NHS
Bury
Clinical Commissioning Group

# Data Security / Information Governance Training Needs Analysis

| | |
|---|---|
| **Version:** | 9.0 |
| **Ratified by:** | NHS Bury CCG Information Governance Steering Group |
| **Date ratified:** | 16 May 2022 |
| **Name of originator /author (s):** | Information Governance Team |
| **Responsible Committee / individual:** | Information Governance Steering Group |
| **Date issued:** | May 2022 |
| **Review date:** | May 2023 |
| **Target audience:** | NHS Bury Clinical Commissioning Group Members and Staff |
| **Equality Analysis Assessed:** | TBC |

# Data Security / Information Governance Training Needs Analysis

## Table of Contents

## 1.0 Introduction

1.1 Information is an extremely valuable resource and is essential for the delivery of high quality services. Good Data Security / Information Governance (IG) practices ensure necessary safeguards for the appropriate use of business and Personal Data are in place and managed effectively. These safeguards can be found in the policies and procedures applicable to all staff but of equal importance is the knowledge and awareness everyone maintains of Data Security / IG to recognise and work within these safeguards.

1.2 The Data Security / IG training requirement also requires that:

- Basic Data Security / IG training is provided for all new starters as part of their induction; and
- Additional training is provided to staff in key roles where applicable.

1.3 The importance of this has been further recognised in the Caldicott Review 2 which states:

**'All staff should receive annual basic Information Governance Training appropriate to their role'**

1.4 The CCG has determined appropriate basic Data Security / Information Governance Training is a mandatory requirements for all staff including permanent, temporary, contractors and agency staff will receive on commencing with the CCG and for this to be refreshed annually

## 2.0 Mandatory Data Security / IG Training

2.1 The following Training Needs Analysis has been undertaken and applies:

- **Basic Information Governance Training**

2.2 All staff, including board members, and those working on behalf of the CCG through consultancy, agency, secondment, apprenticeships or work experience must complete the Data Security Awareness training and achieve the required compliance level.

2.3 The Data Security Awareness training package should be access through the ESR training platform which is accessed on the following link: https://my.esr.nhs.uk

2.4 New starters and staff returning from long-term absence and their training compliance has lapsed **mus**t complete the training **within 7 days** of commencing in post.

2.5 All staff must refresh their knowledge and awareness through re-completing the module **prior to** the 12 months expiry date of their current compliance.

2.6 Where an employee changes role and there are additional Information Governance training requirements for that role, all new training must be completed **within 7 days** of commencing in the new role.

2.7 The CCG have a 'IG Training Month' which is normally every November which assists to ensure there is a controlled way of monitoring compliance and to provide additional support to staff to complete training / deal with any queries.

- **Specialist Data Security / IG Training**

2.8 Additional and / or specialist training will be provided to staff groups or job profile as set out at appendix A. This list is not exhaustive

2.9 There may be occasions where colleagues are required to undertake additional training outside of the agreed Training Needs Analysis as identified through personal development reviews, following learning from a reported data breach, or following a change in legislation, guidance and good practice.

2.10 Additional training will be provided through the provision of internal or external providers and may also include the use of approved NHS Digital workbooks, and locally approved training slides from the IG team. for example:

- Specialist Training module for Caldicott Guardian, Senior Information Risk Owner, Data Protection Officer, Board Members, Information Asset Owner, Information Asset Managers and Information Asset Administrators.
- The Role of the Caldicott Guardian workbook
- Access to Health Records workbook

2.11 Where there would be collective benefit and shared learning from wider training sessions rather than on an individual basis, for example where there is a specific business requirement within or across teams and / or department, these sessions will be arranged by the IG Lead and may be delivered through internal or external facilitation.

## 3.0 Monitoring and Compliance

3.1 The CCG is required to achieve and maintain compliance with Data Security Awareness Mandatory training at 95% or above and must make a declaration of this status as part of the annual Data Protection and Security Toolkit.

3.2 Under GDPR and personal responsibility, 100% of all staff must undertake appropriate training.

3.3 Failure to achieve this target, would mean that Data Security Standard 3 on the Data Security and Protection Toolkit (DSPT) has not been achieved resulting in the CCG not attaining all the mandatory assertions. This means the CCG would not be regarded as a trusted organisation.

3.4 All staff must maintain their required compliance with the mandatory data security module and the necessary specialist training as required.

3.5 Notification is provided from the ESR system one month prior to when the data security awareness training is due to expire. Staff members are required to access this in good time and complete the required training before the expiry date.

3.6 A monthly compliance report will be provided to the Information Governance Steering Group and assurance from the Organisational Development and Learning Team on all mandatory training status.

3.7 Where training is outstanding or lapsed, the Corporate Office will remind the staff member. Where this remains outstanding on the following months report, the noncompliance will be escalated to their line manager. If the training remains outstanding for a third month, this will be escalated to the deputy director / director as appropriate.

3.8 Staff are reminded that non completion of mandatory training may impact on progression through the annual increment pay scales.

3.9 Managers are responsible for ensuring their staff members have completed their training and should discuss this in the annual appraisal and 1-2-1 meetings.

3.10 Compliance levels will be reported to the Information Governance Steering Group at each meeting and included within the Information Governance report to Audit Committee.

## 4.0 Review

4.1 The Training needs analysis will be reviewed annually.

NHS
Bury
Clinical Commissioning Group

**Appendix A – Data Security / Information Governance Training Needs Analysis Matrix**

| Job Role | Frequency | Data Security / IG Modules to be Completed |
|---|---|---|
| Mandatory – All Staff working for or under contract to the CCG including board members | ANNUALLY | Data Security and awareness module or training provided by IG team or workbook. |
| Admin and Clerical<br>(access to personal confidential data) | | None additional |
| Admin and Clerical<br>(no access to personal confidential data) | | None additional |
| Data Protection Officer | ANNUALLY | GDPR / DPA / specialist Data Protection Officer Training provided by an External Training Provider. |
| Caldicott Guardian | ANNUALLY | Caldicott Guardian Training provided by External Training Provider or the Senior IG lead<br>AD hock updates to be provided at IGOG via the Senior IG lead every 6/12 months |
| Senior Information Risk Owner (SIRO) | ANNUALLY | SIRO Training provided by External Training Provider or the Senior IG lead<br>AD hock updates to be provided at IGOG via the Senior IG lead every 6/12 months |
| Senior IG lead | ANNUALLY | Access to Health Records<br>Information Risk Management for SIRO and IAO<br>The Role of the Caldicott Guardian or Accredited Caldicott Guardian Training provided by External Training Provider or by IG Team Any updated training on an ongoing basis |
| Information Asset Owner (IAO) | BIENNIALLY | IAO Training provided by External Training Provider or by Senior IG lead |

| Job Role | Frequency | Data Security / IG Modules to be Completed |
|---|---|---|
| Information Asset Manager (IAM) | BIENNIALLY | IAO Training provided by External Training Provider or by Senior IG lead |
| Information Asset Administrators (IAA) | BIENNIALLY | IAO Training provided by External Training Provider or by Senior IG lead |
| Staff dealing with Subject Access Requests (personal confidential data) | BIENNIALLY | SAR Training provided by External Training Provider or Senior IG lead |
| Corporate Records Management Lead | BIENNIALLY | Up to date training from external provider |
| Business Intelligence and IT Staff | BIENNIALLY | Training provided by External Training Provider or by IG Team |