Essex Partnership University
NHS Foundation Trust

INFORMATION SHARING & CONSENT POLICY

POLICY REFERENCE NUMBER	CP60
VERSION NUMBER	2
KEY CHANGES FROM PREVIOUS VERSION	GDPR compliance
AUTHOR	Information Governance Manager
CONSULTATION GROUPS	IGSSC
IMPLEMENTATION DATE	August 2017
AMENDMENT DATE(S)	April 2018
LAST REVIEW DATE	October 2018
NEXT REVIEW DATE	August 2020
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE	September 2018
RATIFICATION BY QUALITY COMMITTEE	October 2018 (Chair's Action – [redacted] at IGSSC Sept 18 in role of Chair of QC)
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

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.

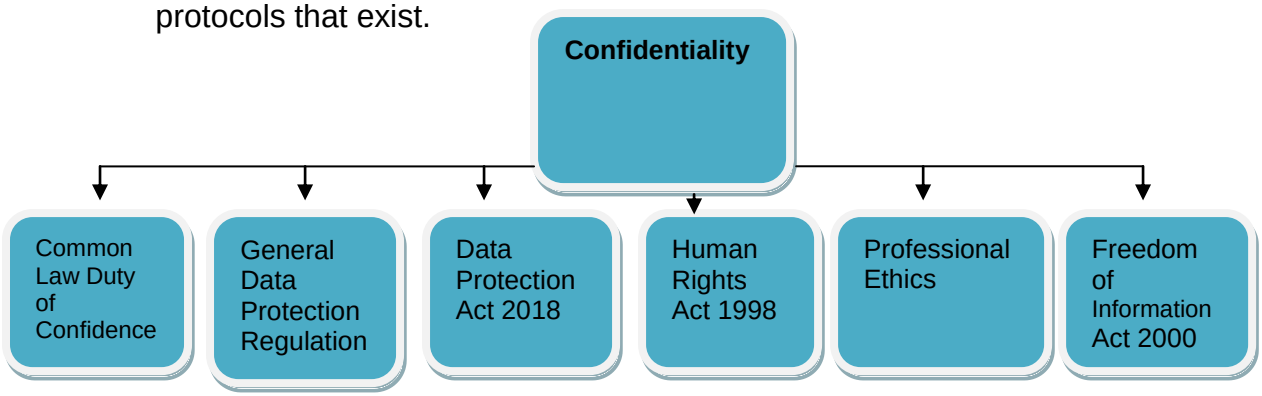
1.2 Sharing information presents risks. Information systems are becoming more complex and widespread. There is a potential for more information about our private lives, often highly sensitive, to become known to more and more people.

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 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 DUTIES

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 DEFINITIONS

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, Viewpoint and others
- On-Line training 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:

- 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