INFORMATION RISK POLICY

POLICY REFERENCE NUMBER | CP57
VERSION NUMBER | 1.2
KEY CHANGES FROM PREVIOUS VERSION | Further 3 month covid extension
AUTHOR | Information Governance Manager
CONSULTATION GROUPS | IGSSC
IMPLEMENTATION DATE | October 2017
AMENDMENT DATE(S) | N/A
LAST REVIEW DATE | N/A
NEXT REVIEW DATE | October 2020 March 2021
APPROVAL BY IGSSC | 15th June 2018
RATIFICATION BY QUALITY COMMITTEE | 13th September 2018
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

This policy ensures 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.

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

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is
The Executive Chief Finance Officer
1.0 INTRODUCTION
2.0 AIMS AND OBJECTIVES
3.0 SCOPE
4.0 RESPONSIBILITIES
5.0 DEFINITIONS
6.0 RISK MANAGEMENT STRUCTURE
7.0 TRAINING
8.0 IMPLEMENTATION
9.0 MONITORING
10.0 REFERENCE OTHER DOCUMENTS

APPENDICES

APPENDIX 1 – RISK PRIORITISATION SYSTEMS

APPENDIX 2 – INFORMATION GOVERNANCE RISK MANAGEMENT STRUCTURE
INFORMATION RISK POLICY

Assurance Statement
This policy ensures 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.

1.0 INTRODUCTION

1.1 Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Essex Partnership University NHS Foundation Trust (the ‘Trust’) continuously manages information risk.

1.2 The Board acknowledges that information risk management is an essential element of broader information governance / security and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions. This is achieved through key approval and review processes / controls – and not by imposing risk management as an extra requirement.

1.3 This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff, stakeholders and the Trust itself and therefore mechanisms to achieve and maintain appropriate protection of the Trust’s business critical information assets, will be developed through the maintenance of an Information Asset Register.

1.4 The risks associated with not complying with this policy include litigation, breach of law as well as loss of reputation to the Trust and potential impacts on service users.

2.0 AIMS AND OBJECTIVES

2.1 The Information Risk Policy will:

- Protect the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant ensuring information is held securely and used appropriately
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes
- Encourage pro-active rather than re-active information risk management
- Provide assistance to and improve the quality of decision making throughout the Trust
- Meet legal or statutory requirements
- Assist in safeguarding the Trust’s information assets
2.2 The following list provides some examples of where / how potential information risks can occur:

- Loss of data held on portable data storage devices (e.g. laptop, memory sticks, dictaphone tapes, iPhones, iPads, etc.)
- Incorrect use of passwords
- Incorrect use of smartcards
- Inappropriate access to personal information
- PC workstation security

The above list is not exhaustive.

3.0 SCOPE

3.1 This policy is to be made available to all Trust staff and observed by all members of staff, both clinical and administrative.

3.2 Information risk should be managed in a robust way within all work areas and should not be seen as the sole responsibility of the Information Governance Team.

3.3 This policy is applicable to all areas of the Trust and adherence should be included in all contracts for out-sourced or shared services. There are no exclusions.

4.0 RESPONSIBILITIES

4.1 The Chief Executive
The Chief Executive has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputational risks.

4.2 Executive Chief Finance Officer and Senior Incident Risk Officer (SIRO)
The Executive Chief Finance Officer (SIRO) has overall responsibility and is familiar with and takes ownership for the implementation and management of the Trust’s information risk policy, with day to day management of the information risk management programme including information privacy and security and will provide assurances / advice to the Board of Directors in relation to information risk, governance and security through periodic reports and briefings.

4.3 Associate Director of System Implementation and Data Quality
The Associate Director of System Implementation and Data Quality will lead the Information Governance Team who will be responsible for the overall implementation and management of national and local guidance on information governance / security / risk, ensuring that processes and systems are established.
4.4 **Information Governance Manager**

The Information Governance Manager will oversee the day to day implementation of processes and systems in relation to information governance / security / risk coordinating the management of the Information Governance Toolkit and local / national guidance acting as a central point of contact / advice for both staff and external organisations.

4.5 **Information Asset Owners (IAOs)**

IAOs will be senior individuals (Deputy, Associate, Assistant Directors) whose role will be to understand and address risks to the identified information assets they ‘own’ and to provide assurances to the SIRO on the security and use of those assets through the process of implementation of information governance / security guidance.

4.6 **Information Asset Administrators (IAAs)**

IAAs will support the IAOs by ensuring that policies and procedures are followed, recognising actual or potential security incidents, consulting IAOs and the Information Governance Manager on incident management, and by ensuring that information asset registers are maintained accurate and up to date.

5.0 **DEFINITIONS**

5.1 Key definitions are:

- **Risk**
  The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood (see Appendix 1).

- **Consequence**
  The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

- **Likelihood**
  A qualitative description or synonym for probability or frequency.

- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.

- **Risk Management**
  The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

- **Risk Treatment**
  Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
    o Avoid the risk
    o Reduce the likelihood of occurrence
    o Reduce the consequences of occurrence
    o Transfer the risk
    o Retain/accept the risk

- **Risk Management Process**
  The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
6.0 POLICY REFERENCES / ASSOCIATED DOCUMENTATION

6.1 To build robust management of information risk the Trust will develop an information governance / security structure relying on the identification and ownership of information assets ensuring a structured approach to reporting and addressing risk.

6.2 The Trust's information risk structure will be developed based on guidance from the Digital Information Policy team, NHS Connecting for Health: NHS Information Risk Management (January 2009), see Appendix 2.

7.0 TRAINING

7.1 To manage information risk effectively all staff will be required to undertake appropriate information governance / security training.

7.2 A staff training needs analysis will be undertaken in line with national guidance and requirements and a record of mandatory training will be kept.

7.3 Information governance / security training is mandatory and will be undertaken via the Trust's OLM e-learning system.

For some specialist staff groups additional training will be required and identified within the Information Governance Toolkit Training Tool.

7.4 The Information Governance Toolkit sets out the compliance levels required and completion of the training modules is recorded and monitoring by information governance leads. Mapping reports will be monitored and sent to operational managers and directors identifying which of their staff are not compliant.

8.0 IMPLEMENTATION

8.1 The management of information risk is complex and the Trust has therefore developed a procedural guideline to support implementation of this policy. These guidelines are available via the Trust's intranet site. They provide comprehensive information and guidance, where appropriate, that ensures all Trust staff are aware of their responsibilities in relation to the management of information / data.
9.0 MONITORING

9.1 The Executive Chief Finance Officer (SIRO) is responsible for monitoring the implementation and effectiveness of this policy and related procedural guidelines.

9.2 Monitoring of identified information risks and asset registers will be undertaken by the Trust’s Information Governance Steering Sub-Committee / Integrated Quality and Governance Steering Committee.

9.3 Information governance leads will provide the Board of Directors with ad hoc updates on any high level risks (red) which need escalating to the Board for further guidance to address those risks.

9.4 Implementation of this policy and its associated procedural guidelines will be undertaken as part of the overall Trust’s policy implementation audit programme.

10.0 REFERENCE OTHER DOCUMENTS

10.1 The following documents should be considered, read in conjunction with this policy and its procedural guidelines:

- Information Governance / Security policy / procedures
- Risk Management Framework
- Adverse Incident policy / procedures— including Serious Untoward Incidents procedures
- Records Management policy / procedures
- Data Protection & Confidentiality policy / procedures
- Checklist for reporting, managing and investigating Information Governance Serious Untoward Incidents (Gateway ref: 13177)
- Conduct and Capability policy / procedures
- Information Governance Toolkit (current version)

END