Essex Partnership University
NHS Foundation Trust

DATA PROTECTION PROCEDURE

PROCEDURE REFERENCE NUMBER:	CPG59a
VERSION NUMBER:	2.2
KEY CHANGES FROM PREVIOUS VERSION	Covid-19 6 month extension applied
AUTHOR:	[redacted]
CONSULTATION GROUPS:	IGSSC
IMPLEMENTATION DATE:	MAY 2018
AMENDMENT DATE(S):	March 2018
LAST REVIEW DATE:	N/A
NEXT REVIEW DATE:	~~April 2020~~ October 2020
APPROVAL BY IGSSC	March 2018
RATIFICATION BY QUALITY COMMITTEE:	
COPYRIGHT	© Essex Partnership University NHS Foundation Trust 2018. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner

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 Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

DATA PROTECTION PROCEDURE

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 PROCEDURE

1.0 INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) defines data as any information which:

- is processed using equipment operating automatically in response to instructions,
- is recorded with the intention of being processed,
- is recorded as part of a relevant filing system,
- forms part of an accessible record, including health records.

1.2 Data Protection is about ensuring that personal data about an individual is processed fairly and lawfully in order to protect the rights of an individual.

1.3 Personal data, within the Trust, is taken to include:

- all identifiable person information, including health records,
- all identifiable staff information,
- any other identifiable personal information held on suppliers, contractors etc.

(***Note***: Whether held in electronic or paper form)

1.4 Certain types of data are regarded as sensitive, and the GDPR Article 9 stipulates that special measures must be taken in the processing and protection of this type of data. **"**Special categories of personal data**"** **(**Sensitive) data includes:

- racial and ethnic origins,
- political opinions,
- religious other similar beliefs,
- membership to a trade union,
- physical or mental health or conditions,
- sexual life,
- processing of genetic data
- biometric data for the purpose of uniquely identifying a natural person
- the commission of any offence, or
- any proceedings for any offence, or the sentence of any court in such proceedings.

1.5 The Trust collects and uses information about identifiable individuals in the course of its operations. This includes current, past and prospective patients, employees, suppliers, contractor clients / customers, and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of personal information to comply with the requirements

of government departments. Under the GDPR, all forms of personal information must be dealt with properly however it is collected, recorded and used – whether automatically, within accessible records or relevant filing systems – and there are safeguards to ensure compliance.

1.6 All staff employed by the Trust are affected by the GDPR

- they have rights as employees about whom data is held, and
- they have obligations as health care professionals who collect data about patients and clients.

2.0 DATA PROTECTION PRINCIPLES

2.1 The aims of this procedure are to deliver fully the Principles of Data Protection, as stated in the GDPR Article 5.
The Principles require that:

2.2 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 purpose;

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 which is inaccurate –having regard for the purpose they are processed for – are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than 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 & 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."

2.3 The Trust has to ensure that all information held on any media is accurate and up to date. The accuracy of the information can be achieved by implementing validation routines, some of which will be system specific and details must be provided of these validation processes to the system/information users.

2.3.1 A definition of data quality is a measure of the degree of usefulness of the data for a specific purpose. Data needs to be:

- ***Complete*** (in terms of having been captured in full)
- ***Accurate*** (the proximity of the figures to the exact or true values)
- ***Relevant*** (the degree to which the data meets current and potential user's needs)
- ***Accessible*** (data must be retrievable in order to be used and in order to assess its quality)
- ***Timely*** (recorded and available as soon after the event as possible)
- ***Valid*** (within an agreed format which conforms to recognised national standards)
- ***Defined*** (understood by all staff who need to know and reflected in procedural documents)
- ***Appropriately sought*** (in terms of being collected or checked only once during an episode)
- ***Appropriately recorded*** (in both paper and electronic records)

2.3.2 Staff should check with service users that the information held by the Trust is kept up to date by asking service users attending appointments to validate the information held.

2.3.3 Staff information should also be checked for accuracy on a regular basis – either by the manager or by the HR/Personnel department. The Trust needs to ensure that cases are closed, when appropriate.

The GDPR (Articles 12,15,16,17,18,19,20,21,22,35) provide the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

2.3.4 Some of these rights have to be determined by the courts and some are assessed on a case by case basis, but generally the Trust supports all of these principles.

2.3.5 Individuals whose information is held within the Trust have rights of access to it; regardless of the media the information may be held / retained.

Individuals also have a right to complain if they believe that the Trust is not complying with the requirements of the Data Protection legislation. *There are some exceptions to this in the area of Mental Health.*

2.3.6 The Trust must ensure an up to date procedure is in place to deal with requests for access to information.

2.3.7 The Access to Health Records Act 1990 will remain to provide access rights to relatives, or those who may have a claim, to deceased service user's records.

2.3.8 Individuals have a right to seek compensation for any breach of the Act which may cause them damage and/or distress.

2.3.9 The Trust will ensure the complaints procedures are reviewed to take account of complaints which may be received because of a breach or suspected breach of the GDPR or DPA 2018

2.4 The GDPR (Article 33, 34, 58, 83) requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

2.4.1 The Trust IM&T has a legal obligation to maintain confidentiality standards for all person identifiable information. This includes the disposal of non-clinical waste.

2.4.2 The Trust must ensure all electronic systems are maintained in line with the ISO/IEC 27000 series relating to Information Security Management.

2.5 The GDPR (Articles 45, 46, 49, 83, 84) imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

2.5.1 There is a statutory requirement for the Trust to notify the Information Commissioner, as part of the notification process, of any transfer of personal data to none EEA countries.

2.5.2 If you need to send person identifiable information to countries outside of the EEA you must discuss this with the Data Protection Officer, prior to any transfer taking place, as the levels of protection for the information may not be as comprehensive as those in the UK.

2.5.3 System Managers are required to check with software suppliers to ensure they conduct any development and bug fixes etc. within the UK or EEA. Where it is determined that any such development or support takes place in a country outside the EEA the Trust Data Protection Officer must be advised immediately. (See Appendix B)

2.5.4 It is advisable to check relevant, up to date information on this topic at, the Information Commissioners web site (www.ico.gov.uk) as part of risk assessment.

3.0 EXEMPTIONS

3.1 Article 23 enables Member States to introduce derogations to the GDPR in certain situations.

Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

There are specific reasons why access to personal data may be denied including:

- Where the data released may cause serious harm to the physical or mental condition of the patient, or any other person.
- Where access would disclose information relating to or provided by a third party (where consent has not been received by the third party to release their data). NB this does not include information recorded by the Trust employees as part of their normal duties.
- Where it is assessed that a patient, under the age of 16, cannot understand the implications of accessing their records.

(***Note***: refer to Access to Records Procedure (CPG9d))

4.0 RETENTION OF INFORMATION

4.1 The Trust will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which they will either be archived or destroyed. This will be done in accordance with the reasonable retention periods detailed in the Trust's Storage, Retention and Destruction of Records Procedural Guidelines (CPG9), which is compliant with the Department of Health Records Management NHS Code of Practice Part II, second edition 2009, and the Codes of Practice for the Management of Records Section 46 of the Freedom of Information Act 2000.

5.0 REPORTING BREACHES

5.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Any potential or actual breaches 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.

In the event of the loss of Trust equipment, IT need to be informed as soon as possible.

(***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 Electronic Staff Briefings
- On-Line training via the NHS Digital 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 (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 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.

END