Essex Partnership University
NHS Foundation Trust

INFORMATION RISK PROCEDURE

PROCEDURE REFERENCE NUMBER	CPG57
VERSION NUMBER	2
KEY CHANGES FROM PREVIOUS VERSION	Three year review; minor changes
AUTHOR	Information Governance Manager
CONSULTATION GROUPS	IGSSC
IMPLEMENTATION DATE	October 2017
AMENDMENT DATE(S)	June 18 (GDPR); Sept 21
LAST REVIEW DATE	September 2021
NEXT REVIEW DATE	September 2024
APPROVAL BY IGSSC	August 2021
RATIFICATION BY QUALITY COMMITTEE	September 2021
COPYRIGHT	

PROCEDURE SUMMARY

These procedures and their associated policy document will ensure that Essex Partnership University NHS Foundation Trust is compliant with its obligations to protect the Trust, its staff, patients, stakeholders and the wider general public from information risks and is compliant with its obligations under the General Data Protection Regulation (2016).

The Trust monitors the implementation of and compliance with this procedure 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 procedure is Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION RISK PROCEDURE

CONTENTS

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION RISK PROCEDURE

Assurance Statement

These procedures and their associated policy document will ensure that Essex Partnership University NHS Foundation Trust is compliant with its obligations to protect the Trust, its staff, patients, stakeholders and the wider general public from information risks and is compliant with its obligations under the General Data Protection Regulation (2016).

1.0 INTRODUCTION

1.1 Information used by the Trust is an important business asset in terms of both clinical management of individuals and the efficient management of services and resources and the substantial personal and confidential information relating to patients, the public and staff that the Trust holds and manages.

1.2 Information risk is inherent in all administrative and business activities and it is vital that confidentiality, integrity and availability of information is maintained and that everyone working for or on behalf of the Essex University NHS Foundation Trust (the 'Trust') understands and continuously manages information risk.

1.3 These procedural guidelines will underline the way in which the Trust manages personal and sensitive information / data and the risks associated with this activity ensuring that such information is dealt with in line with legislation, securely, efficiently and effectively and thus preserving the Trust's reputation.

1.4 The Trust places increasing reliance on technology, computers and, to an extent, third party contractors, to store and manage its information, and with the innovative ways by which information can be communicated, it is at a greater risk. It is therefore important that the Trust follows a consistent approach to safeguard its information, with due regard to the sensitive nature of same held, both in electronic and manual systems.

1.5 The Board of Directors recognises that the aim of information risk management is not necessarily being able to eliminate risk, but rather to provide the structural means to identify, prioritise and manage the risks involved in all Trust activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

2.0 INFORMATION RISK

2.1 The key to managing information risk is to identify, risk assess and monitor information assets across the organisation ensuring any breaches of confidential information / data / assets are reported in accordance with Trust policy.

2.2 Information assets come in many shapes and forms and it is generally best to group information assets in a logical manner and the Trust will manage its information assets by Directorate.

2.3 Information assets include, but are not restricted to:

Personal Information Content	Databases; data files; back-up data; archive data; audit data; paper records (patient case notes / staff records); paper reports
Other Information Content	Databases; data files, audit data; paper records; paper reports
System / Process Documentation	System information and documentation; operations and support procedures; manuals and training materials; contracts and agreements; business continuity plans
Software	Applications and system software; data encryption utilities; development and maintenance tools
Hardware	Computing hardware including: PCs, laptops, PDA, communication devices, e.g. Blackberries and removable media, iPhones, iPads, etc.
Miscellaneous	Environmental services, e.g. power and air conditioning; people skills and experience; shared service (including networks and printers); computer rooms and equipment; records libraries

3.0 RESPONSIBILITIES

3.1 SIRO (Senior Information Risk Owner)

3.1.1 The SIRO will have responsibility for the management of information risks, ensuring regular reporting mechanisms are established (quarterly) with Information Asset Owners / Administrators (IAOs / IAAs) and the Information Governance Manager to monitor those risks through the medium of the Information Governance Group.

3.1.2 The Information Governance Manager will provide ad hoc reports to the Quality Committee and the Information Governance Steering Sub-Committee advising of the processes / systems put in place to manage identified risk.

3.2 IAOs / IAAs

3.2.1 Electronic registers of the Trust's information assets will be held by the IAOs / IAAs of the relevant Directorate with an overall register held by the Information Governance Manager.

3.2.2 IAOs / IAAs will be responsible for ensuring a review of information data flows and asset registers and undertaking risk assessments to identify any information risks.

3.2.3 IAOs / IAAs will provide the SIRO with a regular written report, quarterly, advising of any new information risk and updating on actions identified to address known risks.

3.3 Information Governance Manager

The Trust's Information Governance Manager will initiate and continually update and review a process for recording information flows which in turn will assist in the identification of information assets.

Information risks and associated action plans to reduce or eliminate the risk will be monitored by the Information Governance Steering Sub-Committee / Quality Committee.

Information risks will be risk assessed in line with the Trust's overall Risk Management Strategy.

3.4 Data Protection Officer

The DPO has the expert knowledge of data protection law and practices and detailed understanding of the organisation's business, the purposes for which it processes, or intends to process personal data

The DPO facilitates 'accountability' and the organisations ability to demonstrate compliance with the GDPR

To be available to be contacted directly by data subjects – the contact details of the data protection officer will be published in the organisation's privacy notice.

The Data Protection Officer will take responsibility for providing expert advice and the promotion of data protection compliance and best practice.

3.5 All Staff

All staff will be responsible for managing the risk associated with the information / data that they handle and for ensuring that any identified risks are escalated through line management.

4.0 MANAGING INFORMATION RISK

4.1 Data Flow Mapping

In order to assess where information risks may come from the Trust will undertake regular data flow mapping exercises and updates. Data flow mapping supports the development of Asset Registers and ensures the Trust is aware of any risk areas. This work will be undertaken on an individual basis and in line with national guidance (the most current version of the Information Governance Toolkit).

4.2 Asset Registers

Asset Registers are a recorded document of the Trust's information assets and include detail of, e.g. databases, data files, systems, manuals, etc. See 4.3 above.

The development of the Trust's information asset register will fall out of the data flow mapping exercises with registers being reviewed and amended in line with updates to data flow mapping.

Information assets, amendments, reviews updates and management of identified risks will be the responsibility of the Information Asset Owners supported by, where appropriate, Information Asset Administrators.

4.3 Information Risks

Risks to information / data / assets will be identified through a variety of measures, for example from:

- data flow mapping
- management of Asset Registers
- information governance / security awareness programmes
- Incidents and lessons learned from incidents

Identified risks will be risk rated according to the Trust's risk management strategy and associated risk rating matrix and escalated as appropriate via the most appropriate committee / group (Information Governance Sub-Committee, Trust Records Group, Clinical Governance Sub-Committee / Quality Committee).

Any high risk areas will be escalated through to the Trust's Executive Team / Board of Directors for further advice and guidance.

4.4 Incident Reporting

The reporting of information / data breaches will be undertaken in line with the Records Management, Information Governance / Security and Adverse Incident procedures.

5.0 REPORTING

5.1 Regular reports on data flow mapping, asset registers and the management of information risks will be provided to the SIRO and / or appropriate groups / committees.

5.2 Ad hoc reports will be provided to the Executive Team / Board of Directors when required to advise of newly identified risk, updates to known risks.

6.0 TRAINING

6.1 Training required to manage information risks will fall out of information governance / security training programmes and where appropriate, will be facilitated by the information governance leads (e.g. data flow mapping, asset registers).

7.0 MONITORING AND AUDIT

7.1 Monitoring will take place through internal and external audit of information governance / security processes and the Information Data Security & Protection Governance Toolkit.

END