NHS
Leeds
Clinical Commissioning Group

DATA SECURITY AND INFORMATION GOVERNANCE TRAINING STRATEGY

Version:	1.3
Ratified by:	Audit Committee
Date ratified:	February 2022
Name & Title of originator/author:	Karen Rowe, Information Governance Manager
Name of responsible committee/individual:	Information Governance /Business Intelligence/IT Committee
Date issued:	February 2022
Review date:	February 2023
Target audience:	All Staff

Table of Contents

1 Introduction

NHS Leeds Clinical Commissioning Group (CCG) recognises the importance of staff completing data security awareness training to ensure that the duty of confidentiality owed to patients, families, staff and business partners is respected. A trained workforce confidently uses and shares information fairly and lawfully in the best interests of patients.

2 Aims

The aim of this strategy is to specify the training requirements that are in place to ensure that all staff understand their responsibilities with regard to any information which they come into contact with in the course of their work and to provide assurance to the Governing Body that such information is dealt with legally, securely, efficiently and effectively.

Annual data security awareness training is a mandatory requirement for all staff, to ensure that staff are aware of the duty to share (fairly and lawfully) and how this affects both activity within the CCG and also the local health and wider community in Leeds.

Compliance with the data security awareness training requirements serves to ensure:

- compliance with the UK General Data Protection Regulation and Data Protection Act 2018
- we fulfil the requirements of the Data Security Standards as published by NHS Digital Commission and National Data Guardian
- the confidentiality and legitimate use of personal or medical information
- consent is obtained where appropriate and/or individuals are fully aware of the uses of their personal data
- the accuracy, availability and integrity of records held by the organisation
- appropriate technical and organisational measures are in place to protect information against security threats

3 Scope

This strategy documents the training requirements of all staff who work for or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, Governing Body members, students and any staff working on an individual contractor basis and/or who are employees for an organisation contracted to provide services to the CCG. The strategy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

Access to training for agency and contract staff is dependent on the responsible manager informing Human Resources of the new starter and completing the appropriate forms.

Additionally, a secondary aim is to ensure that specialist data security awareness training is targeted at specific staff groups across the organisation to comply with a number of the Information Governance/Data Security and Protection Toolkit requirements.

4 Accountability/Responsibilities

The Audit Committee is responsible for the review and approval of this strategy, related work plans and procedures and will receive regular updates on compliance and any related issues or risks oversees, monitors and reviews the implementation of information governance

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) has organisational responsibility for all aspects of risks associated with information governance, including those relating to confidentiality and data protection. The SIRO will ensure that an appropriate management framework is put in place. This role is undertaken by the Chief Finance Officer.

Caldicott Guardian

The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for handling patient identifiable information. The Caldicott Guardian approves any use of patient identifiable information. This role is undertaken by the Clinical/Medical Director.

Information Asset Owners and Administrators

A number of senior managers are assigned as Information Asset Owners (IAO) and are directly accountable to the SIRO in relation to their information risks. IAOs provide assurance that information risk is being managed effectively in respect of the information assets that they are responsible for and that any new aspects or changes introduced to their business processes and systems undergo a privacy impact assessment.

An Information Asset Administrator (IAA) may be assigned by an IAO. An IAA will have delegated responsibility for the operational use of an information asset. They will report any risks associated with an information asset (that falls under their responsibility) to the IAO and consult with the IAO where necessary about the operation of an information asset.

Heads of Service

Heads of Service are responsible for ensuring that they and their staff are familiar with this strategy and associated guidance. Training compliance should be monitored by the Heads of Service and any further training needs identified through the appraisal process. They must ensure that any breaches of the strategy are investigated and acted upon.

Employees

Annual data security awareness training compliance is mandatory for all staff. Staff should note that there is a confidentiality clause in their contract and that they are expected to participate in induction training, annual refresher training and awareness raising sessions carried out to inform/update staff on data security and protection issues. Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer system is a disciplinary offence, which could result in dismissal or termination of an employment contract, and must be reported to the SIRO and (in the case of health or social care records) the Caldicott Guardian.

All employees are personally responsible for compliance with the law in relation to data protection and confidentiality and will need to be aware of their responsibilities in relation to any information

governance related legislation that may affect their work duties e.g. Freedom of Information Act. Other responsibilities in relation to a specific policy will be detailed in that policy.

Information Governance Team

The Information Governance team are available to provide information governance advice and guidance.

5 Key Principles

The strategy links directly to the following:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Confidentiality: NHS Code of Practice
- Caldicott Principles

Data security awareness training is mandatory for all staff. This includes awareness and understanding of Caldicott principles and confidentiality, information security and data protection. Completion of data security awareness training must be included in induction for all new staff and completed within 10 working days of their starting date. The Information Governance and Information Security handbooks must be read, prior to any access being provided to the CCG network (available on the extranet).

The necessity and frequency of any further training will be Personal Development Review (PDR) or role based.

6 Implementation and Dissemination

The basic mandatory Data Security Awareness training requirement is fulfilled by completion of the Data Security Awareness Level 1; this can be accessed through ESR, face to face workshops, Virtual training via MS Teams or alternatively through the Elearning for Health portal although should only be used for staff who are not recorded on ESR.

All new staff, directly or indirectly employed, are expected to have completed, or have access provided on their first day of employment, to complete the online elearning (as specified in the induction checklist). Staff are advised to retain a certification of completion for their own records.

7 Training Needs Analysis:

Staff Group	Level	Training Objective/Aim	Module Name	Method of Delivery	Frequency of Training
New starters	Basic	To ensure new starters to the CCG are informed of their responsibilities to maintain good Information Governance and ensure data security.	Data Security Awareness Level 1 Training	E-learning / Face to face workshop / MS Teams Virtual training	Once – within 10 working days of starting in role
All Staff (including Board Members)	Basic	To ensure all staff are informed of their responsibilities to maintain good Information Governance and ensure data security.	Data Security Awareness Level 1 Training	E-learning / Face to face workshop / MS Teams Virtual training	Annually
Information Asset Owners (IAOs)	Intermediate	To describe the key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties.	**TBC**	E-learning / Face to face workshop / MS Teams Virtual training or certified course provider	3 yearly
SIRO	Expert	To assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.	GDPR Practitioner Course SIRO training provided by a certified provider	E-learning or certified course provider	Upon appointment and then annually

Staff Group	Level	Training Objective/Aim	Module Name	Method of Delivery	Frequency of Training
Caldicott Guardian	Expert	To fully understand the role and function of the Caldicott Guardian.	Recognised UK Guardian Council Caldicott Guardian training	E-learning or certified course provider	Annually
Data Protection Officer	Expert	In depth understanding of the General Data Protection Regulation and Data Protection Act (and associated legislation) and information security	GDPR Practitioner Course	Certified Course provider	Continuous development as new legislation is introduced or updated
Cyber Assurance and Compliance Manager	Expert	In depth understanding of the General Data Protection Regulation and Data Protection Act (and associated legislation) and information security	Healthcare Information Security and Privacy Practitioner (HCISPP) / Certified Information Systems Security Professional(CISSP)	Certified Course provider	When the qualification expires or specific to HCISPP, 4 years. Or CISSP, 5 years
Information Governance Manager / FOI Lead	Expert	In depth understanding of the General Data Protection Regulation and Data Protection Act (and associated legislation) and information security	British Computer Society (BCS) Data Protection, FOI Practitioner course, GDPR Practitioner Course	Certified Course provider	Continuous development as new legislation is introduced or updated

8 Compliance

The effectiveness of the training will be demonstrated in a number of ways:

Measure	Detail
Reactive Evaluation	Training feedback forms assessing the trainer's performance as well as whether training objectives were met, should be provided for class room based learning events.
Evaluating Learning	Increase in knowledge after the training is measured by post training assessment test (either online assessment test or paper based assessment test). 80% is the pass mark for the assessments. Successful achievement of the assessment test is recorded against the learners training record.
Behaviour	The extent to which data security and protection training has been put into practice will be subjectively measured by: 1. The results of regular staff IG compliance checks 2. Staff IG awareness survey (typically administered via questionnaire) 3. Numbers of Information Governance related incidents, near misses and risks reported

All staff are responsible for ensuring they remain up to date with all statutory and mandatory training requirements. Line Managers should regularly review training attainment of their staff and take appropriate action to ensure the organisation remains compliant.

9 Associated Policies and Procedures

- Data Protection and Confidentiality Policy
- Incident Management Policy and Guidance
- Information Governance Policy and Management Framework
- Information Security Policy
- Records Management Policy
- Acceptable Use Policy
- Learning and Development Policy
- Disciplinary Policy