



INFORMATION SHARING & CONSENT PROCEDURE

PROCEDURE REFERENCE NUMBER	CPG60
VERSION NUMBER	2.0
KEY CHANGES FROM PREVIOUS VERSION	3-year review. New consent form
AUTHOR	Information Governance Manager
CONSULTATION GROUPS	IGSSC
IMPLEMENTATION DATE	August 2017
AMENDMENT DATE(S)	September 2020
LAST REVIEW DATE	November 2020
NEXT REVIEW DATE	November 2023
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE:	October 2020
RATIFICATION BY QUALITY COMMITTEE:	November 2020
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 Executive Medical Director

INFORMATION SHARING & CONSENT PROCEDURE

CONTENTS

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

- 1.0 INTRODUCTION
- 2.0 DECIDING TO SHARE PERSONAL INFORMATION
- 3.0 PROCESS FOR INFORMATION SHARING IN THE TRUST
- 4.0 SECONDARY USERS
- 5.0 TRAINING
- 6.0 MONITORING AND REVIEW

APPENDICES

APPENDIX 1 – INFORMATION SHARING AGREEMENT TEMPLATE

APPENDIX 2 – TRUST PATIENT CONSENT FORM

APPENDIX 3 – CONSENT GUIDANCE FOR INFORMATION SHARING (FOR STAFF)

APPENDIX 4 – LEGAL DUTIES AND POWERS TO SHARE INFORMATION IN RELATION TO CHILDREN AND YOUNG PEOPLE

APPENDIX 5 – CONSENT TO INFORMATION SHARING TPP (SYSTMONE)

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 / 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.

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

CPG60 - INFORMATION SHARING & CONSENT PROCEDURE

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 delivered 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.

END