health Status
Consultations
Medication
Problems

Investigations
History
Diary and Appointments
Attachments
Referrals
Warnings
Free Text

3.2 Staff responsible for exchanging this data

We the undersigned do hereby agree to implement the terms and conditions of this Data Exchange Agreement.
See sign off sheet at foot of document.

3.3 How will you keep a record of what is exchanged?

Full audit data is available in the GP system which details which information was viewed, when and by whom. It also details whether consent was gained, and if not, the reason for over-riding this.
The information from the GP primary care system will be viewed using EMIS EPR Viewer. The reviewer will not be able to amend or alter the primary care record in any way, and it will only be visible to the clinician for a single episode of care, and when the record is closed, the information will no longer be available. Each patient will be asked consent at the time of accessing the record.

3.4 How is the information going to be exchanged?

Information will be provided from the Practices to SWFT via direct access to EMIS (on a read-only basis) using Emis EPR Viewer.

3.5 Who will have access to this information and what may they use it for?

- The parties shall ensure that only authorised staff has access to the information shared under this agreement, and shall as appropriate, ensure the reliability of such staff.

- The parties shall ensure that staff only have access to information shared under this agreement or in connection with this agreement, on a justifiable, need to know basis and only to the extent that it is necessary for them to perform their duties in connection with this agreement.

- All information shared under or in connection with the agreement shall be treated as confidential and not disclosed (without prior approval) or used by any staff other than the agreed purposes of this agreement.

3.10 Timescales

The data will be shared as required and will be reviewed annually.

3.7 How is the data securely stored?

- All parties will comply with the seventh principle of the DPA 1998, implementing appropriate technical and organisational measures to protect the information shared under this agreement , against accidental loss, destruction, alteration or disclosure
  These measures shall be appropriate to the harm which might result from any unauthorised access or unlawful processing, accidental loss, destruction or damage to the information and having due regard to the nature of the information that is to be protected.

- Each party signing the agreement agrees to adhere to the agreed standards of security. If there is a security breach in which the data is compromised the Practice will be notified at the earliest opportunity, through the post holder identified in sign off sheet.

3.11 How long are you going to keep the data?

The information being shared is on a view only basis and as soon as the clinician has left the record the information is no longer available and is not being stored in SWFT.

3.9 Further Use of Data

The data and information shall only be used for the purposes outlined in this agreement and for no other purpose unless mutually agreed in writing by all parties.

7 Breach of confidentiality

- The parties shall immediately notify each other of any security breach in relation to the information being obtained or shared in the performance of this agreement and shall keep a record of such breaches.

- The party where the breach has occurred will use its best endeavours to recover such information however it may be recorded.

- The party where the breach has occurred shall conduct a full investigation of the breach and the findings of the investigation will be shared with the other parties.

- All parties shall co-operate fully in any investigation that another party considers necessary to undertake as a result of any breach.

8 Complaints procedures

- Each Party shall have policies and procedures in place to address complaints relating to the inappropriate disclosure or failure to disclose information, including Personal Data. Individuals must be provided with information about these policies and procedures where appropriate.

- The Parties shall provide the other Parties with full co-operation and assistance in relation to any complaint or request made, including, without limitation:

- Providing full details to the other Parties (as appropriate) of the complaint or request

- Complying with data access requests within the relevant timescales set out in the DPA

- Providing the other Parties (as appropriate) with any information that may help in responding to, or resolving the complaint or request.

9 Access to Information

The sixth principle of the DPA provides individuals with the right to access information held about them with limited exceptions.

- The Parties shall ensure that only appropriate access to information is granted.

- If a Party receives a request under the subject access provisions of the DPA, and the Personal Data is identified as belonging to another Party, the receiving Party will contact the other Party to determine if the latter wishes to claim an exemption under the provisions of the DPA.

7 Indemnity

Each partner will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner of any data obtained in connection with this agreement.

8 Review of Data Exchange Agreement

This agreement will be reviewed annually or prior to this if a breach occurs.

9 Closure/termination of agreement

Any partner organisation can suspend this DEA 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 is to take place within 14 days of any suspension.

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

10 Appropriate Signatories

IN WITNESS WHEREOF the Parties have signed this Agreement on the date shown below

Name of Party	Caldicott Signature	Name of Signatory	Position of Signatory	Date
South Warwickshire NHS Foundation Trust		**Charles Ashton**	**Medical Director**	

Staff responsible for exchanging this data

M number	Practice Name	Lead GP (PRINT)	Signature	Date
M84036	Abbey Medical Centre	Dr Prosser (Susan Elizabeth)		
M84049	Alcester Health Centre	Dr Wallis (Andrew James)		

M number	Practice Name	Lead GP (PRINT)	Signature	Date
M84617	Arden Medical Centre	Dr Wood (Nigel Charles)		
M84060	Arrow Surgery	Dr Lambert (Richard)		
M84010	Avonside Health Centre	Dr Carter (John Christopher)		
M84018	Bidford Health Centre	Dr Edwards (Deborah)		
M84014	Bridge House Medical Centre	Dr Allwood (Ian Justin)		
M84069	Budbrooke Medical Centre	Dr White (Henry)		
M84038	Cape Road Surgery	Dr Meadon (Richard William)		
M84013	Castle Medical Centre	Dr Rapley (David Michael)		
M84017	Clarendon Lodge Medical Practice	Dr Fullbrook (John Edward)		
M84015	Croft Medical Centre	Dr Warner (Andrew)		
M84029	Cubbington Road Surgery	Dr Collins		
M84009	Fenny Compton Surgery	Dr Sharples (Thomas) & Dr Taylor (Jan)		
M84044	Harbury Surgery	Dr Snowdon (Colin Maxwell)		
M84030	Hasting House Surgery	Dr Gunton (Helen)		
M84024	Henley-in-Arden Medical Centre	Dr Taylor (Catherine Mary)		
M84062	Kineton Surgery (Vale of Red Horse)	Dr Kanwar & Dr Layton-Henry (Jenny)		
M84620	Lapworth Surgery	Dr Rowland (Gareth)		
M84603	Lisle Court Medical Centre	Dr Madagan (Nigel)		
M84066	Meon Medical Centre	Dr Clarke (Karen Louise)		
M84002	Pool Medical Centre	Dr Walter (Stephen)		
M84028	Priory Medical Centre	Dr Box (Mark Jolyon)		
M84021	Rother House Medical Centre	Dr Crook (Timothy George Alfred)		
M84040	Sherbourne Medical Centre	Dr Ainsworth (Paul)		
M84025	Shipston Medical Centre	Dr Gilder (Jane)		
M84026	Southam Surgery	Dr Wright (Michael)		
M84059	Spa Medical Centre	Dr Pandya (Kirit)		
M84608	Studley Health Centre	Dr Buckley (Margaret Patricia)		
M84047	Tanworth in Arden Medical Centre	Dr Green (Keith Nicholas)		
M84063	The New Dispensary	Dr Vara (Nilesh)		
M84043	Trinity Court Surgery	Dr Buckley (David)		
M84070	Warwick Gates Family Health Clinic	Dr Campbell (Francis Stephen)		
M84032	Waterside Medical Centre	Dr Wilkinson (Yvonne)		
M84064	Whitnash Medical Centre	Dr Holtby (Kate Elizabeth)		

Appendix F- 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 data 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 the 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 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 DEA has signed a confidentiality agreement and are these held on behalf of the Chair?

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.

Distribution This document has been distributed to:

Name	Title	Date of Issue	Version