Essex Partnership University
NHS Foundation Trust

CONFIDENTIALITY PROCEDURE

PROCEDURE REFERENCE NUMBER:	CPG59b
VERSION NUMBER:	5.2
KEY CHANGES FROM PREVIOUS VERSION	Covid-19 6 month extension applied
AUTHOR:	[redacted]
CONSULTATION GROUPS:	IGSSC
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	March 2018; August 18
LAST REVIEW DATE:	N/A
NEXT REVIEW DATE:	~~April 2020~~ October 2020
APPROVAL BY IGSSC COMMITTEE:	July 2018
COPYRIGHT	

POLICY SUMMARY
The purpose of this Procedure is to ensure that staff understand their responsibilities regarding the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 ("DPA"), thereby ensuring that lawful and correct processing of personal information is a key part of building and maintaining trust and confidence in Essex Partnership University NHS Foundation Trust (the "Trust").
The Trust monitors the implementation of and compliance with this policy in the following ways;
The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate.

Services	**Applicable**	**Comments**
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is the Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CONFIDENTIALITY PROCEDURE

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CONFIDENTIALITY PROCEDURE

Assurance Statement

The purpose of this Procedure is to ensure that all staff understand their responsibilities regarding confidentiality of data, thereby ensuring that lawful and correct processing of personal information is a key part of building and maintaining trust and confidence in Essex Partnership University NHS Foundation Trust (the "Trust").

1.0 INTRODUCTION

1.1 All legislation relevant to an individual's right to confidentiality and the ways in which that can be achieved and maintained are paramount to the Trust. This relates to roles that are reliant upon computer systems such as: service user administration, payment, purchasing, invoicing and treatment planning. Legislation also regulates the use of manual records relating to service users, staff and others whose information may be held within the Trust.

1.2 Patients expect that information about them will be treated as confidential and are given that assurance in the Patient Charter (1997), 'everyone working for the NHS is under a legal duty to keep your records confidential.' Patients who feel that confidence has been breached may issue a complaint under the NHS complaints procedure or they could take legal action.

2.0 CONFIDENTIALITY GUIDANCE SECTION

2.1 Access to Confidential Information

2.1.1 It is the Trust's responsibility to protect the rights of patients, staff and individuals, who expect confidentiality of personal information held and processed by the Trust.

2.1.2 The Trust expects that all employees ensure that all confidential information attained in the course of their work is treated in strict confidence, and is in addition to responsibilities associated with individual professional codes of practice.

2.1.3 It will be the individual responsibility of all service managers to keep all confidential information safe and secure and identify measures within their own area of responsibility, which limit access to information to authorised personnel only.

2.1.4 All information obtained by Trust employees in the course of their work may only be disclosed to third parties *with the express consent of the individual* and as authorised by the Trust, or where required by order of a court or where it can be justified in the wider public interest under the General Data Protection Regulation.

2.1.5 Any decision to disclose confidential information about a patient's treatment or care should always, in the first instance, be brought to the attention of the patient's Responsible Medical Officer. It will be their responsibility to assess whether disclosure of information is in the interests of the patient and liaison with the person in charge, decide whether the patient is able to give informed consent. Any decision relating to the disclosure of personal data about a patient to a third party, whether that disclosure is verbal or written, should be recorded in the patient's health records.

2.1.6 If any doubt exists concerning the nature of information being classified as confidential, Trust employees are advised to treat the information as confidential and seek clarification from their service manager or the Trust's Data Protection Officer, before disclosing information.

2.1.7 Any disclosure of confidential information, not in accordance with the terms of these guidelines or its associated policy, will be viewed as a serious breach of discipline and will be dealt with under the Trust's disciplinary rules and procedures.

2.2 **Requests for Confidential Information**

2.2.1 All requests for confidential information concerning a patient, staff or other individual, including requests from third parties, must be passed to the appropriate service manager, who will be responsible dealing with the matter, adhering to the guidelines set out within this policy. Further clarification and advice may be sought from the Trust's Information Governance Team or Data Protection Officer.

3.0 CALDICOTT PRINCIPLES

3.1 The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel was chaired by Dame Fiona Caldicott and it set out six Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. Since then, when deciding whether they needed to use information that would identify an individual, an organisation should use the Principles as a test. The Principles were extended to adult social care records in 2000.

The Caldicott Principles (revised 2013) are:

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality (added in 2013)

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

4.0 THIRD PARTY REQUESTS FOR CONFIDENTIAL INFORMATION

4.1 In cases where requests for confidential information about a patient are made from a third party, the patient will be informed unless it can be demonstrated by the patient's Responsible Medical Officer and / or the Trust's nominated representatives that it is not in the interests of the patient to do so.

4.2 It will be the normal practice of designated Trust employees to record requests for confidential information from third parties and this should be recorded in the patient's health records along with the actions taken as a result of the request.

5.0 REPORTING BREACHES OF CONFIDENTIALITY

5.1 Any potential or actual breaches of confidentiality must be reported to the line manager immediately.

5.2 The Information Governance Team should be notified and a DATIX incident report completed. The Information Governance Team will be able to give advice on how to rectify / reduce the impact of the breach.

(***Note***: refer to Information Security Incident Reporting Procedure (CPG50d)

6.0 TRAINING AND SUPPORT

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 Trust Today, Viewpoint and others
- On-Line training via the NHS Digital 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 (HR21).

7.0 MONITORING AND REVIEW

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

7.2 The Executive Chief Finance Officer is responsible (as the Trust SIRO) with the Caldicott Guardian for the implementation of these procedural guidelines and its associated policy document.

END