Essex Partnership University
NHS Foundation Trust

Information Asset Register Procedure

PROCEDURE REFERENCE NUMBER:	CPG50g
VERSION NUMBER:	2
KEY CHANGES FROM PREVIOUS VERSION	3 year review
AUTHOR:	Information Governance
IMPLEMENTATION DATE:	May 2018
LAST REVIEW DATE	May 2021
NEXT REVIEW DATE:	May 2024
APPROVAL BY IGSSC:	April 2021
APPROVAL BY QUALITY COMMITTEE	May 2021
COPYRIGHT	

PROCEDURE SUMMARY
This document sets out the procedure to ensure that all information assets are identified and regularly assessed to ensure the confidentiality and security of the organisations information is maintained.
The Trust monitors the implementation of and compliance with this procedure in the following ways:
All Information Governance Policies and the Information Governance Toolkit Developed in line with NHS England guidance and the Caldicott Review.

Services	Applicable	Comments
Trustwide	✓	IAO & IAA applicable

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

Information Asset Register Procedure

1.0 INTRODUCTION

1.1 This policy applies to Essex Partnership University NHS Foundation Trust, subsequently referred to in this document as 'the Trust'.

1.2 Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure they are protected at all times and are available and accurate to support the operation of the organisation. The Trust must ensure that all information assets that hold or process personal data are protected by technical and organisational measures appropriate to the nature of the asset and the sensitivity of the data. There should be formal information security risk assessment and management programme and operating systems under the organisations control must support appropriate access control functionality.

1.3 All information assets of the Trust should be identified and the Trust must have a nominated Senior Information Risk Owner (SIRO). The SIRO is required to ensure owners are identified for all Information Assets, Information Asset Owners (IAOs), with responsibility for managing the risks to those assets. Whilst responsibility for implementing and managing Information Asset controls may be delegated to Information Asset Administrators (IAAs) or equivalent, accountability should remain with the nominated owner of the asset.

1.4 The Department of Health has issued guidance to all NHS organisations on the process to be followed in identifying information assets, and allocating local ownership and responsibility for assessing any risk of data loss or information security for these assets. It is part of the guidance that risk assessments are performed regularly to ensure that the organisation complies with the Information Governance Assurance Programme and regular risk assessments are a requirement in the Information Governance Toolkit (IGT), which is mandated for all NHS organisations.

1.5 Potential losses arising from breaches of IT and information security include physical destruction or damage to the organisations computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions. In addition, healthcare organisations process personal confidential data (PCD) of particular sensitivity, which needs to be protected from loss or inappropriate disclosure.

2.0 OBJECTIVE

2.1 All information assets should be accounted for, understood, have a designated owner and be appropriately protected.
This will ensure compliance with:

- The Data Protection Act 2018 (DPA)
- The General Data Protection Regulation (GDPR)
- The Caldicott Report and subsequent review on personal confidential data
- The Information Security standard ISO 27001/2

3 SCOPE

3.1 The Information Asset Register Procedure applies to all business functions across the Trust, and covers information, information systems, networks, physical environment and relevant people who support those functions. It relates to both manual and electronic information, whether transmitted across networks or telephone lines, sent by fax, spoken in conversations or printed as hard copy (see **Appendix 2** for examples of information assets).

4 INFORMATION ASSET OWNERS (IAOs)

4.1 Information Asset Owners (IAO) are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. The SIRO/IAO hierarchy identifies accountability and authority to effect change where required to mitigate identified risk

(see risk assessment process at **Appendix 3**).

4.2 The role of the Information Asset Owner is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good. The Information Asset Owner will also be responsible for providing or informing regular written reports to the SIRO, a minimum of annually on the assurance and usage of their asset.

4.3 The information asset owner will:

- ensure access to the asset is appropriately controlled in accordance with its classification and the Trust policies on information security, confidentiality, access and information sharing.

- ensure that the backup and business continuity arrangements are appropriate in accordance with its classification

- ensure that the asset is managed in accordance with the GDPR, DPA data protection principles and Caldicott Principles if the information asset processes Personal Confidential Data.

5 INFORMATION ASSETS

5.1 Information Assets (IA) are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation. Information assets are likely to include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data. Non-computerised records systems should also have an asset register containing relevant file identifications and storage locations.

5.2 Business processes and activities, applications and data should all be considered as Information Assets; however, their importance to the Trust may vary (Appendix 2).

6 INFORMATION ASSET REGISTER

6.1 Information Assets should be documented in a Trust asset register (IG Toolkit requirement, template at Appendix 1). In practice, a number of Trust asset registers may exist (e.g. departmental, HR Register, hardware register), and many will be *ad hoc*. As a priority, it is essential that all critical Information Assets are identified and included in this asset register, together with details of the 'Information Asset Owner' and risk reviews undertaken. The corporate Business Continuity Plan will also list these as critical information assets.

6.2 Each Information Asset Owner should be aware of what information is held and the nature and justification of information flows to and from the assets they are responsible for.

7 IDENTIFICATION OF NEW ASSETS

7.1 The Data Security & Protection Toolkit has a requirement for a documented plan to be developed to investigate and identify all remaining information assets that comprise or hold personal data and to assign responsibility for any identified, including details in the information asset register (IAR).

7.2 The Plan will be implemented by:

- Ensuring that Data Privacy Impact Assessments (DPIA) are included in any procurement process where new systems are implemented. This has a data mapping form within the template to ensure new assets are captured.

- The asset register will be reviewed by the Trust on a regular basis (at least annually) and circulated to all staff for them to review and refresh the asset register.

- The Asset Register will be reviewed at the Information Governance Steering Sub-Committee annually.

8 RISK

8.1 Appropriate security measures must be viewed as necessary for protection against a risk of an event occurring or to reduce the impact of such an event. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

The Threat — Of something damaging the confidentiality, integrity or availability of information held on systems or manual records.

The Impact — That such a threat would have if it occurred.

The Chance — Of such a threat occurring.

8.2 All new projects and procurements of IT systems will have a risk assessment as part of the project, and any existing systems should have periodic risk assessments, including those carried out by local management and internal/external audit services. Any risks identified as high must be reported to the Data Protection Officer (or equivalent) and if appropriate recorded on the IG risk register and/or escalated to the Trust corporate risk registers and Governing Bodies.

8.3 Controls can then be implemented to reduce the assessed risks in one of the following ways:

- Avoid the Risk
- Transfer the Risk
- Reduce the Threats
- Reduce the Vulnerabilities
- Reduce the Possible Impact
- Detect Unwanted events, react and recover from them.

There will always be residual risks and these should be reviewed on a regular basis to ensure that additional controls are having an effect on the likelihood rating. Risk Assessment Process is **Appendix 3.**

9 EQUALITY IMPACT ASSESSMENT

9.1 The Trust aims to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all. This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the Trust must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

10 DUE REGARD

10.1 This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

11 PROCEDURE REVIEW

11.1 This procedure will be reviewed in line with Data Security & Protection Toolkit requirements or where changes occur in national policy or legislation.

END