Essex Partnership University
NHS Foundation Trust

DATA PROTECTION & CONFIDENTIALITY POLICY

POLICY REFERENCE NUMBER:	CP59
VERSION NUMBER:	3
KEY CHANGES FROM PREVIOUS VERSION	3 year review; minor changes
AUTHOR:	Alice Williams
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	March 2018; September 2021
LAST REVIEW DATE:	September 2021
NEXT REVIEW DATE:	September 2024
APPROVAL BY IGSSC:	August 2021
RATIFICATION BY QUALITY COMMITTEE:	September 2021
COPYRIGHT	

POLICY SUMMARY

The purpose of this Policy is to ensure that staff understand their responsibilities regarding the General Data Protection Regulation (GDPR) & Data Protection Act (DPA) and the 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").

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 Executive Chief Finance & Resources Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

DATA PROTECTION & CONFIDENTIALITY POLICY

CONTENTS

THIS IS AN INTERACTIVE CONTENTS PAGE, BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THE SECTION THAT YOU WANT.

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

DATA PROTECTION & CONFIDENTIALITY POLICY

1.0 INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) came into force on 25th May 2018. The new DPA 2018 is the UK legislation to come out of the GDPR; this enables the UK to stay in line with the EU as the original DPA1998 is considered no longer fit for purpose.

1.2 The GDPR is closely linked to the Freedom of Information and Human Rights Acts. Its focus is on promoting the rights of individuals in respect of their data, how it is used, stored and shared. Applies to 'Data *Controllers'* and 'Data *Processors'* - the controller says how and why personal data is processed.

1.3 The Trust has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, the NHS Executive, other advisory groups to the NHS and guidance issued by professional bodies.

1.4 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.

1.5 Patients expect that information about them will be treated as confidential and are given that assurance in the NHS Constitution for England, '.You have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure' Patients who feel that confidence has been breached may issue a complaint under the NHS complaints procedure or they could take legal action.

1.6 The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised persons include NHS staff who are not involved in either the clinical care of the patient or the associated administration processes.

1.7 Non-compliance with the relevant legislation could result in individuals, employees and the Trust being prosecuted for offences under the GDPR. Article 5 GDPR requires that personal data shall be:

"a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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 not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

Article 5(2) requires that:

"The controller shall be responsible for, and be able to demonstrate, compliance with the principles."

1.7.1 The risks associated with not complying with this policy and the associated procedures includes litigation, breach of law as well as loss of reputation to the Trust and potential impact on the service user.

2.0 MANAGEMENT AND STAFF RESPONSIBILIES

2.1 The Chief Executive

2.1.1 The **Chief Executive** has overall responsibility for Data Protection and Confidentiality within the Trust.

2.2.2 The implementation of, and compliance with, these procedures and the associated policy is delegated to the Director of IT

2.2 The Data Protection Officer

2.2.1 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.

2.3 Service / Team / Ward Managers

2.3.1 The day-to-day responsibilities for enforcing these guidelines will lay with individual service managers and other nominated staff. In order to fulfil their roles, the Data Protection Officer will ensure that regular training is provided to remind designated staff of these responsibilities and the most effective way of ensuring adequate information security and confidentiality.

2.4 Individual Data Users

2.4.1 All employees of the Trust, who record and/or process personal data in any form (referred to as "Data Users"), must ensure that they comply with:

- The requirements of the GDPR & Data Protection Act (including the Data Protection Principles).
- The Trust's data protection and confidentiality related policies, including any procedures and guidelines, which may be issued from time to time.

2.4.2 A breach of the GDPR, DPA and/or the Trust's data protection and confidentiality related policies and procedures may result in disciplinary proceedings and may lead to an individual being personally liable for the breach.

2.4.3 Consideration should be given towards contacting the Data Protection Officer for data protection advice concerning the following:

- When developing a new computer system for processing personal data;
- When using an existing computer system to process personal data for a new purpose as it may be necessary to notify an amendment to an existing registration;
- When creating a new manual filing system containing personal data;
- When using an existing manual filing system containing personal data for a new purpose.

3.0 DEFINITIONS

3.1 ***"Personal Data"***

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;

3.2 ***"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.

3.3 ***Confidentiality (NHS Code of Practice)***

3.3.1 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.

3.4 ***Personal Information***:- (***The GDPR applies to both automated personal data and to manual filing systems)***

- Forename
- Surname
- Date of Birth
- Sex
- Address
- Postcode
- NHS Number, hospital number or other patient number
- Staff payroll number
- Bank details

(This list is not exhaustive...)

3.5 ***Processing*** includes (but is not limited to):-

- Obtaining
- Recording
- Retrieval
- Consultation
- Holding
- Disclosing
- Use
- Transmission
- Erasure
- Destruction

(This list is not exhaustive...)

3.6 A ***data subject*** is an individual who is the subject of the personal data. A data subject must be a living individual.

3.7 ***Data Controller***:-

- The individual, company or organisation who determines the purpose and the manner in which personal data may be processed.
- The Data Controller is EPUT

3.8 ***Data Processor*** in relation to personal data, means any other person other than an employee of the Data Controller who processes data on behalf of EPUT.

3.9 ***Recipient***, in relation to personal data means any person to whom data is disclosed (including employees or agents of EPUT

3.10 ***Third Party***, means any person other than; the data subject, EPUT, any processor or other person authorised to process for EPUT

3.11 The ***Information Asset Owner (IAO)*** is the person or group of people who have been identified by management as having responsibility for the maintenance of the confidentiality, availability and integrity of that asset. The asset owner may change during the lifecycle of the asset.

3.12 The ***Information Asset Administrator (IAA)*** is the person or group of people who have been identified by the Information Asset Owner as having responsibility for adding information to the asset.

3.13 The IAO and nominated IAA will record their team assets on the Information Asset Management System (IAMS). This is a requirement with the NHS Digital Information Governance Toolkit. These assets are monitored and kept up to date. The Information Governance Team will advise and guide the nominated person from each team.

4.0 REPORTING BREACHES

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

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

4.3 In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

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

5.0 TRAINING AND SUPPORT

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 Electronic Staff Briefings
- 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 (HR21).

6.0 MONITORING AND REVIEW

6.1 The procedural guidelines will be reviewed in line with this policy document and / or whenever changes in legislation, guidance from 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 SIRO for the implementation of these procedural guidelines and its associated policy document.

7.0 REFERENCE TO OTHER DOCUMENTATION / LEGISLATION (Appendix 1)

7.1 Reference should be made to the following related documents:

- CPG59(b) – Confidentiality Procedure
- CPG59(a) – Data Protection Procedure
- CP / CPG53 – Whistle blowing Policy and Procedures
- CP / CPG25 – Freedom of Information Policy and Procedures
- CP / CPG50 – Information Governance and Security Policy and Procedures
- CP / CPG9 – Records Management Policy and Procedures
- CP61 – Paper and Electronic Corporate Records Procedure
- CP / CPG28 – Closed Circuit Television (CCTV) Policy
- CP60 / CPG60 – Information Sharing and Consent Policy and Procedures
- General Data Protection Regulation (2016)
- Data Protection Act 2018
- Police and Criminal Evidence Act 1984
- The Children's Act 1989
- Human Rights Act 2000
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998

- The Computer Misuse Act 1990
- The Access to Health Records Act 1990
- Access to Medical Records Act 1988
- Health and Social Care Act 2001 (Section 60)
- HSG (96)15:E5498 – The NHS IM&T Security Manual (Ensuring Security & Confidentiality in NHS Organisations)
- NHS Code of Practice: Confidentiality (Dept of Health Guidance)
- HSC 1990/012: Caldicott Guardians (Established the role of the Caldicott Guardian within Health Service organisations)
- HSC 2002/012: Caldicott Guardians & Implementing the Caldicott Standards into Social Care (Provides guidelines relating to sharing of service user identifiable information)
- HSC 1999/053: For the Record (Provides guidance to improve the management of NHS records, explains the requirements to select records for permanent preservation, lists suggested minimum requirements for records retention and applies to all information, regardless of the media, applicable to all personnel within the NHS such as service users, employees, volunteers etc.)
- ISO/IEC 27000 Series – Information Security Standards (This is the accepted industry standard for information management and security
- Health and Social Care Act 2012/2015
  (This list is not exhaustive)

END