NHS
Bury
Clinical Commissioning Group

Information Security Policy

Version:	2.0
Ratified by:	NHS Bury CCG Information Governance Steering Group
Date ratified:	July 2021
Name of originator /author (s):	Greater Manchester CSU - IT Department NHS Bury CCG Information Governance Team
Responsible Committee / individual:	NHS Bury CCG Information Governance Steering Group
Date issued:	October 2021
Review date:	July 2022
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Information Security Policy CCG.GOV.017.2.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	GMSS - IT Department; NHS Bury CCG Information Governance Team
This document should be read in conjunction with	• Information Governance Framework • Information Governance Policy • Confidentiality and Data Protection Policy • Record Management Policy • Encryption Policy
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Development Team
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place, Knowsley St Bury, BL9 0SN Main Telephone Number: 0161 762 3100
Copies of this document are available from	The corporate PA office, electronic versions. CCG website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
0.1 = draft 1	NHS Bury CCG IM&T Steering Group	February 2014
1.1 = Policy once ratified	NHS Bury Clinical Commissioning Group	February 2014
1.4 = review	NHS Bury CCG Information Governance Team	October 2021
2.0 = policy once ratified	NHS Bury CCG Information Governance Steering Group	July 2021

Information Security Policy

Contents

Contents

1. Assurance Statement

1.1 This policy sets out a framework of governance and accountability for Information Security management across the Clinical Commissioning Group (CCG). The policy along with the Information Security Management Code aims to provide and develop a positive culture of information security throughout the CCG by maintaining:

- **Confidentiality:** protecting information from unauthorised access and disclosure
- **Integrity:** safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion
- **Availability**: ensuring that information and associated services are available to authorised users whenever and wherever required.

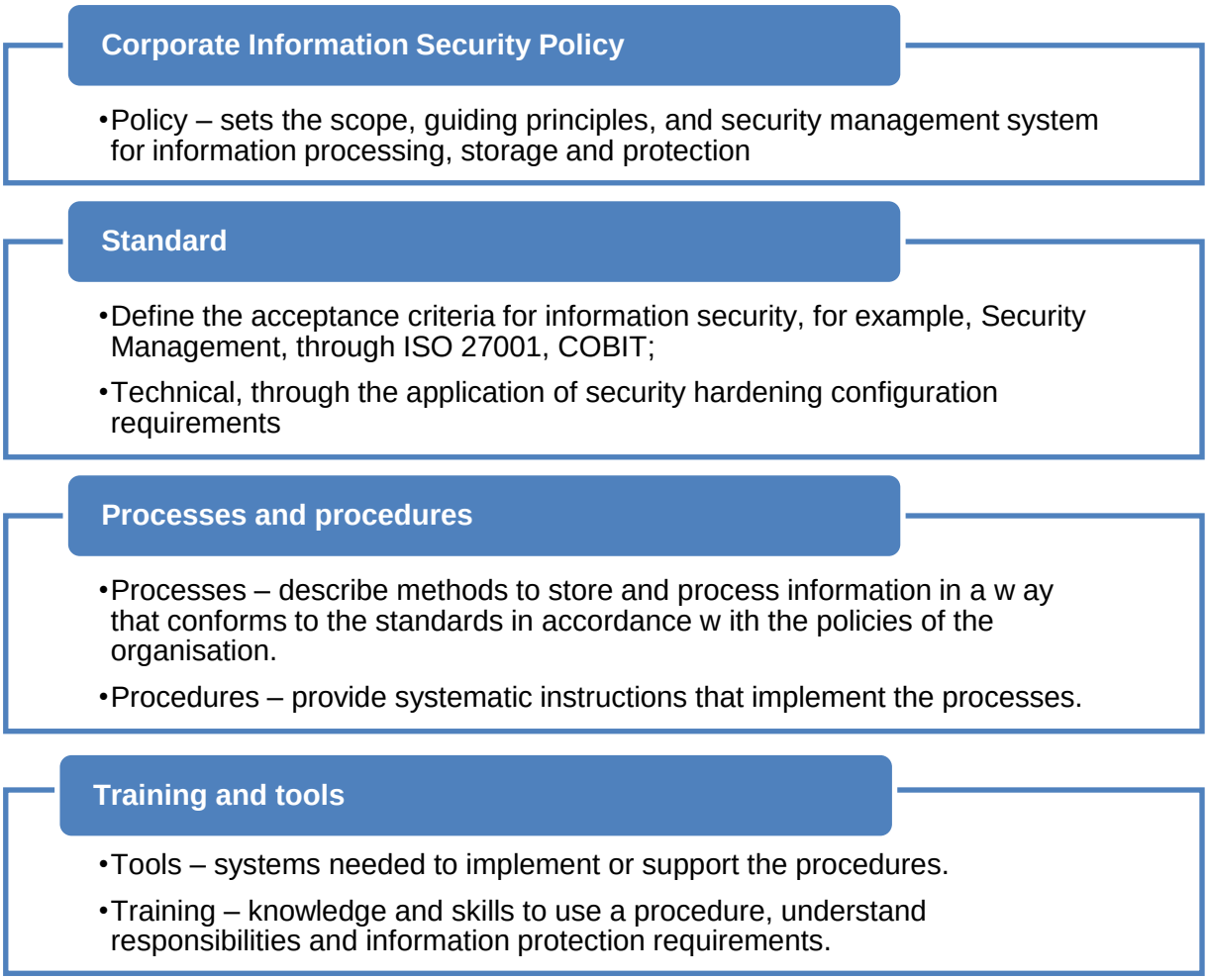
2. Introduction

2.1 The Information held and managed by the Clinical Commissioning Group (henceforth known as “the CCG”) is an asset that all staff have a duty and responsibility to protect. The availability of complete and accurate information is essential to the CCG functioning in an efficient manner.

2.2 The aims and objectives of the CCG Information Security Policy is to set out a framework for the protection of the organisation’s information and information assets to:

- protect against threats, whether internal or external, deliberate or accidental
- enable information sharing in a secure and consistent manner
- encourage consistent and secure use of information
- ensure all users of CCG information systems have a clear understanding of their roles and responsibilities in the protection and use of information
- ensure the continuity of IT Services and minimise disruption to business operations
- ensure the CCG meets its legal and fiduciary responsibilities

2.3 The CCG Information Security Policy is a high-level document that utilises a number of controls to protect the organisations information. The controls are delivered through policies, standards, processes, procedures, supported by tools and user training.



3. Aims & Objectives

3.1 This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

3.2 The CCG Information Security Policy, standards, procedures and processes applies to all forms of information, including but not limited to:

- verbal communication by telephone and social media
- information (printed or written);
- information stored in manual filing systems
- communications, including those sent by post, courier, electronic mail, text messaging and Bluetooth
- information that is stored in and/or processed by information systems including servers, personal computers (PCs), laptops, mobile phones, tablet devices, personal digital assistant (PDA) and any other mobile device that is allowed access to the information systems and information

- transmission of or passing information to third parties or others that are external to the CCG.

4. Definition of Terms

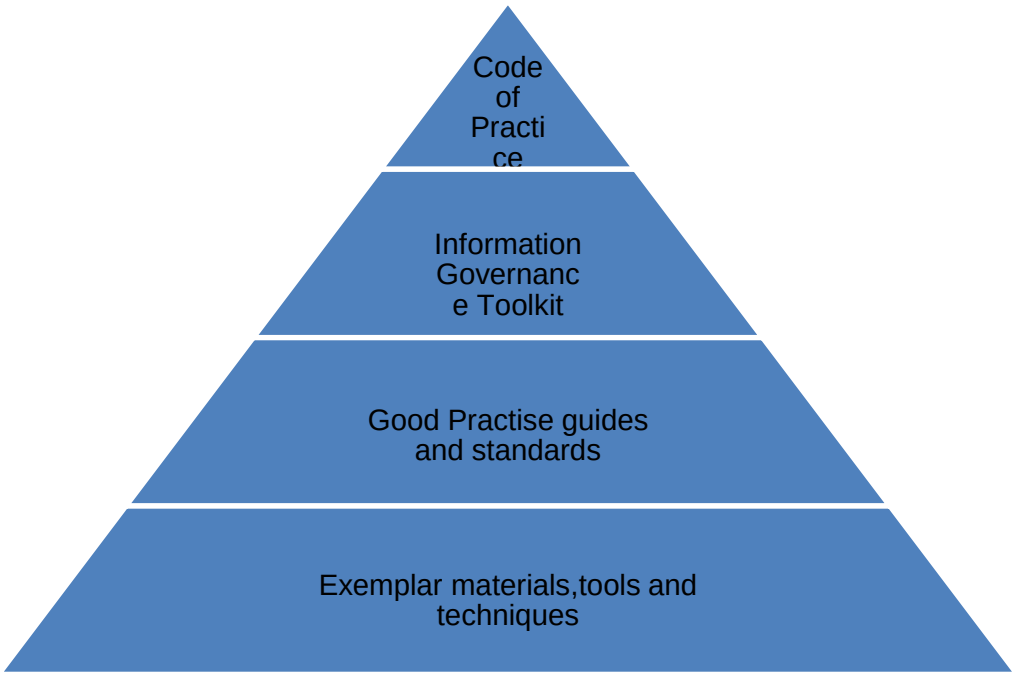
4.1 Information Security Management

4.1.1 The 'Information Security Management: NHS Code of Practice' is a guide to the methods and required standards of practice in the management of information security, for those who work within or under contract to, or in business partnership with NHS organisations in England.

4.1.2 It is based on current legal requirements, relevant standards and professional best practice.

4.1.3 This Code of Practice replaces HSG 1996/15 – NHS Information Management and Technology Security Manual, and provides a key component of Information Governance arrangements for the NHS.

4.1.4 It is part of an evolving information security management framework because risk factors, standards and practice covered by the Code will change over time. The guidelines contained within the Code of Practice apply to NHS information assets of all types.



4.2 Confidentiality

4.2.1 The 'Confidentiality: NHS Code of Practice' sets out the required standards of practice concerning confidentiality and patients' consent to use their health records.

4.2.2 It is a guide for those who work within or under contract to NHS organisations and is based on legal requirements and best practice

5. Duties and Responsibilities

- Overall accountability for procedural documents across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.
- Overall responsibility for the Information Security Policy lies with the CCG's Information Security Lead or equivalent role who has delegated responsibility for managing the development and implementation of technical and operational procedural documents to IT Services and Line Managers.
- Staff will receive training regarding the policy from a number of sources:

    - policy/strategy and procedure manuals
    - line manager;
    - specific training course;
    - other communication methods (e.g. Team Brief / team meetings); intranet; and
    - Information Governance toolkit (data security & protection toolkit) training.

6. Main policy

6.1 Risks

- The CCG will undertake risk assessments to identify, quantify and prioritise information security risks. Controls will be selected and implemented to mitigate the risks identified.
- Risk assessments will be undertaken using the Risk Assessment methodology to identify and estimate the magnitude of risks and in accordance with the CCG's Information Risk Policy.

6.2 Information Security Policy

- The Information Security Policy document sets out the CCG's approach to managing Information Security.
- The Information Security Policy is approved by the CCG and is communicated to all staff, constituent businesses, contractual third parties, partners, suppliers, agents and others who will have access to CCG information and information systems.
- The Information Security Policy will be reviewed, at least annually, and approved by the CCG Information Governance Steering Group. Changes or amendments will be made and approved accordingly.

6.3 Information security - Protection

- It is a statement of management intent that the policy of the CCG will be to ensure that information will be protected from a loss of:
- Confidentiality- ensuring that information is accessible only to those that are authorised
- Integrity- safeguarding the accuracy and completeness of information
- Availability - ensuring that authorised users have access to relevant information when required and in a timely manner

6.4 Information security – Requirements

- The CCG will implement technical and operational standards, policies and processes that align with prevailing standards such as ISO27001 (Information Security Management).
- The requirements of policy, processes and procedures will be incorporated into the CCG operational procedures and contractual agreements.
- Information stored and processed by the CCG will be appropriate to business requirements and no information will be stored or processed unnecessarily.
- Business continuity plans will be developed, implemented, maintained and tested and such plans will be a contractual obligation of any relevant supplier.
- All breaches of information security, actual or suspected will be reported and suitably investigated in line with information incident management procedures which will provide guidance on what constitutes an information incident.
- Training and education regarding information security will be given to staff, contractors and third parties as well as any others who will have access to CCG information and information systems.

6.4.1 Coordination of information security

- The security of information will be achieved through assigning information security roles and co-ordinating the implementation of this policy across the CCG, constituent businesses and third parties
- Where required, government approved external specialist advice will be drawn on to address new and emerging threats and standards.

6.4.2 Information security responsibilities

- The Information Security Lead or equivalent, is the designated owner of the Information Security Policy, responsible for the maintenance and update, ensuring timely review and approval and ensuring supporting policies, standards, processes and procedures are in place.
- The CCG auditors will attest to the adequacy and effectiveness of controls to protect the CCG information and make recommendations where deficiencies are found.
- Heads of departments and line managers are responsible for ensuring all staff, contracted third parties (whether individual or an entity) are made aware of and comply with the Information Security Policy including supporting policies, standards, processes and procedures.

6.5 Asset management

- All CCG assets, for example, people, information (electronic and hardcopy), software, computer and communication equipment and service utilities, will be accounted for and have an owner.
- The CCG will implement controls that will ensure its assets are appropriately protected
- Owners of such assets will be responsible for the maintenance and protection of assets they are assigned.

6.6 Human resource security

- Responsibilities for compliance to information security will be included in job descriptions and terms and conditions of employment.
- Where appropriate, and in line with relevant HR guidance and legislation, background checks will be carried out on new employees. These background checks will be relative to the level and classification of information employees will access within the CCG.
- Suppliers will be responsible for conducting appropriate background checks on contractors and third parties who will have access to the CCG information and information systems.

6.7 Physical and environmental security

- Restricted information will be physically protected from unauthorised access, damage, interference and/or alteration.
- Information processing facilities will be housed in secure areas. These areas must be protected by defined and approved security perimeters with appropriate security barriers and entry controls.

6.8 Communications and operations management

- Responsibilities will be assigned and policies, processes and procedures for the management, operation and on-going security and availability of all data and information processing facilities will be implemented.
- To reduce the risk of inadvertent, negligent or deliberate misuse of the CCG information systems, separation of duties or responsibilities, will be implemented.
- Appropriate controls will be applied to all types of communication, internal and external, to ensure only information required to be communicated is, the communication is secure and reaches the intended recipient.

6.9 Access control

- Access to CCG information will be controlled, with access driven by business requirements.
- Staff will be granted access to CCG information systems based on their role and to a level that will enable them to carry out their job responsibilities.

- Staff will ensure that information processed within an information system is accurate but also that the methods used to process information are not flawed such as segregation of duties and input validation.
- Information security requirements will be defined and communicated during the development of business requirements for new systems or changes to existing systems. Procurement, Finance, other IAOs and IG will collaborate to ensure that a fit for purpose system is delivered.
- Controls to mitigate risks identified during design, procurement, development, testing and deployment will be implemented.

6.10 Information security incident management

- The CCG will develop and implement a formal incident reporting and escalation process.
- All staff contractors and third parties will be made aware of procedures for reporting security incidents or vulnerabilities that may have an adverse impact on the security, integrity or availability of the CCG information systems.
- Information security incidents and vulnerabilities associated with information systems will be reported within an agreed timeframe and prescribed corrective action taken.

6.11 IT service continuity management

- A business continuity management process will be implemented to minimise the impact of a disruption of service and to recover from the loss of information assets.
- A business impact analysis will be conducted, by the business, to assist in defining appropriate controls against the consequences of disasters, security failures, loss of service and loss of service availability.
- The CCG will ensure arrangements are in place to protect critical business process from the effects of major failures or disasters, of information systems or services, and to ensure timely resumption.

6.12 Compliance

- The CCG will abide by any law, statute, regulatory and/or contractual obligations affecting its information and information systems.
- The design, operation, maintenance, use and management of information systems will comply with all statutory, regulatory and contractual security requirements.
- All staff, contractors and third parties and all others that are, or have been, authorised to access are required to comply with the Information Security Policy and its' supporting standards, policies, processes and procedures.
- Failure to comply could result in disciplinary and/or legal action.

7. Other policies and procedures

7.1 The CCG shall maintain policies and procedures for the effective management of all records. Other policies and relevant procedures that affect this policy but not limited to

are:

- Information Governance Framework
- Information Governance Policy
- Confidentiality and Data Protection Policy
- Record Management Policy
- Encryption Policy

7.2 Other relevant practises are:

- 'Confidentiality: NHS Code of Practice'
- 'Information Security Management: NHS Code of Practice'
- 'Records Management: NHS Code of Practice'

8. Monitoring arrangements

- Performance against Key Performance Indicators will be reviewed on an annual basis and used to inform the development of future procedural documents.
- This Policy will be reviewed at least on an annual basis, and in accordance with the following as and when required:
    - legislative changes
    - good practice guidance
    - case law
    - significant incidents reported
    - new vulnerabilities changes to organisational infrastructure