Essex Partnership University
NHS Foundation Trust

INFORMATION SHARING & CONSENT POLICY

POLICY REFERENCE NUMBER	CP60
VERSION NUMBER	3.1
KEY CHANGES FROM PREVIOUS VERSION	Minor amendments
AUTHOR	Information Governance Manager
CONSULTATION GROUPS	IGSSC
IMPLEMENTATION DATE	August 2017
AMENDMENT DATE(S)	April 2018; Sept 21; July 2021
LAST REVIEW DATE	November 2020
NEXT REVIEW DATE	November 2023
APPROVAL BY IGSSC	October 2020
RATIFICATION BY QUALITY COMMITTEE	November 2020
COPYRIGHT	

POLICY SUMMARY

This Policy document aims to ensure that all information held by Essex Partnership University NHS Foundation Trust (the 'Trust') about patients / clients / staff is kept secure and is only used / shared for the purpose for which the information was collected, in accordance with legal requirements and best practice

The Trust monitors the implementation of and compliance with this policy in the following ways;

This document should be read in conjunction with service specific information sharing agreements.

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is Executive Medical Director

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION SHARING & CONSENT POLICY

CONTENTS

THIS IS AN INTERACTIVE CONTENTS LIST – CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION SHARING & CONSENT POLICY

Assurance Statement

This Policy document aims to ensure that all information held by Essex Partnership University NHS Foundation Trust (the 'Trust') about patients / clients / staff is kept secure and is only used / shared for the purpose for which the information was collected, in accordance with legal requirements and best practice.

1.0 INTRODUCTION

1.1 Sharing Information can bring many benefits. It can support more efficient, easier access to services. It can help make sure that the vulnerable are given the protection they need, and organisations can co-operate in delivering the care that those with complex needs rely on.

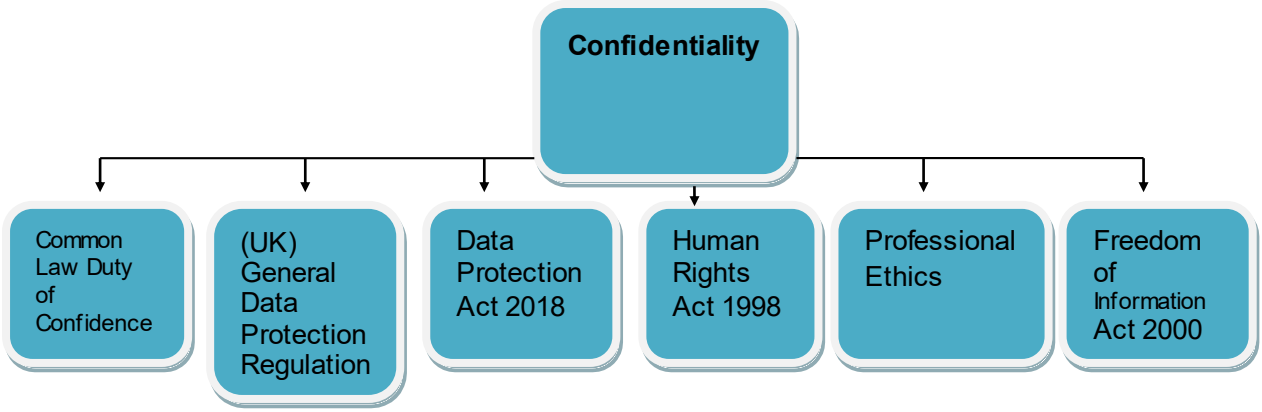
1.2 Sharing information presents risks. Information systems are becoming more complex and widespread. There is a potential for more information about our private lives, often highly sensitive, to become known to more and more people.

1.3 This information sharing policy and procedure sets out the obligations and commitments that staff must follow to ensure that legislation is not breached and patients/clients/families/carers/staff/employees confidentiality is maintained.

1.4 The (UK) General Data Protection Regulation , Data Protection Act 2018, the Common Law Duty of Confidence and Human Rights Act 1998 (Article 8) play a major role in the use, access and protection of information.

1.5 The Freedom of Information Act 2000 gives everyone the right to ask for information held by a public authority, to be told whether the information is held, and, unless exempt, to have a copy of the information.

1.6 The diagram below, Payne (2003), is a visual image of how many legal and statutory requirements fit together. These have been taken into account when producing this policy and procedure and the various information sharing protocols that exist.



2.0 PURPOSE

2.1 The purpose of this policy is:

- To provide a framework to clarify procedures relating to the sharing of information.
- To ensure everyone working with confidential information understands the importance of information sharing, where it improves care for service users and it is for the direct continuing care of service users.
- To ensure that only the minimum information necessary for the purpose should be shared.
- To ensure that when information needs to be shared, that sharing complies with the law, guidance and best practice.
- To ensure that service users' rights are respected.
- To ensure that confidentiality is adhered to unless there is a robust public interest in disclosure or a legal justification to do so.
- To outline the importance and benefits of information governance training.

3.0 DUTIES

3.1 Chief Executive

3.1.1 The Chief Executive is ultimately responsible for the secure storage and confidentiality of all information held within the organisation but the secure transfer of person-identifiable or sensitive information remains with the Caldicott Guardian.

3.2 Caldicott Guardian

3.2.1 The appointed Caldicott Guardian for the Trust must approve transfers of information that relate to the use of sensitive/person-identifiable information.

3.3 Senior Information Risk Owner (SIRO)

3.3.1 The appointed SIRO for the Trust is responsible for the information risk associated with the transfer of information.

3.4 Information Governance Manager

3.4.1 The Information Governance Manager is responsible for co-ordinating improvements in: data protection, the confidentiality code of conduct, and information security.

3.5 The Data Protection Officer

3.5.1 The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.

3.6 **All staff**

3.6.1 All staff who handle information have a responsibility to ensure the information is stored securely and kept confidential at all times. Staff should only have access to information on a strict need to know basis and only as part of their legitimate activity to undertake their job roles.

3.6.2 All information sharing need to have a lawful justification.
Every member of staff contemplating sharing information should refer to the associated policies and procedures. Appendix 3 Consent Guidance for Information Sharing for a short explanation of the following areas:

- What is consent?
- An overview as to when information can and cannot be shared
- Examples of best practice
- The General Data Protection Act Articles 6 & 9
- Contact the Information Governance team for help if unsure.

4.0 DEFINITIONS

4.1 ***What is confidential information?***

4.1.1 Confidential information is information which must not be divulged or shared without permission.

4.1.2 Confidential information is a wide ranging concept which embraces commercial secrets as well as person-identifiable or sensitive information. It can cover a wide range of information and can often have great value.

4.1.3 A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.

- It is a legal obligation that is derived from case law.
- It is a requirement established within professional codes of conduct; and
- It must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures.

4.2 What is person-identifiable Information? (The GDPR applies to both automated personal data and to manual filing systems)

4.2.1 Means any information relation to an identified or identifiable natural person (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:

- Name
- Address
- Telephone Number
- Postcode
- Occupation
- Payroll Number
- Date of Birth
- NHS Number
- National Insurance Number
- Carer's Details
- Next of Kin Details
- Bank Details
- Lifestyle
- Family Details
- Voice and Visual Records (e.g. Photographs, Tape Recordings, CCTV)

(This list is not exhaustive....)

4.3 ***What is sensitive person-identifiable information?***

4.3.1 ***Special categories of personal data"(sensitive) Article 9***

Means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- Health or Physical Condition
- Sexual Life
- Racial or Ethnic Origin
- Religious beliefs
- Political Views
- Criminal Convictions
- Trade Union Membership
- Genetic
- Biometric

(This list is not exhaustive....)

4.3.2 For this type of information even more stringent measures should be employed to ensure that the information remains secure.

5.0 LEGAL DUTIES AND POWERSTO SHARE INFORMATION IN RELATION TO CHILDREN AND YOUNG PEOPLE

5.1 In addition to legislation about information sharing, there are a large number of specific acts of Parliament that give a duty or power to share information about children and young people for various purposes. Appendix 4 gives information about these statutory duties and powers.

6.0 TRAINING

6.1 The Trust will maintain a high level of information governance / security awareness within the organisation by ensuring that all staff receive appropriate, job relevant, training. This may include:

- Team Briefings
- Publications via Electronic bulletins, and others
- Additional On-Line training in the event of a data breach via the Connecting for Health Information Governance website.
- Training via the Trust's e-learning programme (OLM)
- It will be a mandatory requirement for all staff involved in any type of information governance / security breach to complete training, irrespective of previous sessions.
- Training will be done in accordance with the Induction and Mandatory Training Policy.

7.0 MONITORING AND REVIEW

7.1 This document will be reviewed in line with changes in legislation, guidance from Department of Health, the NHS Executive or the Information Commissioner's Office requirements.

7.2 The Executive Medical Director is responsible as the Caldicott Guardian in association with the Executive Chief Finance Officer-SIRO, for the implementation of these procedural guidelines and its associated policy document

8.0 REFERENCE TO OTHER DOCUMENTATION / LEGISLATION

8.1 Related Policies/Procedures:

- Freedom of Information Policy and Procedures
- Information Governance and Security Policy and Procedures
- Records Management Policy and Procedures
- Data Protection and Confidentiality Policy and Procedures

8.2 Related Guidance / Legislation:

- (UK) General Data Protection Regulation
- Respecting Patient Confidentiality – A guide to the use of patient's medical records
- Data Protection Act 2018
- Human Rights Act 2000
- Children's Act 1989
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988 (as amended by the Copyright Computer Programs Regulations 1992)
- Access to Health Records Act 1990 (Where not superseded by the General Data Protection Regulation or Data Protection Act 2018)
- Access to Medical Records Act 1988
- Electronic Communications Act 2000
- Health and Social Care Act 2001 (Section 60)
- NHS Code of Practice: Confidentiality (Dept of Health Guidance)

This list is not exhaustive.

END

APPENDIX 2

Last Name			**First Name**		
NHS No.		**Date of Birth**		**Unit / Ward**	

Form 1.5

CONSENT TO SHARE INFORMATION FORM

Please discuss this form or any queries you may have with your care professional at your clinical assessment appointment.

Please think about whether you will give permission (your consent) to share your information where it is in your best interests.

If you have any further questions please phone the Patient Advice and Liaison Service (PALS) on 0800 085 7935

I have received a copy of the "Your Information - What you need to know" leaflet and have considered the options below.

I, confirm that I give Essex Partnership University NHS Foundation Trust my permission to share any information about me, where it is in my best interests, as follows:

Please tick box:

	To any organisation Essex Partnership University NHS Foundation Trust consider it in my best interests to do so. Such as Social services, General Practitioner, Benefits Agency, Probation, Police, Court Officials, Housing Department, Education Department, Legal Representatives.
	To the following people – please tick all relevant boxes and *please name*

	Next of Kin	
	Nearest Relative	
	Substantive (Main) Carer	
	Carer	
	Family	
	Others	

Are there any exceptions or do you have any specific wishes not covered above

Patient Signature	
Date	

For completion by Care Professional				
Has Patient got Capacity	**Yes**		**No**	

SHARING INFORMATION (Guidance for Patients)

Respecting Your Confidentiality

Essex Partnership University NHS Foundation Trust pledges to respect your confidentiality at all times. This is your right under the law.

This leaflet talks about your health and social care records and the information we hold about you (names, address, date of birth, ethnicity and so on) called personal information.

Our Pledge

Our pledge to you means that

- If a health or social care professional needs to see your records for your treatment they will not pass on any information they read to any unauthorised person
- We will seek your permission if an outside organisation asks to see your records
- We will not pass on any personal information (like your address, phone number or other personal details) to anyone without your permission.
- You can make a complaint if you think confidentiality has been broken
- You can see a copy of your records to make sure they are accurate
- You can ask for all letters written about you to be copied to you.

Sometimes in your best interests it is helpful to share some information with other organisations. This leaflet explains why and how we will ask for your consent.

We have to provide statistics and data to the Department of Health (and similar bodies) about the services we provide but all personal details (or any identifiable information) are removed.

Sharing Health and Social Care Information

We provide many services in partnership with your General Practitioner, other NHS Trusts, Social Care agencies and local authority departments. This means that sometimes we will need to share your health and social care records with others involved in your care or treatment. We have procedures and protocols that govern how we share information which safeguard your right to confidentiality.

Access to Your Health / Social Care Records

The Data Protection Act 2018 gives people who have received NHS and Social Care services the right to access their own personal records. It is important that you trust staff with your personal information and our policy on the use of their information is your guarantee that your personal information will not be passed to others without proper safeguards.

If you would like to know more about how we use your information you can speak to the person in charge of your care or the Trust's Caldicott Guardian.

If you want a leaflet about seeing your records, or how to ask for copies of all letters written about you, please call Patient Advice and Liaison (PALs) on Freephone 0800 085 7935 (Essex & Bedfordshire)

Your Right to Know
Please read this leaflet so that you can understand how we may use information about you. Please ask us if you need any more explanation. You can also help to keep your details up to date by telling us when anything changes in any way, for example if you move home.

What is Personal Information?
This is information about you - your name, address, date of birth. We also take information about your health (you maybe disabled), your family situation (and next of kin), your ethnic origin and religion.

What are Health / Social Care Records?
These are the notes and letters that health and social care professionals write about all aspects of your care and treatment.

Why Does the Trust Keep Records?
The law says we have to, but it also benefits you. Records allow us:

- to understand your needs so we can plan your care
- to make sure we provide high quality care
- to give you a record of what has happened to you
- to train new staff
- to carry out research about developing good quality services.

There are many groups who may provide care for you, each keeping their own information about you. You may be asked to give the same information several times and so sharing your information with these groups, with your permission, will reduce these requests and save your time.

To make sure that your information is safe, groups must sign an agreement with us to treat your information as private and that they will only use it for the purpose of the help they are giving you.

These groups have rules about how they use your information and if they want to they must ask your permission.

At the end of this leaflet there is a consent form where you can tell us what you give us permission to share.

How Does Sharing Information Help Me?
Sharing information means that you won't be asked for the same details so often. Care professionals will not need to keep asking you basic information.

Can I Say No?
Yes you can and you can withdraw your permission at any time. However, please talk to a member of staff about this and any worries you have.

Are There Exceptions or Special Circumstances?
There are limited times when we have to provide information without asking you, for example a Court may order us to do so, or where someone could be in danger or if there has been a serious crime.

What About The Freedom of Information Act?
Personal information is exempt from requests under the Freedom of Information Act.

Can I Limit What Sort Of Information Is Shared?
Yes. In most cases we will tell you what type of information is likely to be shared with others. If there is something or someone you do not want us to pass information onto, we will not do so.

How is My Information Kept Safe?

- We will only share information with other professional organisations that pledge to keep it confidential
- We will only share what is absolutely necessary to make sure your services are delivered safely and effectively
- We use secure computer networks – the general public do not have access to them
- We will keep a record of everyone outside this Trust who has asked to see your information and when and why they did
- It will only be shared where it is in your best interests, not the Trust's or someone else's

What If I Think My Information Is Being Misused?
If you think your personal information is being misused please tell us quickly so that we can take steps to correct the situation.

The Trust has a complaints procedure that can deal with your concerns (see information at the end of this leaflet)

The Caldicott Guardian
Under the law every Trust has to have a senior manager who makes sure that confidentiality is respected throughout the organisation. This is called the Caldicott Guardian (named after the lawyer who chaired an important inquiry into confidentiality). You can write to the Caldicott Guardian about any concerns you may have:

The Caldicott Guardian
Essex Partnership University NHS Foundation Trust
The Lodge
Lodge Approach
Runwell
Wickford, Essex
SS11 7XX

Telephone: 0300 123 0808
E-mail: milind.karale@nhs.net

More Information
If you want a leaflet / more information about:

- making a complaints
- having a copy of your records
- having letters written about you, copied to you
- the Freedom of Information Act
- the Data Protection Act
- anything else

Please call the Patient Advice and Liaison Service on Freephone 0800 085 7935 or 0800 013 1223.

You can make a complaint during office hours by phoning 0300 123 0808.

Essex Partnership University
NHS Foundation Trust

INFORMATION SHARING & CONSENT PROCEDURE

PROCEDURE REFERENCE NUMBER	CPG60
VERSION NUMBER	2.2
KEY CHANGES FROM PREVIOUS VERSION	New section (3.3)
AUTHOR	Information Governance Manager
CONSULTATION GROUPS	IGSSC
IMPLEMENTATION DATE	August 2017
AMENDMENT DATE(S)	Sept 20; July 21; Dec 21
LAST REVIEW DATE	November 2020
NEXT REVIEW DATE	November 2023
APPROVAL BY IGSSC	21st June 2021
RATIFICATION BY QUALITY COMMITTEE:	14 September 2017

PROCEDURE SUMMARY

This Procedure document aims to ensure that all information held by Essex Partnership University NHS Foundation Trust (the 'Trust) about patients / clients / staff is kept secure and is only used / shared for the purpose for which the information was collected, in accordance with legal requirements and best practice.

The Trust monitors the implementation of and compliance with this procedure in the following ways:

This document should be read in conjunction with service specific information sharing agreements

Services	Applicable	Comments
Trustwide	✓	
Essex MH&LD		
CHS		

The Director responsible for monitoring and reviewing this procedure is The Chief Finance & Resources Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION SHARING & CONSENT PROCEDURE

CONTENTS

THIS IS AN INTERACTIVE CONTENTS LIST – PLEASE CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION SHARING & CONSENT PROCEDURE

Assurance Statement

This Procedure document aims to ensure that all information held by Essex Partnership University NHS Foundation Trust (the 'Trust) about patients / clients / staff is kept secure and is only used / shared for the purpose for which the information was collected, in accordance with legal requirements and best practice

1.0 INTRODUCTION

1.1 Sharing Information can bring many benefits. It can support more efficient, easier access to services. It can help make sure that the vulnerable are given the protection they need, and organisations can co-operate in delivering the care that those with complex needs rely on.

1.2 Sharing information presents risks. Information systems are becoming more complex and widespread. There is a potential for more information about our private lives, often highly sensitive, to become known to more and more people.

1.3 This information sharing policy and procedure sets out the obligations and commitments that staff must follow to ensure that legislation is not breached and patients/clients/families/carers/staff/employees confidentiality is maintained.

1.4 The Freedom of Information Act 2000 gives everyone the right to ask for information held by a public authority, to be told whether the information is held, and, unless exempt, to have a copy of the information.

2.0 DECIDING TO SHARE PERSONAL INFORMATION

2.1 Any information sharing must be necessary and any information shared must be relevant and not excessive. Before sharing information you should decide:

- Why you need to share confidential information.
- Do you need to share information in a personally identifiable form or would anonymised, pseudonymised, or statistical information be enough?
- What legal provisions exist that require or permit you to share information?
- Whether any issues might arise as the result of sharing confidential information.
- Is consent from the individual required, and if so how would you obtain consent, what would you do if consent is withheld. (Please see Appendix 2 - Trust Patient Consent Form, this will be completed on the Clinical Systems and uploaded to Health Information Exchange (HIE).

3.0 PROCESS FOR INFORMATION SHARING IN THE TRUST

3.1 In order for the Trust to meet its obligation under the Data Security and Protection Toolkit, information sharing protocols or agreements must be in place with all non NHS organisations (and all NHS organisations outside the Trust's remit). All staff who share confidential information must ensure that a protocol or agreement exists before sharing any information with non NHS Organisations. The Trust Caldicot Guardian and SIRO will review and if appropriate, approve all information sharing protocols and agreements that cover the sharing of corporate or patient information.

3.2 Any information to be shared electronically must first be encrypted or password protected. When submitting information sharing protocols or agreements for consideration, details of the method in which data will be shared must be given to ensure the information is secure in transit.

3.3 Documentation transfer within the Trust requiring a password must follow the password guidance within the password policy.
This requires a complex password that is changed as per policy.
The password must be sent by the safe haven method where it is sent or phoned over to the recipient separately from the document.
This includes departments that send regular documents to several recipients/shared inboxes and staff who have a secretary or personal assistant.

4.0 SECONDARY USES

4.1 Health professionals may receive requests for disclosure of patient information from those not directly involved in the patient's care. Such secondary use of confidential information falls into three broad categories:

- Use within the NHS for administration, planning, audit, commissioning and payment by results.
- Use by agencies commissioned by the NHS to carry out such roles on its behalf.
- Use where confidential information goes beyond healthcare provision in the NHS to include research and education.

4.2 Patient/client/staff/employee data may be disclosed to an appropriate and secure authority and used for secondary purposes if:

- They are required by law.
- The patient/client/staff/employee has given explicit consent.
- The health professional is satisfied, in some limited circumstances that the patient/client/staff/employee is aware of the use and has not objected to it and so has effectively provided implied consent.
- Disclosure is authorised by the Ethics and Confidentiality Committee of the National Information Governance Board under S251 of the NHS Act 2006.

- The health professional is satisfied that the legal and professional criteria for disclosure without consent in the 'public interest' have been met and has sought advice from the Caldicott Guardian, Information Governance Manager , professional body or defence organisation in the case of any doubt.

4.3 In the absence of patient/client/staff/employee consent, anonymised data should be used for any secondary purpose where it is practicable to do so. Some secondary uses of confidential data are for social purposes unconnected with the provision of health care, e.g. for insurance or employment purposes. Such disclosure requires explicit patient/client/staff/employee consent.

5.0 TRAINING

5.1 The Trust will maintain a high level of information governance / security awareness within the organisation by ensuring that all staff receive appropriate, job relevant, training. This may include:

- Team Briefings
- Publications via staff communications, and others
- On-Line training via the Connecting for Health Information Governance website.
- Training via the Trusts' e-learning programme (OLM)
- It will be a mandatory requirement for all staff involved in any type of information governance / security breach to complete training, irrespective of previous sessions.
- Training will be done in accordance with the Induction and Mandatory Training Policy.

6.0 MONITORING AND REVIEW

6.1 This procedural guideline will be reviewed in line with its associated policy document and / or whenever changes in legislation, guidance from NHS Digital, Department of Health, the NHS Executive or the Information Commissioner's Office require.

6.2 The Executive Medical Director is responsible as the Caldicott Guardian in association with the Executive Finance Officer / Senior Information Risk Owner (SIRO) for the implementation of these procedural guidelines and its associated policy document.

7.0 ADDITIONAL GUIDANCE AND CONSIDERATIONS.

What you need to do or consider	Where you can find it in the data sharing code
Identify your objective in sharing the data	• Deciding to share data • Data sharing agreements
Be clear as to what data you are sharing	• Deciding to share data • Data sharing agreements
Understand the position following UK exit from the EU	How is this code affected by the UK's exit from the European Union?
Consider the benefits and risks of sharing and not sharing	• What is the purpose of this code? • The benefits of data sharing • Deciding to share data
Carry out a Data Protection Impact Assessment (DPIA)	Deciding to share data
Put in place a data sharing agreement	• Data sharing agreements • Accountability
Ensure you follow the data protection principles	Data protection principles
Check your data sharing is fair and transparent	Fairness and transparency
Identify at least one lawful basis for sharing the data before you start sharing it	• What is our lawful basis for sharing? • Lawful basis for sharing personal data
Put in place policies and procedures that allow data subjects to exercise their individual rights easily	• What about access and individual rights? • The rights of individuals • Law enforcement processing

Be clear about sharing data under the law enforcement processing provisions of Part 3 DPA 2018, and sharing between the UK GDPR/Part 2 DPA 2018 and Part 3 DPA 2018		Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the UK GDPR and Part 2 DPA 2018
Demonstrate a compelling reason if you are planning to share children's data, taking account of the best interests of the child		Data sharing and children
Share data in an emergency as is necessary and proportionate. Plan ahead as far as possible		Data sharing in an urgent situation or in an emergency
Document your decisions about the data sharing, evidencing your compliance with data protection law		• Accountability • Data sharing agreements
Put in place quality checks on the data		What information governance arrangements should we have?
Arrange regular reviews of the data sharing arrangement		• When should we review a data sharing arrangement? • Accountability
Agree retention periods and make arrangements for secure deletion		• Security • Accountability

END

Extract from the General Data Protection Regulation

Art. 5 GDPR Principles relating to processing of personal data

1. Personal data shall be:

    1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

    4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

    5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

    6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Art. 6 GDPR Lawfulness of processing

1. [1]Processing shall be lawful only if and to the extent that at least one of the following applies:

    1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

    2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

    3. processing is necessary for compliance with a legal obligation to which the controller is subject;

    4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[2]Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. [1]The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

   1. Union law; or

   2. Member State law to which the controller is subject.

   [2]The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. [3]That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. [4]The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

   1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

   2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

   3. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

   4. the possible consequences of the intended further processing for data subjects;

   5. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Art. 7 GDPR Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. [1]If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. [2]Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. [1]The data subject shall have the right to withdraw his or her consent at any time. [2]The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. [3]Prior to giving consent, the data subject shall be informed thereof. [4]It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Art. 9 GDPR Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

    1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

    2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

    3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

    4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

    5. processing relates to personal data which are manifestly made public by the data subject;

    6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

END

Essex Partnership University
NHS Foundation Trust

INFORMATION FOR PATIENTS / CARERS / RELATIVES ON SHARING INFORMATION

CORE INFORMATION FOR PATIENTS

- We *ask* you for information so that you can receive proper care and treatment.
- We *keep* this information, together with details of your care, because it may be needed if we see you again.
- We *may use* some of this information for other reasons: for example, to help us protect the health of the public generally and to see that the NHS runs efficiently, plans for the future, trains its staff, pays its bills and can account for its actions.
- Information may also be needed to help educate tomorrow's clinical staff and to carry out medical and other health research for the benefit of everyone.
- Sometimes the law requires us to *pass on* information: for example, to notify a birth.
- The NHS Central Register for England & Wales contains basic personal details of all patients registered with a general practitioner. The Register does not contain clinical information.

You have a right of access to your health records

EVERYONE WORKING FOR THE NHS HAS A LEGAL DUTY TO KEEP INFORMATION ABOUT YOU CONFIDENTIAL.

You may be receiving care from other people as well as the NHS.
So that we can all network together for your benefit we may need to share some information about you.
We only ever use or pass on information about you if people have a genuine need for it in your and everyone's interests. Whenever we can we shall remove details which identify you.
Anyone who receives information from us is also under a legal duty to keep it confidential.
If you agree, your relatives, friends and carers will be kept up to date with the progress of your treatment.

THE MAIN REASONS FOR WHICH YOUR INFORMATION MAY BE NEEDED ARE:

- **Health care and treatment**
- **Looking after the health of the general public**

Managing and planning the NHS, e.g.

- making sure that our services can meet patient needs in the future
- paying your doctor, nurse, dentist, or other staff, and the hospital which treats you for the care they provide
- auditing accounts
- preparing statistics on NHS performance and activity (where steps will be taken to ensure you cannot be identified)
- investigating complaints or legal claims

Helping staff to review the care they provide to make sure it is of the highest Standard

- **Training and educating staff** (but you can choose whether or not to be involved personally)
- **Research** approved by the Local Research Ethics Committee. (If anything to do with the research would involve you personally, you will be contacted to see if you are willing)

If at any time you would like to know more about how we use your information you can speak to the person in charge of your care or to the Information Governance Team or Data Protection Officer.

Essex Partnership University
NHS Foundation Trust

CPG60 – Appendix 1

INFORMATION SHARING PROTOCOL

Title of Agreement				
Organisation Name	**Head Office Address**	**Telephone**	**Email**	**ICO Registration reference**
Essex University Partnership NHS Foundation Trust	The Lodge, Lodge Approach, Runwell Wickford Essex SS11 7XX	01268 407737	Epunft.info.gov@nhs.net	ZA242481

Version Control	
Date Agreement comes into force	
Date of Agreement review	
Agreement owner (Organisation)	
Agreement drawn up by (Author(s))	
Status of document – DRAFT/FOR APPROVAL/APPROVED	
Version	

Essex Partnership University
NHS Foundation Trust

Information Sharing Protocol

1. Purpose

The parties have entered into this Information Sharing Agreement to facilitate and enable the smooth transition of Information Sharing between them. The Information Sharing Agreement is a requirement of the DSPT and also meets the best practice guidance of the Information Commissioner's Data Sharing Code of Practice. This could consist of data being transferred just once or on an ongoing regular basis, as agreed by the parties involved.

Benefits to the patient will include:

Benefits to the patient will include timelier sharing of information between EPUT and …….

2. Information to be shared

The types of information listed above is not exhaustive and additional information can be shared if certain criteria is met and this will be considered on a case by case basis, as appropriate.

3. Legal Basis for Sharing information

The purpose of this information sharing agreement is to provide a detailed process for information sharing between/for the …….. service/ organisations

This information Sharing Agreement is entered into for the purpose of the parties sharing information as required or permitted under the data protection legislation and any other relevant legislation which shall include (but not limited to:

- Data Protection Act 2018
- General Data Protection Regulation 2016
- Freedom Of Information Act 2000
- Human Rights Act 1998
- Mental Health Act 1983
- Health and Social Care Act 2012
- Mental Capacity Act 2015
- HSCIC Guide To Confidentiality
- Information Governance/Caldicott 2 Review: to share or not to share
- Records Management NHS Code or practice
- NHS England Safe Haven Procedure
- NHS Constitution
- Information Security Management: Code Of Practice

- Data Sharing Code Of Practice
- Privacy Notices Code Of Practice
- Any Other Relevant Legislation, Standards or Guidance

The parties acknowledge and agree that they will share information whenever either or both parties are under a statutory duty to do so. In this case, the party requesting the information shall make clear in its Data Securing Request the legislation underpinning the request for information and the disclosure of information shall comply with the relevant legislation and be made in accordance with the terms of this Information Sharing Agreement, if applicable.

The parties acknowledge and agree that they will not be bound by the terms of this Information Sharing Agreement in the event either or both of them are prohibited to share information by any legislation.

If consent is deemed to be required for the sharing of personal data, this will be a transparent process.

Where it has been identified that the parties are permitted to share information without obtaining consent, this should be justified, if required, under their statutory or legal powers. Data subjects should be made aware of this decision and provided with the details of the data share, unless, by doing this will risk harm to others or hinder any investigation or legal proceeding.

The decision to share information without consent will be fully documented and held within the patients 'care record'.

It is good practice to seek freely given, specific, informed and valid consent of individuals to share their information. However disclosure may be lawful in certain circumstances without consent, for example the performance of public functions, legal obligations, prevention/detection of crime.

(Explain the legal power(s) you have that allow you to share the information – include how the sharing is consistent with the ***General Data Protection Regulation 2016*** *(GDPR)).*

Personal Data	**Special Categories of Data**
Sharing personal information in accordance with this protocol is lawful under the *General Data Protection Regulation 2016* article 6(dropdown)	Sharing personal information in accordance with this protocol is lawful under the *General Data Protection Regulation 2016* article 9: (if appropriate): *[please complete]*:
Vital Interests	*Article 9(2)(h)*
Legitimate Interests	

Other legislation or statute as follows
Children's Act 2004, Section 10 & 11- Cooperation to improve well-being.
Children's Act 1989. Part III: Section 17 (1) (provision of service)

Fair Processing in accordance with *General Data Protection Regulation 2016* article 12.

Fair processing requirements have been satisfied by:
Information of both parties' Fair Processing Notices being either fully available on their respective publicly available websites or available on request (via electronic or hardcopy):

The information listed above will be available to the data subjects in the following methods:

- Your health records: what you need to know (EPUT leaflet)
- Your health records: what you need to know (EPUT Poster)
- ...
- ...

4. Access and individuals' rights

(Explain what to do when an organisation receives a DPA or FOI request for access to shared data).

Subject Access is an individual's right to have a copy of information relating to them which is processed by an organisation.

Once information is disclosed from one agency to another, the recipient organisation becomes the **Data Controller** for that information. With regards to subject access requests, the **Data Controller** has a statutory duty to comply with Article 15, unless an exemption applies. It is good practise for the recipient organisation to contact the originating organisation. This enables the originating organisation to advise the use of any statutory exemptions that may need to be applied prior to disclosure to the requesting individual.

If a party receives a request for information under the Freedom of Information (FOI) Act [2000] that relates to data that has been disclosed for the purposes of this Information Sharing Protocol, it is best practice to seek advice from the originating organisation prior to release. This allows the originating organisation to rely on any statutory exemption under the provisions of the FOI Act and to identify any perceived harms. However, the decision to release data under the FOI Act is the responsibility of the agency that received the request.

5. Keeping information secure

All information shared between the parties involved in this ISP will be held in a secure location with limited access and used only for the purposes listed in this agreement.

- Each party shall ensure that access to information provided by the other party under this ISP will only be granted to those staff who 'need to know' the information.
- The information shared between the parties must not be disclosed to any third party.
- All information held on portable devices must be encrypted to industry standard FIPS 140-2/256-bit asymmetrical encryption
- All data will remain and be stored on servers physically located within the United Kingdom.

Security for the exchange of information will be achieved through a secure - fill in exchange type (e.g. secure site, secure nhs.mail to nhs.mail)

Partners receiving information will:

- Ensure their employees can only access the shared information appropriate to their role;
- Ensure that their employees of appropriately trained to understand their responsibilities to maintain confidentiality and privacy;
- Protect the physical security of the shared information.

6. Information format and frequency of sharing

The format the information shared is either in - insert format type here (e.g. Microsoft excel or csv file).

The frequency with which the information will be shared is a (……) transfer of information.

7. Data Retention

(Include detail here how long each organisation will retain the information for).

Information will be retained in accordance with each partners' data retention policy and in any event no longer than is necessary.

For the purposes of this agreement, destruction means that data must be irretrievable following destruction or deletion, in accordance with ISO27001 international standard for information security.
The controller will retain information in accordance with the Department of Health's retention of records schedules.
The processor must not make multiple copies of the data.

The processor shall ensure that the destruction of data will also take place for backup media and provide written confirmation to the controller when destruction has taken place.

8. Responsibility for exchanging these data and ensuring data are accurate

Each of the data providers will ensure the accuracy of the data being shared using their own internal quality assurance checks.

For the purposes of this Protocol the responsibilities are defined as:
Caldicott Guardians and Senior Information Risk Owners (SIRO) who have signed the Information Sharing Agreement as having overall responsibility within their own organisation have the duty for ensuring the organisation has the necessary powers to share the information requested. Any information shared must only be used for the purpose as requested.
The parties in discharging their obligations under this information sharing agreement shall comply with the eight data protection principles.
The parties shall ensure that the information shared is relevant and proportionate to the purpose for which it is shared and will comply with the Data Protection Act, information will not be passed to any third party other than allowed by law, retention for the intelligence purposes shall be allowed but only in line with the Data Protection Act.

EPUT have/have not undertaken a privacy impact assessment as under this information sharing agreement information will be shared only where the parties are legally required or permitted to do so.
All parties involved have agreed that the service users (data subjects) need to be informed of the following:

- What information is going to be shared
- In what format is the data going to be exchanged
- Who the information is going to be shared with
- For what purposes it will be used

Unless by doing so would risk harm or self to others or hinder any investigation or legal proceedings.

Data Controllers for this Protocol are:

Joint Data Controllers for this Protocol are:
["Joint" covers the situation where the determination is exercised by data controllers acting together, typically with written data controller agreements1 setting out the purposes for processing, the manner of processing and the means by which joint data controller responsibilities will be satisfied. The participation of the parties may take different forms and need not necessarily be equally shared across all aspects of the processing. Their contributions may be sequential or simultaneous and their liability if something goes wrong may differ.]

Data Controllers in Common for this Protocol are:
["In common" is where data controllers share a pool of personal data, often disclosing data to each other but with each processing the data independently of the other(s). As with 'joint' arrangements, data controllers in common should have written agreements and processes for ensuring that all data controller responsibilities are satisfied. Each needs to exercise due diligence in ensuring that all parties involved are meeting the requirements of law.]

Data Processors are:
[A data processor can be anyone (other than an employee of the data controller) who processes the data on behalf of the data controller. The Act imposes specific obligations upon data controllers when the processing of personal data is carried out on their behalf by data processors.

Where Data Processors are a part of this Protocol, the data controller retains full responsibility for the actions of the data processor – if there is a data protection breach then the data controller remains responsible. The key obligation is that the processing by a data processor must be carried out under a written contract which requires the data processor to act only on instructions from the data controller. In the absence of a written contract a Partner to this protocol will be a data controller in its own right and will need to meet all the requirements of the Data Protection Act 2018 and the General Data Protection Regulations 2016.

9. Complaints

Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.

10. Breach of Confidentiality

(Provided detail here of what the expectation in the event of a breach of the data sharing initiative. Including who should be contacted and reporting timescales).

Any reported potential or actual breach of security or inappropriate / unauthorised disclosure of data will be investigated. It is the responsibility of the Data Provider to report the incident following its own internal reporting processes for data breaches.

11. Agreement

We undertake to implement and adhere to this protocol.

Signed by Governance Lead

Print:……

Signed:……..……

On behalf of
(Organisation):……..……..

Signed by Governance Lead

Print:……

Signed:……..……

On behalf of
(Organisation):……..……

Signed by Governance Lead

Print:……

Signed:……

On behalf of
(Organisation):……

Definitions

GDPR	General Data Protection Regulation
DPA	The Data Protection Act
FoIA	Freedom of Information Act
Personal Information	"Personal Data" as defined in the above DPA GDPR
Personnel	Partner organisations' employees, officers, elected members, directors, voluntary staff Consultants and other contractors and their sub-contractors
Sensitive personal data	As defined in the above DPA GDPR
Service users	Recipients of the partner organisations' health and care services. Also known as "data subjects" within the meaning of the DPA 2018 / GDPR
ISA's	Information Sharing Agreements
PIA/DPIA	Privacy impact assessments Data Privacy Impact Assessments
SIRO	Senior Information Risk Owner

Appendix 3

CONSENT GUIDANCE FOR INFORMATION SHARING

1. Introduction

The aim of this document is to give guidance to enable personal information concerning service users to be shared between organisations without compromising confidentiality unless there is a legal requirement, or an overriding public interest to do so.

Confidentiality is an essential requirement for the preservation of trust between service users and health professionals and is subject to legal and ethical safeguards. Service users should be able to expect that information about their health which they give in confidence will be kept confidential unless there is a compelling reason why it should not. There is also a strong public interest in maintaining confidentiality so that individuals will be encouraged to seek appropriate treatment and share information relevant to it.

As a general principle all personal information must only be collected, held and shared on a strict 'need to know' basis and all decisions to share information that are not directly associated with the direct continuing healthcare of the patient should be recorded.

2. Purpose

The purpose of this document is to provide specific guidance for all staff on consent and information sharing issues. This document forms an appendix to the Trust's Information Sharing & Consent Policy and Procedure.

3. Consent

Consent is required in all cases of sharing service user identifiable information unless disclosure is required by law, or there is an overriding public interest in disclosure.

3.1 Definition of Consent

Consent to disclosure may be explicit or implied. It may also be consent to disclosure of specific information to a particular person or body for a particular purpose or it may be consent to general future disclosure for particular purposes. In either case consent should be informed and freely given.

Consent is defined in "Confidentiality: NHS Code of Practice (2003) as follows:

(a) Informed Consent

All consent should be fully informed. Every patient should be informed about what happens to the information they give to the NHS (it is the minimum requirement under the General Data Protection Regulation). For each episode of care you should ensure that your service user is aware of who will see their information and what you will be doing with it and give them the

opportunity of saying 'no' to information sharing, unless legislation dictates otherwise.

All service users should receive the following information:

- Who the Data Controller is
- Why the information is needed
- The purposes for which the information will be processed
- Who will see the information
- Any disclosures that may need to be made to other organisations (e.g. Acute Hospitals, Social care, Clinical audit, GP, Mental Health Teams, Drug Teams etc)
- The circumstances in which information may be disclosed without consent, where there is an overriding public interest (e.g. child protection, or serious crime.)
- Information restricted by legislation (e.g. serious communicable diseases.)
- Information that must be passed on because of legislation (e.g. births, deaths, cancer registries, abortion.)

If service users have any reservations about information sharing then explain that the direct continuing care could be affected by restrictions placed on sharing. If service users still refuse to share any information then you have not gained consent for that particular information and the service user's wishes must be respected (unless there is a legal requirement, or an overriding public interest in disclosure.)

(b) Implied Consent

Service user agreement that has been signalled by behaviour (this consent also needs to be fully informed).

Implied consent is not a lesser form of consent but in order for it to be valid it is important that service users are made aware that information about them will be shared, with whom it will be shared, and of their right to refuse. Health professionals bear responsibility for the disclosures they make, so when consent is taken to be implied, they must be able to demonstrate that the assumption of consent was made in good faith and based on good information. If not, it is no consent at all and some other justification will be needed for its disclosure. In addition to information provided face to face in the course of a consultation, leaflets, posters and information included with an appointment letter can play a part in conveying to service users the reality and necessity of information sharing. Implied consent is usually sufficient for direct service user care (see paragraph 4.1 below).

(c) Express/Explicit Consent

Articulated service user agreement. Clear and voluntary indication of preference or choice, usually given orally or in

writing and freely given in circumstances where the available options and the consequences have been made clear. Explicit consent is the ideal as there is no doubt as to what has been agreed.

3.2 Recording Consent

Record in the service user's record if the service user has been provided with and understands the notice/leaflet regarding information sharing and has not said 'no' to sharing any part of their information.

Where a service user has refused to share information this should be recorded in the service user's record, dated and time stamped. That information must not be shared (unless there is a legal requirement or an overriding public interest in disclosure.)

3.3 Keeping Consent Up To Date

It is essential that children, once they gain capacity, are asked to confirm their own choice, as a previous recorded choice regarding consent will have been made by another party, on their behalf, which may not reflect their own choice.

It may also be essential to revisit the consent at other times e.g. when changes which impact on how information is used are introduced. Consent should also be reviewed whenever there are changes to information sharing/disclosure during an episode of care.

4. What You Need To Know Before Sharing Information

4.1 Sharing Information With Other Health Professionals

In the absence of evidence to the contrary, service users are normally considered to have given implied consent for the use of their information by health professionals for the purpose of the care they receive. Information sharing in this context is acceptable to the extent that health professionals share what is necessary and relevant for service user care on a 'need to know' basis. Healthcare and social care although often closely related, do not always fall into the same category, and disclosures of information to social care usually require explicit consent from competent service users. Sometimes two competing interests come into conflict, such as the service user's informed refusal to allow disclosure, and the need to provide effective treatment to that person. A service user's refusal to allow information sharing with another health professional may compromise service user safety, but if this is an informed decision by a competent person it should be respected.

4.2 Multi – Agency Working

Health professionals during the course of their treatment of service users will have contact with partner organisations from time to time. These include social care, housing and benefits agencies. Health professionals should from the outset discuss with service users the desirability of sharing information with other agencies as appropriate.

Other agencies may wish to be involved in discussions about service users at various points in their treatment, or to attend case conferences, or multi- disciplinary meetings. Health professionals may also be invited to attend external case conferences organised by partner organisations to discuss the health and welfare of service users. In all these circumstances information sharing should take place with explicit consent or in the absence of explicit consent where disclosure is required by law, or there is an overriding public interest in disclosure.

4.3 Assessment Of Capacity

All people aged 16 and over are presumed, in law, to have the capacity to give or withhold their consent to disclosure of confidential information unless there is evidence to the contrary. A service user who is suffering from a mental disorder or impairment does not necessarily lack the capacity to give or withhold their consent. Equally, service users who would otherwise be competent may be temporarily incapable of giving valid consent due to factors such as extreme fatigue, drunkenness, shock, fear, severe pain or sedation. The fact that an individual has made a decision that appears to others to be irrational or unjustified should not be taken on its own as conclusive evidence that the individual lacks the mental capacity to make that decision. If, however, the decision is clearly contrary to previously expressed wishes, or is based on a misperception of reality, this may be indicative of a lack of capacity and further investigation will be required.

There is no presumption of capacity for people under 16 in England, and Wales, and those under this age must demonstrate their competence by meeting certain standards set by the courts. The central test is whether the young person has sufficient understanding and intelligence to understand fully what is proposed.

To demonstrate capacity individuals should be able to:

- Understand in simple language (with the use of communication aids, if appropriate) what is to be disclosed and why it is being disclosed
- Understand the main benefits of disclosure
- Understand, in broad terms, the consequences of disclosure
- Retain the information long enough to use it and weigh it in the balance in order to arrive at a decision
- Communicate the decision (by any means)
- Make a free decision (i.e. free from undue pressure)

4.4 Adults Who Lack Capacity

4.4.1 Temporary Or Permanent Mental Incapacity

Service users with mental disorders or learning disabilities should not automatically be regarded as lacking the capacity to give or withhold their consent to disclosure of confidential

information. Unless unconscious, most people suffering from a mental impairment can make valid decisions about some matters that affect them. An individual's mental capacity must be judged in relation to that particular decision being made. If therefore a service user has the requisite capacity, disclosure of information to relatives or third parties requires service user consent. One of the most difficult dilemmas for health professionals occurs where the extent of such service user's mental capacity is in doubt. In such cases health professionals must assess the information which is available from the service user's health record and from third parties. They should attempt to discuss with service users their needs and preferences as well as assess their ability to understand their condition and prognosis. If there is still doubt about a service user's competence to give or withhold consent, health professionals should seek a second opinion.

4.4.2 Relatives, Carers And Friends

If a service user lacks capacity, health professionals may need to share information with relatives, friends or carers to enable them to assess the service user's best interests. Where a service user is seriously ill and lacks capacity, it would be unreasonable always to refuse to provide any information to those close to the service user on the basis that the service user has not given explicit consent. This does not, however, mean that all information should be routinely shared, and where the information is sensitive, a judgement will be needed about how much information the service user is likely to want to be shared, and with whom. Where there is evidence that the service user did not want information shared, this must be respected.

4.4.3 Next Of Kin

Although widely used, the phrase 'next of kin' has no legal definition or status. If a person is nominated by a service user as next of kin and given authority to discuss the service user's condition, such a person may provide valuable information about the service user's wishes to staff caring for the service user. However, the nominated person cannot give or withhold consent to the sharing of information about the service user and has no rights of access to the service user's medical records. The service user may nominate anyone as next of kin. In the absence of such a nomination, no-one can claim to be next of kin.

4.4.4 Proxy Decision-Makers

In England and Wales, the Mental Capacity Act 2005 allows people over 18 years of age who have capacity to appoint a welfare attorney to make health and personal welfare decisions once capacity is lost. The Court of Protection may also appoint a deputy to make these decisions. Where a service user lacks

capacity and has no relatives or friends to be consulted, the Mental Capacity Act requires and Independent Mental Capacity Advocate to be appointed and consulted about all decisions about 'serious medical treatment', or place of residence. An attorney or deputy can also be appointed to make decisions relating to the management of property and financial affairs. In the case of health information, health professionals may only disclose information on the basis of the service user's best interests.

4.4.5 Abuse And Neglect

Where health professionals have concerns about a service user lacking capacity that may be at risk of abuse or neglect, it is essential that these concerns are acted upon and information is given promptly to an appropriate person or statutory body, in order to prevent further harm. Where there is any doubt as to whether disclosure is considered to be in the service user's best interests, it is recommended that the health professional discusses the matter on an anonymised basis with a senior colleague, the Caldicott Guardian, Information Governance Manager or Trust Solicitor. Health professionals must ensure that their concerns and the actions they have taken or intend to take, including any discussion with the service user, colleagues or professionals in other agencies, are clearly recorded in the service user's medical records

4.5 Children And Young People

4.5.1 Competent Children

There is no presumption of capacity for people under 16 in England, Wales and Northern Ireland and those under that age must demonstrate they have sufficient understanding of what is proposed. However, children who are aged 12 or over are generally expected to have capacity to give or withhold their consent to the release of information. Younger children may also have sufficient capacity. When assessing a child's capacity it is important to explain the issues in a way that is suitable for their age. If the child is competent to understand what is involved in the proposed treatment, the health professional should, unless there are convincing reasons to the contrary, for instance abuse is suspected; respect the child's wishes if they do not want parents or guardians to know. However, every reasonable effort must be made to persuade the child to involve parents or guardians particularly for important or life-changing decisions.

4.5.2 Children Who Lack Capacity

The duty of confidentiality owed to a child who lacks capacity is the same as that owed to any other person. Occasionally, young people seek medical treatment, for example, contraception, but are judged to lack the capacity to give

consent. An explicit request by a child that information should not be disclosed to parents or guardians, or indeed to any third party, must be respected except in the most exceptional circumstances, for example, where it puts the child at risk of significant harm, in which case disclosure may take place in the 'public interest' without consent. Therefore, even where the health professional considers a child to be too immature to consent to the treatment requested, confidentiality should still be respected concerning the consultation, unless there are very convincing reasons to the contrary. Where a health professional decides to disclose information to a third party against a child's wishes, the child should generally be told before the information is disclosed. The discussion with the child and the reasons for disclosure should also be documented in the child's record.

4.5.3 Parental Responsibility

Anyone with parental responsibility can give or withhold consent to the release of information where the child lacks capacity. Not all parents have parental responsibility.

- In relation to children born after 1 December 2003, both of a child's biological parents have parental responsibility if they are registered on a child's birth certificate.
- In relation to children born before these dates, a child's biological father will only automatically acquire parental responsibility if the parents were married at the time of the child's birth or some time thereafter. If the parents have never been married, only the mother automatically has parental responsibility, but the father may acquire that status by order or agreement. Neither parent loses parental responsibility on divorce.
- Where the child has been formally adopted, the adoptive parents are the child's legal parents and automatically acquire parental responsibility.
- Where the child has been born as a result of assisted reproduction, there are rules under the Human fertilisation and Embryology Act 2008 that determine the child's legal parentage.
- In some circumstances people other than parents acquire parental responsibility, for example by the appointment of a guardian or on the order of a court.
- A local authority acquires parental responsibility (shared with the parents) while the child is the subject of a care or supervision order.
- In some circumstances parental responsibility can be delegated to other carers such as grandparents and child-minders.

If there is doubt about whether the person giving or withholding consent has parental responsibility, legal advice should be sought.

Where an individual who has parental responsibility refuses to share relevant information with other health professionals or agencies and the health professional considers that it is not in the best interest of the child (for example, it puts the child at risk of significant harm), disclosure may take place in the public interest without consent.

4.5.4 Safeguarding Children

Where health professionals have concerns about a child who may be at risk of abuse or neglect, it is essential that these concerns are acted upon and information is given promptly to an appropriate person or statutory body, in order to prevent further harm. The best interests of the child or children involved must guide decision-making at all times. Knowing what to do when service users do not want confidential information disclosed, despite this being the best way to ensure that they do not suffer harm or abuse, is very difficult for health professionals. Health professionals should not make promises to the child about confidentiality that they may not be able to keep but, as in the case of any service user, trust is best maintained if disclosure is not made without prior discussion between the health professional and the child, unless to do so would expose the child or others to an increased risk of serious harm.

Where there is any doubt as to whether disclosure is in the child' best interests, it is recommended that the health professional discusses the matter anonymously with an experienced colleague, Safeguarding Children and Families Team, the Caldicott Guardian, Information Governance Manager, Trust Solicitor, their professional body or defence body.

Health professionals must ensure that their concerns, and the actions they have taken, or intend to take, including any discussion with the child, colleagues or professionals in other agencies, are clearly recorded in the child's medical record. Health professionals may be involved in case reviews for which the child's records may need to be disclosed, but care should be taken not to disclose the notes of other family members without consent unless it can be justified in the public interest.

4.6 Best Interests

All decisions taken on behalf of someone who lacks capacity must be taken in their best interest. A best interest judgement is not an attempt to determine what the service user would have wanted. It is as objective a test as possible of what would be in the service user's

actual best interests, taking into account all relevant factors. A number of factors should be addressed including:

- The service user's own wishes (where these can be ascertained)
- Where there is more than one option, which option is least restrictive of the service user's future choices
- The view of the parents, if the service user is a child
- The views of people close to the service user, especially close relatives, partners, carers, welfare attorneys, court-appointed deputies or guardians, about what the service user is likely to see as beneficial

4.7 Public Interest

4.7.1 General Principles

In the absence of service user consent (a legal obligation or anonymisation) any decision as to whether identifiable information is to be shared with third parties must be made on a case by case basis and must be justifiable in the 'public interest'. Public interest is the general welfare and rights of the public that are to be recognised, protected and advanced. Disclosures in the public interest based on the common law are made where disclosure is essential to prevent a serious and imminent threat to public health, national security, the life of the individual or a third party or to prevent or detect serious crime. Ultimately, the public interest can only be determined by the courts. However, when considering disclosing information to protect the public interest, health professionals must:

- Consider how the benefits of making the disclosure balance against the harms associated with breaching the service user's confidentiality both to the individual clinical relationship and to maintaining public trust in a confidential service.
- Assess the urgency of the need for disclosure.
- Persuade the service user to disclose voluntarily.
- Inform the service user before making the disclosure and seek his or her consent, unless to do so would increase the risk of harm or inhibit effective investigation.
- Disclose the information promptly to the appropriate body.
- Reveal only the minimum information necessary to achieve the objective.
- Seek assurance that the information will be used only for the purpose for which it is disclosed.
- Document the steps taken to seek or obtain consent, and the reasons for disclosing the information without consent.
- Be able to justify the decision.
- Document both the extent of and grounds for the disclosure.

Health professionals should be aware that they risk criticism, and even legal liability, if they fail to take action to avoid serious harm. There is no specific legislation which tells health professionals whether or not to disclose information in a particular case, but general guidance about the categories of cases in which decisions to disclose may be justifiable are below. Guidance should be sought from the Caldicott Guardian, Information Governance Manager, Trust Solicitor, professional body or defence body where there is any doubt as to whether disclosure should take place in the public interest.

4.7.2 Serious Crime And National Security

There is no legal definition as to what constitutes a 'serious crime'. In the Police and Criminal Evidence At 1984 a 'serious arrest-able offence' is an offence that has caused or may cause:

- Serious harm to the security of the state or to public order.
- Serious interference with the administration of justice or with the investigation of an offence.
- Death.
- Serious injury.
- Substantial financial gain or serious loss.

This includes crimes such as murder, manslaughter, rape, treason, kidnapping and abuse of children or other vulnerable people. Serious harm to the security of the state or to public order and serious fraud will also fall into this category. In contrast, theft, minor fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

4.7.3 Public Safety

A common example of what can be categorised as public safety occurs in connection with the assessment of service users with, for example, diabetes, epilepsy, defective eyesight, hypoglycaemia or serious cardiac conditions who have been advised by health professionals to discontinue driving, but who nevertheless continue. The DVLA should be informed if anybody is thought to be at risk.

Issues of public safety may similarly arise in circumstances where an individual who legitimately possesses firearms is thought by health professionals to be a risk because of drug or alcohol addiction or a medical condition such as depression. The police should be informed if anybody is thought to be at risk.

5. Information Sharing That Requires Express Consent

National guidance has identified certain areas of information sharing that must only be carried out on an express/explicit consent basis. Consent is required for information sharing that does not directly contribute to direct continuing healthcare, unless there is a robust public interest in releasing information

without the service user's consent or you have the express/explicit consent in writing, from the service user or recorded in the service users health record.

For most information sharing issues that are not for the direct continuing care of a service user you should consult the Caldicott Guardian or Information Governance Manager.

The following table gives further details

Carers and Relatives	Generally where a service user has the capacity to consent express/explicit consent is required before sharing health information. Confidentiality can be a highly controversial issue. Carers want and need information about the person they are caring for, whereas professionals feel bound by codes of conduct on confidentiality.
NHS Complaints Committees	Complaint Committees will invariably need service user information. However, express consent of the complainant, and any other service users whose record may need to be reviewed, is required prior to disclosure.
Management Purposes	Commissioners, prescribing advisors, financial audit, resource allocation etc., - no restrictions are imposed if the data is anonymised or pseudonymised.
Occupational Health Professionals	Information on staff referred to occupational health departments. However, if clinicians are the service users, the powers of professional regulatory bodies for disclosure may apply.
Researchers	The use of service user information for research goes beyond health care provision in the NHS and explicit service user consent is therefore required. For example, whilst most people would be happy to be included in research there may be some that might object on the grounds of, for example, 'religion'. However, if the research project is to use anonymised or pseudonymised data, (which is preferable) no restrictions are imposed, (refer to anonymisation and pseudonymisation below. Alternatively, an application can be made to the Ethics and Confidentiality Committee of the National Information Governance Board under section 251 of the NHS Act 2006. Before any research project can be undertaken an application must be made to the Local Research Ethics Committee for approval and before making any application to the Ethics and Confidentiality Committee Of the National Information Governance Board under Section 251 of the NHS Act 2006.

Teaching	According to the Confidentiality: NHS Code of Practice teaching is not to be regarded as direct healthcare purposes and will require explicit consent.
Sure Start Teams	Disclosures to Sure Start teams for anything other than the direct continuing healthcare of young children needs explicit consent from parents. Example: extracting lists of children's names who are below the age of 5 from information held by an organisation to enable Sure Start to target certain groups of families to give them toothpaste samples would require explicit consent.
The Media	You need explicit consent to release information to the media about care and treatment (including a service user's presence in a hospital) unless there is an exceptional robust public interest in releasing information.
Police	Information required by the Police either needs explicit consent of the service user, a Court Order or, where criminal activities are concerned refer to section 6.1 below on Enabling Information Sharing in the Public Interest.
Solicitors	Solicitors requesting information must produce an up to date written signed consent from the service user before you release any information. If you have any doubts as to the authenticity of the consent or the fact that the whole of the service user's record has been requested contact the service user direct – you must obtain consent from any third parties before releasing third party information.

6. Legislation Enabling/Requiring/Restricting Information Sharing

6.1 Enabling Information Sharing in the Public Interest

The following legislation permits information to be shared without seeking consent e.g. if you believe someone has committed serious harm, or a serious crime, However the legislation does not require you to do so. Decisions to share should be made on a case by case basis, and in the public interest.
In some circumstances, the DPA 2018 provides an exemption from particular GDPR provisions. If an exemption applies, you may not have to comply with all the usual rights and obligations.

There are several different exemptions; these are detailed in Schedules 2-4 of the DPA 2018. They add to and complement a number of exceptions already built in to certain GDPR provisions.
The exemptions in the DPA 2018 Schedules 2-4 can relieve you of some of your obligations for things such as:

1. Child Protection (Children's Act 1989 and the Protection of Children Act 1999). Allows information to be shared if a child is considered at risk of significant harm.
2. Prevention and Detection of Crime (Section 115 of the Crime and Disorder Act 1998) – e.g. request from the Police where someone is suspected of committing a serious crime.

3. Disclosures to a health professional within a Sure Start team under the NHS Act 1997 where disclosures directly and only support healthcare of young children. (If health records are to be held within partner organisations, parents must be properly informed).

Some exemptions apply to only one of the above, but others can exempt you from several things.

Some things are not exemptions. This is simply because they are not covered by the GDPR. Here are some examples:

- **Law enforcement** – the processing of personal data by competent authorities for law enforcement purposes is outside the GDPR's scope (e.g. the Police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of the Data Protection Act 2018.

- **National security** – personal data processed for the purposes of safeguarding national security or defence is outside the GDPR's scope. However, it is covered by Part 2, Chapter 3 of the DPA 2018 (the 'applied GDPR'), which contains an exemption for national security and defence.

6.2 Requiring Information Sharing

Information can be shared without consent if requested to do so by the following public bodies/officials but service users should be informed that disclosure has been required:

1. Courts, including a coroner's court, tribunals and enquiries – Only give the information requested in the order and no more. Many different Acts give courts the powers to issue court orders.
2. General Medical Council (GMC) – Entitled to access confidential patient health records as part of an investigation under the Medical Act 1983. The GMC have indicated that they would always try to obtain consent first.
3. Audit Commission – Entitled to access confidential patient health records as part of an investigation under section 6 of the Audit Commission Act 1998.
4. Health Service Ombudsman – Has the same powers as the courts to disclose person identifiable information. Any request made should be complied with, without obtaining a court order.
5. Healthcare Commission – The Healthcare Commission's legal name is the Commission for Healthcare Audit and Inspection. It was formed by the Health and Social Care Act 2003 launched on 1st April 2004.
6. Public Health and Infectious Diseases – Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1988.
7. Immunisations and vaccinations – Under the Education Act 1944 information must be passed to NHS Trusts from schools.

8. Births and Deaths – The Births and Deaths Act 1984 provides for the registration of births, still-births and deaths.
9. Abortion Regulations 1991 – a doctor carrying out a termination of pregnancy must notify the Chief Medical Officer, giving a reference number and the date of birth and postcode of the woman concerned.
10. Section 251 of the NHS Act 2006 – gives the Secretary of State for Health power to make regulations permitting the disclosure of identifiable information without consent in certain circumstances. Health professionals can apply to the Ethics and Confidentiality Committee of the National Information Governance Board, an independent public body which advises the Secretary of State for Health in England and Wales about the lawful disclosure of service user identifiable information.
11. Members of Parliament – Non-statutory investigations (e.g. Members of Parliament). If a MP states, in writing that he/she has a service user's consent for disclosure this may be accepted without further contact with the service user but – carefully consider the request and contact the service user if in any doubt.

6.3 Restricting Information Sharing

Health professionals are required by law to restrict the disclosure of some specific types of information, for example:-_

1. Human Fertilisation and Embryology Act 2008
2. NHS (Venereal Diseases Regulations) 1974 and the NHS Trusts and PCTs (Sexually Transmitted Diseases) Directions1992
3. The Gender Recognition Act 2004
4. The Adoption Act 1976

7. Anonymisation and Pseudonymisation

7.1 Anonymisation

Information can be used without service user consent and requires the removal of:

- Name
- Address
- Full postal code
- NHS number
- Date of Birth
- Local Identifiers
- Anything else that could identify a service user e.g. photograph, x-ray, dental records etc.

Information that has been anonymised can never be reverted back to its original form.

Information may be used more freely if the subject of the information is not identifiable in any way. When anonymised data will serve the purpose, health professionals must anonymise data to this extent and,

if necessary, take technical advice about anonymisation before releasing data. Whilst it is not ethically necessary to seek consent for the use of anonymised data, general information about when their data will be anonymised should be available to service users.

7.2 Pseudonymisation

Pseudonymisation is sometimes referred to as reversible anonymisation. Patient identifiers, such as name, address or NHS number, are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference. Where those who are using data have no means to reverse the process, and so no way to identify an individual from the data they have, the data may be treated as anonymised and there is no common law requirement to seek consent for their use. For those who have access to both pseudonymised data and the means to reconstitute them, they should be treated as identifiable. The use of pseudonymised data is common in research. As with anonymised data, service users should generally be informed when it is intended that their information will be pseudonymised.

8. Deceased persons

Although the General Data Protection Regulation and the DPA 2018 does not apply to records of deceased persons the ethical obligation to respect a service user's confidentiality extends beyond death. The Information Tribunal in England and Wales has also held that a duty of confidence attaches to the records of the deceased under section 41 of the Freedom of Information Act 2000. If a patient has requested that their information is not disclosed after their death this must be respected. The Access to Health Records Act 1990 gives limited statutory rights of access to those who 'may have a claim' arising out of the death of a deceased patient. Care must always be taken when sharing records of the deceased and advice should be sought in cases of doubt.

Appendix 4

Legal Duties and Powers to Share Information in relation to Children and Young People

Statutory Provisions to Information Sharing – Child Protection

Agency	Why do you want to share/request information?	From whom do you wish to share/request information?	Legal basis to share/request information
Any agency or public body	There is reasonable cause to suspect that a child is suffering or is likely to suffer significant harm	Social Care	Section 47 Children's Act 1989
Children's Services	To undertake enquiries in order to decide if action should be taken to safeguard or promote the child's welfare	Any agency who may have information	Section 47 (1) Children's Act 1989
Local Housing Authority, Special Health Authority, Primary Care Trust, NHS Trust	Children's Services request for information in order to decide if action should be taken to safeguard or promote the child's welfare	Children's Services	Section 47 (9) Children's Act 1989

Child Protection – People Unsuitable to Work with Children/Vulnerable Adults

Agency	Why do you want to share/request information?	From whom do you wish to share/request information?	Legal basis to share/request information
Any organisation employing a person in child care position	An individual has been found guilty of misconduct (whether or not in the course of his/her employment)	Department of Education and Skills, Department of Health	Protection of Children Act 1999 Section 2A
Any organisation dealing with child care	The organisation wishes to offer a job to a person in a child care capacity	Department of Education and Skills, Department of Health	Protection of Children Act 1999 Section 3

Any organisation employing a person in a care of vulnerable people position	A person is found to be unsuitable to work with vulnerable people	Department of Health	Care Standards Act 2000 Section 82

Children with a Disability

Agency	Why do you want to share/request information?	From whom do you wish to share/request information?	Legal basis to share/request information
Children's Services/Local Authority	To compile and maintain a register of disabled children	Health	Children's Act 1989 Section 17 (2)
Any Local Authority Service	There is a need for health or housing provision and Health or Housing can assist with the assessment	Primary Care Trust, Health Authority or Local Housing Authority	Section 47 National Health Service Act and Community Care Act
Children's Services/Local Authority	To compile and maintain a register of blind; partially sighted; deaf with speech; deaf without speech; hard of hearing; and general classes (those whose primary handicap is neither visual nor auditory)	Health Services	National Assistance Act 1948 Section 29

Children with Special Educational Needs

Agency	Why do you want to share/request information?	From whom do you wish to share/request information?	Legal basis to share/request information
Education/Health	To assess a child's SEN	Health, Education, Children's Services. Also they should seek advice from child's parent, Head Teacher, the teacher who taught the child,	Section 322 Education Act 1996 Education (Special Education Needs) (England)

		the person who the authority are satisfied has experience of teaching children with SEN. Medical advice from the Health Authority. Psychological advice. Advice from social care. Any other advice which the LEA considers appropriate	(Consolidation) Regulation 2001 (SI 3455/2001) Regulation 7(1)
LEA	Considering making an assessment of SEN. LEA under obligation to send copies of the notice stating they are considering an assessment of SEN	Children's Services, Health Authority, Head Teacher of School pupil registered with (if any). If the child receives education from an early education provider, to the head of SEN in relation to that provider	Education (Special Education Needs) (England) (Consolidation) Regulation 2001 (SI 3455/2001), Regulation 6

Children and Young People involved or likely to be involved in Crime and Disorder

Agency	**Why do you want to share/request information?**	**From whom do you wish to share/request information?**	**Legal basis to share/request information**
Police, Housing, National Park Authority, Health, Probation; Youth Offending Team	Have reasonable belief that a child or young person is likely to commit a crime and therefore to prevent crime occurring	Any appropriate agency that can assist the child or young person to prevent them from committing a crime. E.g. Health, Youth Offending, Voluntary Agency if appropriate	Crime & Disorder Act 1998 Section 115; Section 17 (1); Section 37 and Section 38. (Information disclosed must be on a need to know basis and minimum amount provided

A Child or Young Person who is in the Care of the Local Authority

Agency	Why do you want to share/request information?	From whom do you wish to share/request information?	Legal basis to share/request information
Children's Services	Because a Looked-After Child is being accommodated at an establishment at which education is provided	The Local Education Authority of the area in which the establishment is located	Children Act 1989 Section 28
	Because parents/carers of a LAC have moved to another area and have another child	Social care in the new area	FPC rule 23 Family Proceedings Court (Children Act) Rules 1991 CC10.20(3) rule Family Proceedings Rules 1991
	To inform an assessment of a child. Because a Judge has made a finding of fact which has implications for other children	LEA, Health Authority, relevant agencies	For documents before a Court in any proceedings under the Children Act or Adoption Act leave must always be obtained prior to disclosing (sharing)
Any Health Authority or Local Education Authority	Because a child is being accommodated by them and they are obliged to inform Social care of this fact Social care has to ensure the child's welfare is being adequately safeguarded and promoted	Children's Services in area where the child is being accommodated	Children Act 1989 section 85

A Child or Young Person who is Leaving or Has Left Care

Agency	**Why do you want to share/request information?**	**From whom do you wish to share/request information?**	Legal basis to share/request information
Children's Services	Because a young person is entitled to leaving care services and social care has a duty to keep in contact with such a young person and to provide advice and assistance A young person is eligible if he/she has been in care for a period of 13 weeks or more since he/she was 14 and has left care after 16 but is still under 21. It does not include children who have received respite care or if the young person has returned home	Any agency that may have any information about the young person which enables the LA to undertake its statutory duty. Most likely to be Health Services but could by any agency (GP registration)	Children Act 1989 Section 23 and Section 24, as amended by Children (Leaving Care) Act 2000 sections 24, 24A to 24D
Children's Services	Because Children's Services has lost contact with an eligible care leave and has to take reasonable steps to locate them	Any agency who has this information, most likely Health	Children Act 1989 Section 23 and Section 24, as amended by Children (Leaving Care) Act 2000 sections 24, 24A to 24D

General Functions, Powers and Duties (Implied Statutory Powers)

To use implied statutory powers, stronger justification is required to demonstrate that it is necessary to share sensitive data without explicit consent

Agency	Why do you want to share/request information?	From whom do you wish to share/request information?	Legal basis to share/request information
Any Local Authority Department	Because the department has a statutory duty to carry out a particular function, e.g. filling in the Pupil Level Annual School Census by the LEA	Other agencies (including voluntary agencies) that hold relevant information to enable the LA department to carry out its statutory duty. Without the information they would not be able to carry out the particular function	Section 111 of the Local Government Act 1972, give LA's the power 2to do anything which is calculated to facilitate, or is conducive or incidental to the discharge of any of their functions"
Any Local authority Department	Because the local authority considers that with the information it can: (a) promote or improve the economic well-being in their area (b) promote or improve the social well-being of their area (c) promote or improve the environmental well-being of their area	Any other agency who holds relevant information	Section 2 of the Local Government Act 2000, which gives the LA "a power to do anything they consider is likely to achieve any one or more of the objectives" as set out in column 2. So long as there are no restrictions or prohibitions or limitations in other enactments, i.e. must be compatible with the requirements of the Data Protection Act and Human Rights Act and Common Law Duty of Confidence
Any Health Service within NHS	To provide a comprehensive health service in England and	Other NHS practitioners working within the Health	National Health Service Act 1977, Section 2

	Wales to improve the physical and mental health of the population and to prevent and diagnose and treat illness	Service and practitioners from other agencies e.g. social care, who are carrying out health service functions that would otherwise be carried out by the NHS	
Any Health Service within NHS and Local Authority	In order for Health to exercise their Health Service functions and for the LA to exercise its functions in order to secure and advance the health and welfare of the people of England and Wales	Other NHS practitioners working within the Health Service and practitioners from other agencies e.g. social care, who are carrying out health service functions that would otherwise be carried out by the NHS	National Health Service Act 1977, Section 22
Any Local Authority; any Local Education Authority; any Local Housing Authority; Any Health Authority	Because it is felt that a child or young person or family is in need of services to safeguard and promote the welfare of a child or young person. Section 17 of Children's Act states a child is in need if: (a) He/she is unlikely to achieve or maintain, or to have the opportunity of achieving or maintaining a reasonable standard of health or development without the provision for him/her of services by a local authority under this part (b) His/her health or development is likely to be	Other agencies within this partnership who are involved with the child, young person or family and with any other agency that may provide the appropriate services (including voluntary agencies)	Children's Act 1989. Part III: • Section 17 (1) (provision of service) This places a general duty on every LA "to safeguard and promote the welfare of children within their area who are in need and so far as is consistent with that duty, to promote the upbringing of such children by their families, by providing a range and level of services appropriate to those children's needs" • Section 27 (1)(2) and (3) (other agencies acting on behalf of the

	significantly impaired, or further impaired, without the provision for him/her of such services (c) He/she is disabled. "Family" includes any person who has parental responsibility for the child and any other person with whom he/she has been living		LA) • Section 17(5) (voluntary agencies) Section 17(10) and (11) (definition of a child in need) Section 2 Local Government Act 2000
Health Service	A child or young person has physical or mental health problems which require extra services	Any agency that can provide appropriate health services (that could be voluntary agency providing a health service)	National Health Service Act 1977, Section 1
Children's Services	Because it is felt that another organisation could assist them to provide support for children in need and or their families. Any authority to whom such a request is made has duty to cooperate provided that the request is not incompatible with the performance of its own obligations or unduly prejudice the performance of their own functions	Other local authorities, any local education authority, any local housing authority, any health authority	Children Act 1989, Section 27
Children's Services	Record involvement of agency with child or young person, investigate suitable service provision to improve the wellbeing of children so far as	Districts, Police, Probation, Youth Offending Team, any health authority, local education authority, schools, probation board, Youth	Children's Act 2004, Section 10 & 11

	relating to: (a) physical and mental health and emotional wellbeing; (b) protection from harm and neglect; (c) education, training and recreation; (d) the contribution made by them to society; (e) social and economic well-being	Offending Team providers under section 114 Learning and Skills Act 2000; the governor of a prison or secure training centre in England (or, in the case of a contracted out prison or secure training centre, its director); the British Transport Police Authority; a person registered in England for child minding or the provision of day care; a registered social landlord; a voluntary organisation	
Children's Services	A Database: (a) name, address, gender, DoB (b) a number identifying him/her (c) the name and contact details of any person with parental responsibility who has care of him/her at any time (d) details of any education being received by him /her (e) the name and contact details of any person providing primary medical services in relation to him/her under Part 1 of the NHS Act 1977 (c.49) (f) the name and contact details of any person providing	Districts, Police, Probation, YOT, any health authority, local education authority, probation board, YOT providers under section 114 Learning and Skills Act 2000	Children's Act 2004 Section 12 (1,2,3,4)

	to him/her services of which description as the SoS regulations specify (g) information as to the existence of any cause for concern in relation to him/her Information of such description, not including medical records or other personal records, as the SoS regulations specify		

HEALTH SERVICE

General functions/powers/duties

Section/Regulation	Description
Section 1 National Health Service Act 1977	"1(1) It is the Secretary of State's duty to continue the promotion in England and Wales of a comprehensive health service designed to secure improvement: a) In the physical and mental health of the people of those countries, and b) In the prevention, diagnosis and treatment of illness, And for that purpose to provide the effective provision of services in accordance with this Act"
Section 31 Health Act 1999	This section allows the Secretary of State to make regulations in connection with enabling the NHS bodies and local authorities to enter into prescribed arrangements in relation to prescribed functions on the NHS bodies and prescribed health-related functions of local authorities
NHS Bodies and Local Authorities Partnership Arrangements Regulations 2000 (S.I.2000/617)	These regulations are made under s31 Health Act 1999 and allow NHS bodies and local authorities to enter into partnership arrangements in relation to the exercise of any NHS functions if the partnership arrangements are likely to lead to an improvement in the way in which those functions are exercised.

Adoption Agencies Regulations 1983 (S.I. 1983/1964)	Regulation 6(5) obliges the adoption agency to consult its medical adviser in relation to arrangements for access to and disclosures of health information which is required or permitted by virtue of regulation 15
NHS (General Ophthalmic Services) Regulations 1986 (S.I. 1986/975)	This requires opticians to keep records and imposes an obligation to disclose to the PCT or the Secretary of State on request
Section 47 Children Act 1989	S47(9) provides, "Where a local authority are conducting enquiries under this section, it shall be the duty of any person mentioned in subsection (11) to assist them with those enquiries (in particular by providing relevant information and advice) if called upon by the authority to do so"
Section 85 Children Act 1989	
Section 47 National Health Service and Community Care Act 1990	This section concerns the assessment of needs for community care. It provides that when a local authority is assessing need and it appears that there may be a need for health or housing provision, the local authority shall notify the PCT, Health Authority or local housing authority an invite them to assist, to such extent as is reasonable in the circumstances, in the making of the assessment
NHS (General Dental Services) regulations 1992 (S.I. 1992/661) Schedule 1 Para 25	These regulations place an obligation on dentists to keep records and to disclose to a PCT, the Secretary of State, the Dental Practice Board or a dental officer on request
Section 31 Health Action 1999	S31(3)(g) provides that regulations may make provisions as to the sharing of information between NHS bodes and local authorities
Section 60 Health and Social Care Act 2001	This allows for the SoS to make regulations in respect of the processing of prescribed patient information for medical purposes if he considers it necessary or expedient: a) In the interests of improving patient care, or b) In the public interest
Heath Service (Control of Patient Information) Regulations 2002 (S.I. 2002/1438)	These regulations are made under 260 of the Health and Social Care Act 2001 and provide circumstances when confidential patient information may be processed for medical purposes

Appendix 5

Consent to Information Sharing in TPP SystmOne

SystmOne supports patient choice not only in terms of whether information is 'shared out' between organisations (i.e. between the Trust and GP Practices) which is known as NHS CRS level, but also whether it is 'shared in' between units in an organisation, this is known as the patients 'unit level sharing preference'

It should be noted that allowing 'sharing out' only allows those units at which a patient is registered to have access to the patient record, this means that if a patient consents to sharing at NHS CRS Level at their GP Practice, only those units within the Trust that have the patient registered will be able to see the patients record, not all units within the Trust, therefore the majority of patient records will not be seen outside of the GP Practice.

1. Unit Level Sharing Preference

Any clinician when referring a patient into another service within the Trust should explain to the patient the ability within SystmOne to share their health records with the service to which they are being referred. If the patient consents/dissents to sharing this should be indicated on the referral.

Within the Trust, patients are usually registered within a unit by an administrator. If the patient has been referred to the unit by another Trust unit then that referral should state whether or not the patient has been informed and consented/dissented to sharing their record. If this is the case the administrator can mark the record as shareable/private as per the Quick Reference Guide to setting sharing preferences.

If the patient has dissented to share at NHS CRS level then the sharing preferences will be set to 'implicit dissent' and the record will remain private until the patient is asked for their consent/dissent to share.

When a clinician has their first consultation with that patient they must then explain the sharing ability of SystmOne and update the sharing preferences within the record accordingly.

An example of how sharing preferences can be set is given below.

2. NHS CRS Level Sharing Preference

Every person registered on the PDS (Patient Demographics Service) has a global flag which indicates, in broadest terms, whether or not they wish to participate in the NHS Care Records Service (NHS CRS). The flag known as the patient's NHS CRS information sharing preference, can be viewed and changed in SystmOne but is ultimately held on PDS and will be accessed in time by all clinical systems delivered by NHS Connecting for Health as part of the National Programme for IT.

The NHS CRS flag is set initially to 'Implied Consent' on PDS. When a patient specifies an NHS CRS information sharing preference, the flag should be changed to either explicit consent or dissent accordingly.

When a patient explicitly consents or dissents to NHS CRS information sharing, their choice will affect how their information is shared not only within SystmOne, but across the NHS Care Record Service as a whole. It determines two things: 1) whether information in the patient's electronic record will be shared outside of the legal organisation by which it was created; 2) whether the patient's Summary Care Record, if they wish to have one, will be shared.

If a patient's NHS CRS information sharing preference is set to dissent, this will not prevent the clinician they are seeing from creating a Choose and Book referral, as clinical communications of this nature are not impacted by sharing preferences.

3. Sharing preferences for individual events

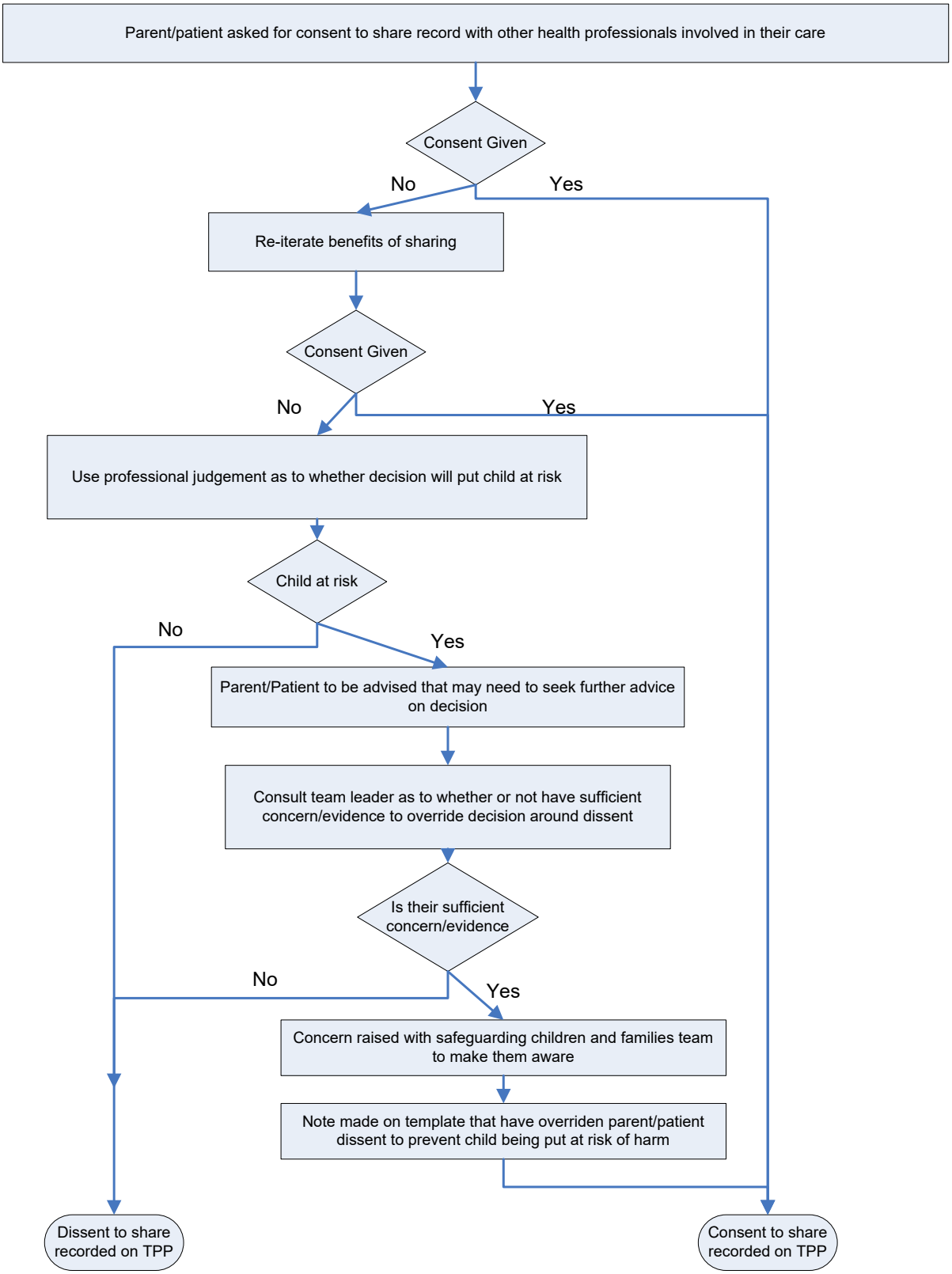
SystmOne allows users to set the sharing preference for individual events in the patient record, based on the patient's wishes. This means that, where the record sharing preference as a whole has been set to 'shareable', it is still possible to mark individual events that the patient wishes to keep within the confines of the unit as private.

An 'event' refers to any information entered into the patient record with the same date and time stamp.

4. Obtaining consent to share children's records

Consent for sharing of children records should be sought using the guidance in appendix 4 section 4.5. If consent is not given by either the person with parental responsibility or the child, the following guidance should be followed: (see page 45 below)

Sharing Diagram on TPP (SystmOne)



Sharing Example

The patient is receiving care from three organisations: GP, District Nursing and Smoking Cessation. The patient wants their GP and District Nurse to share information with each other and the patient wants both the GP and District Nurse to be able to access the information being recorded by the Smoking Cessation service; however the patient does not want the Smoking Cessation service to see any other medical information. The sharing settings would be as follows:-