Essex Partnership University
NHS Foundation Trust

INFORMATION GOVERNANCE & SECURITY PROCEDURE

PROCEDURE NUMBER:	CPG50
VERSION NUMBER:	2
KEY CHANGES FROM PREVIOUS VERSION	GDPR
AUTHOR:	Information Governance Team
CONSULTATION GROUPS:	IGSSC
IMPLEMENTATION DATE	April 2017
AMENDMENT DATE(S)	July 2018
LAST REVIEW DATE	July 2018
NEXT REVIEW DATE	July 2021
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE	September 2018
RATIFIED BY QUALITY COMMITTEE	N/A
COPYRIGHT	

POLICY SUMMARY		
The purpose of these procedural guidelines is to establish the governance arrangements and responsibilities for information security providing a framework through which the elements of information governance / security will be met. This will make sure that the intention to promote and build a level of consistency across the Trust to safeguard information is achieved and ensure it is understood and that all Trust staff are aware of their individual responsibilities. The risk associated with not having a procedure document in relation to information governance / security and access to Trust facilities (IT, Email, Internet, Portable Media) is an uncoordinated approach to its safe use which could render the Trust vulnerable in terms of legal implications of staff use of facilities and lack of organisational controls to safeguard users and 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 The Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION GOVERNANCE & SECURITY PROCEDURE

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION GOVERNANCE & SECURITY PROCEDURE

Assurance Statement

1.0 INTRODUCTION

1.1 These procedural guidelines aim to set out the Essex Partnership University NHS Foundation Trust's (the "Trust") rules relating to information governance / security and apply to all business functions and cover all information systems, networks, physical environment, third party contractors, and relevant people who support those business functions.

1.2 The information used by the Trust is an important business asset in terms of both the 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 employees that the Trust is required to hold and manage. It is vital that the confidentiality, integrity and availability of information / data is maintained. Information governance / security deals with the way an NHS Trust handles personal and sensitive information / data and allows the organisation and individuals to ensure that such information is dealt with in line with legislation, securely, efficiently and effectively and in doing so preserving the Trust's reputation.

1.3 Increasing reliance is placed on technology, computers and, to an extent, third party contractors, to store and manage information, and with 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 some held, both in electronic and manual systems.

1.4 The principle objective of information governance / security management is to implement appropriate administrative, technical and physical safeguards to ensure the security of these assets.

2.0 GENERAL INFORMATION

2.1 It is the policy of the Trust that all information / data systems operated by the Trust (electronic or manual) are secure systems, which comply with the requirements of the Data Protection Act, the Computer Misuse Act, the British Standard for Information Security ISO/IEC 27000 series (using the International Standard Organisations Code of Practice ISO27002) and the Information Governance Toolkit, as appropriate. It is the aim of the Trust that its entire staff will be aware of the need to maintain secure systems and that staff will fully understand their responsibilities as outlined in these procedural guidelines.

2.2 Line managers will be responsible for ensuring that their staff are aware of these procedures and their contents and for ensuring that their staff abide by them.

2.3 Failure by any employee of the Trust to abide by the contents of this document will be viewed as a serious matter and may result in disciplinary action.

2.4 This document sets out the Trust processes for the safe and legal use of the facilities provided by the Trust, for example, internet / Email access, IT and portable media and paper / manual processes and should be read and observed by any member of staff using these facilities.

3.0 IMPLEMENTATION & MANAGEMENT

3.1 Information governance / security is not just a matter of restricting unauthorised access to information / data, it is also a question of ensuring that the confidentiality, integrity and availability of the information / data is maintained.

3.2 The appendices attached to these procedural guidelines will provide detailed information on the processes to be followed to ensure that information governance / security guidance is met in relation to:

- Integrated Governance Strategy
- Information Governance Framework
- Records Strategy
- IM&T Security Policy
- Virtual Private Network (VPN) Remote Access Policy / Procedures
- Data Protection and Confidentiality Policy / Procedures
- Freedom of Information Policy / Procedures
- Health Records Management Policy / Procedures
- Data Quality Policy
- Closed Circuit Television (CCTV) Policy / Procedures
- Information Governance and Security Policy
- IT&T Security Procedures
- Internet/Intranet/Email Access and Use Procedures
- Incident Reporting Procedures
- Information Sharing and Consent Policy / Procedures
- Paper and Electronic Corporate Records (Laserfiche) Policy / Procedures

This list is not exhaustive....

4.0 RISK

4.1 The Director of ITT will ensure that each of the Trust's systems is subject to regular security risk assessments. The degree of detail of the assessment will depend on the value of the asset(s). All reports produced will remain confidential.

4.2 To ensure compliance of systems with NHS security policies and standards the Trust will ensure that the security of IT&T systems will be regularly assessed. Risk assessments will be regularly carried out and the technical and IT&T facilities checked for compliance with ISO/IEC 27000 series - Information Security Management, the Code of Practice for information Security, which forms the basis of the NHS security policy.

4.3 Key leads will manage risk by identifying, controlling and minimising risk to an acceptable level, by undertaking appropriate risk assessment processes to assess threats, vulnerabilities and the resulting impact upon information assets.

4.4 Any risk that cannot be reduced to an acceptable level by imposing existing Trust controls (e.g. policy, procedure, process) will be escalated to the Information Governance Steering Sub-Committee / Quality Committee as appropriate and entered onto the information governance / security risk register for monitoring by same.

4.5 The processes involved in risk analysis will be to identify and value the asset(s), threats and vulnerabilities and then calculate the risk.

4.6 **Countermeasures**

4.6.1 Introducing 'countermeasures' will involve identifying, selecting and adopting appropriate and cost-justified security and contingencies in order to reduce risks to an acceptable level.

4.6.2 These 'countermeasures' may act in different ways, including:

- Reducing the likelihood of attacks or incidents occurring.
- Reducing the system's vulnerability.
- Reducing the impact of an attack or incident, should it occur.
- Detecting the occurrence of attacks or incidents.
- Assisting the progress of recovery from an attack or incident.

4.6.3 The Security Officer will regularly re-examine the use of any countermeasures and their continuing suitability and effectiveness. A report will be produced following any assessment.

5.0 TRAINING

5.1 All Trust staff will undertake, as part of their general induction, mandatory training on information governance / security and related areas such as confidentiality, Data Protection, record keeping.

5.2 Specific staff training will be undertaken by those staff appointed with key roles in relation to information governance / security, e.g. Information Governance Managers / Information Security Officers and Information Asset Owners.

5.3 All mandatory training will be recorded for monitoring purposes. Reference should be made to HR21 – Induction and Mandatory Training Policy and related Procedures.

6.0 MONITORING, REVIEW AND PERFORMANCE MANAGEMENT

6.1 The Quality Committee will have overall responsibility for overseeing the implementation of these procedural guidelines and will take forward any action relating to information governance / security within the Trust.

6.2 The Information Service Management Board and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of these guidelines.

6.3 These procedural guidelines will be reviewed every three years in line with Trust policy unless changing circumstances or central policy requires an earlier review.

6.4 The Information Governance Manager and / or Information Security Officers will provide the Quality Committee, the Executive Team and Board of Directors with relevant reports on information governance / security developments, breaches and facility usage on a regular basis, in line with Committee schedules.

6.5 Trust information governance leads will undertake internal audit of staff awareness of information governance / security on a yearly basis via the media of staff questionnaires. Outcomes of these audits will be reported to the Information Governance Steering Sub-Committee for action planning to address any gaps.

6.6 The use and any misuse / abuse of the Trust's electronic facilities (e.g. Email, Internet) will be monitored by the IT&T department and outcomes will be provided to the Executive Team as part of the Performance Department's Quarterly Performance Monitoring Report.

6.7 Any breaches in information governance / security will be investigated in line with Trust policy (Serious Untoward Incidents [CP3/CPG3], Information Incident Reporting Procedures (CPG50) and / or Disciplinary Policy [HR27/HRPG27]) and reported through the Information Governance Steering Sub-Committee / Caldicott Network as appropriate. The Caldicott Network will be responsible for:

- escalating any issues to the Quality Committee
- ensuring the actioning and publication of lessons learned following any breach investigations across the Trust

7.0 REFERENCE TO OTHER DOCUMENTATION / LEGISLATION

7.1 This document should be read in conjunction with other national guidance, Trust policies and procedures and other relevant legislation, including:

- Information Quality Assurance
- British Standard for Information Security ISO/IEC27000 series
- NHS Caldicott Report Recommendations
- The National Health Service Act (2006)
- Data Protection Act (2018)
- Access to Health Records Act (1990) (Where not superseded by the Data Protection Act (2018))
- Freedom of Information Act (2000) (FOI) (including Publication Scheme)
- The Environmental Information Regulations (2004) (EIR)
- Computer Misuse Act (1990)
- Electronic Communications Act (2000)
- The Re-Use of Public Sector Information Regulations (2005)
- The Civil Contingencies Act (2004)
- The Human Rights Act (2000)
- The Copyright, Designs and Patents Act (1988) (as amended by the Copyright Computer Programs Regulations (1992))
- The Health and Safety at Work Act (1974)
- Regulation of Investigatory Powers Act (2000)
- Crime and Disorder Act (1998)
- Health and Social Care Act (2000)
- The Common Law Duty of Confidentiality
- General Data Protection Regulation

This list is not exhaustive.....

END