NHS
Bury Clinical Commissioning Group

Information Governance Policy

Version:	4.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Date ratified:	19th September 2017
Name of originator /author (s):	GMSS Information Governance Team
Responsible Committee / individual:	Audit Committee
Date issued:	January 2018
Review date:	December 2019
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Completed Equality Analysis:	Yes

Further information regarding this document

Document name	Information Governance Policy CCG.GOV.009.4.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	GMSS Information Governance Team
This document should be read in conjunction with	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff; Safe Transfer of Information Policy (safe haven).
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Development Team
Published by	NHS Bury Clinical Commissioning Group 21 Silver Street Bury BL9 0EN Main Telephone Number: 0161 762 3100
Copies of this document are available from	The corporate PA office

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
2.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	17th November 2014
3.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	18th November 2015
3.1 = policy once reviewed	GMSS IG Team	18th August 2017
4.0 = policy once ratified	NHS Bury Clinical Commissioning Group Information Governance Operational Group	19th September 2017

Information Governance Policy

Contents

1. Introduction and Aims

1.1. The purpose of this Policy is to provide guidance to all NHS Bury CCG (referred to as “the CCG”) staff on Information Governance.

1.2. Information Governance (IG) is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.

1.3. The CCG recognises the role Information Governance plays in ensuring the organisation processes and handles its personal, sensitive, business information in accordance with UK laws and Department of Health Policy, thus protecting the CCG, its employees and just as importantly, its patients.

1.4. Information Governance affects ALL employees, including anyone providing a service on behalf of the CCG, whether permanent or temporary. EVERYBODY has responsibilities for IG on a day-to-day basis, regardless of their working environment (clinical or non clinical). Contractors working for the CCG are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply.

1.5. It is of paramount importance to ensure that information is efficiently and legally managed, and that the appropriate policies, procedures, guidance and management accountability and structures provide a robust governance framework for information management.

1.6. The Information Governance Agenda of this CCG will be managed by the Greater Manchester Shared Services (GMSS), Information Governance team.

1.7. The GMSS IG Team will establish and maintain policies and procedures on behalf of the CCG to ensure compliance with requirements contained in the Department of Health Information Governance Toolkit.

1.8. Information Governance sits alongside Clinical Governance, Research Governance and Corporate Governance. It provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of personal information ensuring:

- Compliance with the law;
- information available, secure and confidential at all times;
- educating, influencing and advising good practice;
- audit, investigate, enforce and support corrective action where required; and
- year on year improvement plans.

1.8.1 It also provides a consistent way for employees to deal with the many different information handling requirements including:

- Information governance management;
- clinical information assurance;
- confidentiality and data protection assurance;
- corporate information assurance;
- information security assurance; and
- secondary use assurance.

1.9. Core to Information Governance is setting information handling standards and giving the CCG the tools to achieve the standards. Its purpose is to support the CCG and individuals to be consistent in the way they handle personal and corporate information and avoid duplication of effort, leading to improvement in:

- Information handling activities;
- patient and service user confidence in care providers; and
- employee training and development.

1.10. Information Governance operates under four fundamental aims:

- Support the provision of high quality care, by promoting the effective and appropriate use of information;
- encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- develop support arrangements, provide staff with appropriate tools and support them to discharge their responsibilities to consistently high standards; and
- enable organisations to understand their own performance, and manage improvement in a systematic and effective way.

1.10.1 The Information Governance framework and this policy sets out aims to ensure that information is used, effectively, efficiently, securely and legally, in order to deliver the best possible care.

1.11. The aims of this document are:

- to maximise the value of organisational assets by ensuring that data is:
  - held securely and confidentially;
  - obtained fairly and lawfully;
  - recorded accurately and reliably;
  - used effectively and ethically; and
  - shared and disclosed appropriately and lawfully.

- to protect the organisations information assets from all threats, whether internal or external, deliberate or accidental. The CCG will ensure:
  - information will be protected against unauthorised access;
  - confidentiality of information will be assured;
  - integrity of information will be maintained;
  - information will be supported by the highest quality data;
  - regulatory and legislative requirements will be met;
  - business continuity plans will produced, maintained and tested;
  - information security training will be available to all staff; and
  - all breaches of information security, actual or suspected, will be reported to, and investigated by the GMSS IG Team. .

2. Scope

2.1. 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 organisations 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.

2.2. This policy covers all aspects of information within the organisation, including (but not limited to):

- Employee/Patient/Client/Service User information;
- staff information (personnel);
- organisational information.

2.3. This policy covers all aspects of handling the way the organisation holds, obtains, records, uses and shares information, including (but not limited to):

- Structured records systems – paper and electronic;
- transmission of information – fax, email, post and telephone.

2.4. This policy covers all information systems purchased, developed and managed by or on behalf of, the CCG and any individual directly employed or otherwise by the CCG.

2.5. Accurate, timely and relevant information is essential in continuing to deliver the highest quality care throughout the area. As such it is the responsibility of all staff at all levels to ensure and promote the quality of information and to actively use information effectively in decision making processes.

3. Information Governance Policy Framework

3.1. The CCG will maintain an Information Governance Policy Framework. This will be supported by a set of Information Governance related policies and procedures to cover all aspects of Information Governance which are aligned with the NHS Operating Framework and the Information Governance toolkit requirements.

3.2. The Policy framework will encompass the following policies:

- Information Security Policy;
- Data Protection and Confidentiality Policy;
- Records Management Policy.

3.3. In addition, the following policy will be part of the Information Security suite of policies which will be supported by those framework documents above.

- Acceptable Use of IT Policy

3.4. This policy list is not exhaustive and will be expanded if the CCG Information Governance framework requires further development. .

4. Principles

4.1. The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The CCG fully supports the principles of corporate, clinical and information governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and information of a commercially sensitive nature. The CCG also recognises the need to share information with other health and social care organisations and other agencies in a controlled manner consistent with the interests of the patients and, in some circumstances, the public interest, in the line with the Freedom of Information Act 2000.

4.1.1. Four key strands support the Information Governance Policy:

- Openness:
- Legal Compliance;

- Information Security and Confidentiality;
- Information Quality Assurance;

4.2. Openness

- Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the General Data Protection Regulation (GDPR) and the Data Protection Act 1998;
- non-confidential information on the CCG and its services should be available to the public through a variety of media, in line with the Freedom of Information Act 2000;
- patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients;
- the CCG will have clear procedures and arrangements for handling queries from patients and public;
- the CCG will have clear procedures and arrangements for liaison with the press and broadcasting media.

4.3. Legal Compliance

- The CCG regards all identifiable personal information relating to patients and staff as confidential. Health care related information will be regarded as sensitive along with certain other types of information (e.g. Child protection data);
- the CCG regards all identifiable personal information relating to patients and staff as confidential except where national policy on accountability requires otherwise;
- the CCG regards all corporate information as confidential;
- the CCG is required to establish and maintain policies to ensure compliance with the GDPR, Human Rights Act, Computer Misuse Act, Privacy and Electronic Communications Act , Common Law of Confidentiality and any other relevant legislation;
- the CCG will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

4.4. Information Security and Confidentiality

- The Head of Service for Integrated Governance, provides the following Information Security support:
  - Use of the Head of Service for Integrated Governance Information Security (IS) qualifications as a qualified lead auditor for Information Security;
  - Undertake an IS Audit of a key information Asset process and generate a report for the CCG SIRO.
- the CCG will work towards attaining and maintaining compliance against the International / British Standard for Information Security Management ISO 27001;
- the CCG will establish and maintain policies for the effective and secure management of its information assets and resources;
- the CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training;
- the CCG will have regularly maintained business continuity plans for all critical infrastructure components and core information systems;
- the CCG will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

4.5. Information Quality Assurance and Records Management

- The CCG will establish and maintain policies and procedures for information quality assurance and the effective management of records;
- the CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements;
- managers are expected to take ownership of, and seek to improve, the quality of information within their services;
- wherever possible, information quality should be assured at the point of collection;
- data standards will be set through clear and consistent definition of data items, in accordance with national standards;
- the CCG will promote information quality and effective records management through policies, procedures/user manuals and training.

5. Roles, Responsibilities and Accountabilities

5.1. The CCG Governing Body

5.1.1 It is the role of the CCG Governing Body to define the CCG's policy in respect of Information Governance, taking into account legal and NHS requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy. To fulfil its obligations, the Governing Body has delegated authority for Information Governance to the Audit Committee. The Senior Information Risk Owner is a member of the Governing Body.

5.2. Chief Officer

5.2.1 The Accountable Officer of the CCG, the Chief Officer, has overall accountability and responsibility for Information Governance in the CCG and is required to provide assurance, through the Annual Governance Statement that all risks to the CCG, including those relating to information, are effectively managed and mitigated.

5.3. Data Protection Officer (DPO)

The DPO is required as part of the changes to the Data Protection Act which will now be the General Data Protection Regulation. The DPO's role is to inform and advise CCG and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

5.4. Senior Information Risk Officer (SIRO)

5.4.1. The Chief Financial Officer of the CCG is the nominated SIRO. The SIRO is responsible for ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist. They should be familiar with risk management and the organisations response to risk.

5.4.2. The role of the SIRO is to take ownership of the CCG's information risk policy, act as advocate for information risk at the Governing Body and provide written advice on the Annual Governance Statement in regard to information risk.

5.4.2.1 Information Asset Owners (IAO's) / Administrators (IAA'S) under the responsibility of the SIRO:

- Information Asset Owners (IAO's) will be identified and provided with training and support and will carry out risk assessments on the information assets, to protect against unauthorised access or disclosure within their area;
- will ensure the integrity of the information within their area and restrict the use to only authorised users who require access;
- will be accountable and provide assurance that information risk is being managed effectively for their assigned information assets;
- be aware of what information is held within their assigned assets and ensure there is legal justification for the assets and any flows of data;
- will ensure that all personal data can at all times be obtained promptly from the Information Asset when required.

5.5. Caldicott Guardian

5.5.1. The Caldicott Guardian is the conscience of the organisation and is responsible for ensuring that the CCG process satisfies the highest practical standards for handling patient information. This includes ensuring any sharing of patient data is justified and lawful.

5.6. Information Governance Leads

5.6.1. The Information Governance Lead will be supported by the GMSS IG Team and will be accountable for ensuring effective management, accountability, compliance and assurance for all aspects of Information Governance.

5.6.2. The management of the annual Information Governance work programme will be delegated from the Information Governance Lead to the GMSS.

5.7. Information Governance Operational Group

5.7.1. The Information Governance Operational Group (IGOG) oversees the implementation of the Information Governance strategy, policy, completion of the annual baseline assessment and associated work programme, and ad hoc Information Governance related work streams or projects. The CCG IG Lead, Caldicott Guardian and the SIRO are members of the IGOG. The IGOG will provide any relevant committees with regular updates and reports and highlight any risks to compliance.

5.8. Line Managers/Senior Managers

5.8.1. All managers are responsible for ensuring that staff are compliant with, and working to, all relevant policy and procedure in relation to Information Governance. Managers should ensure that supporting standards and guidelines are built into local processes and that there is on-going compliance on a day to day basis. Any incidents or policy breaches relating to confidentiality or information security are reported immediately. In addition, managers will ensure that anyone providing a service on behalf of the CCG complete a confidentiality statement before commencing employment.

5.9. All Staff

5.9.1. All staff, whether permanent, temporary or contracted, working in a clinical or non-clinical environment are responsible for ensuring that they are aware of the Information Governance requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Any incident involving a breach or suspected breach of the General Data Protection Regulation and the Data Protection Act 1998 will be reported to their line manager immediately, and where they are not available the CCG Information Governance Lead.

5.9.2. All staff have a responsibility to ensure they complete the mandatory training requirements of the organisation, Information Governance is part of these training requirements. Further information regarding IG training can be found on the CCG Training Needs Analysis (TNA)

5.9.3. The CCG will ensure that all employees including contractors have access to and are trained on the Information Governance Policy and are given sufficient information and/or guidance to be able to perform their duties in line with Information Governance policy and the associated laws/regulations that govern it. The Confidentiality Code of Conduct must be read and signed by all employees this includes contractors.

5.9.4. Elements of Information Governance, particularly confidentiality should be written in all contracts of employees, SLAs and Contracts for services. Information Governance considerations should form part of any procurement of a service, piece of software or information sharing agreement.

6. Information Governance Toolkit and Annual Performance

6.1. An assessment of compliance of requirements, within the Information Governance Toolkit will be undertaken each year. A proposed action/work programmes will be maintained, and annual assessments will be presented to the CCG for approval.

7. Training and Communication

7.1. To ensure all Information Governance policies and procedures are effective the CCG must make all staff aware of their Information Governance obligations. Information Governance training is mandatory for all members of staff. Any new staff members including temporary, contractors will be required to complete Information Governance training as part of their induction.

7.1.1. Information Governance training is mandated to be undertaken on an annual basis.

7.1.2. Where staff have specific Information Governance roles within the CCG i.e. Caldicott Guardian, SIRO etc. additional Information Governance training will be required.

7.2. To maintain high staff awareness the CCG will direct staff to a number of sources:

- Policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods, for example, team meetings; and staff intranet

7.3. All staff will be reminded that it is their responsibility to adhere to the policy.

8. Monitoring and review

8.1. The CCG will undertake or commission from the GMSS IG Team regular assessments and audits of its framework, policies and procedures to monitor compliance and make improvements where identified.

8.2. Where Information Governance incidents have been reported via the CCG’s incident reporting process investigations will be initiated.

8.3. This Policy will be reviewed every 2 years. An earlier review may be warranted if one of more of the following occurs:

- legislative changes; good practice guidance; case law;
- significant incidents reported; new vulnerabilities; and
- changes to organisation infrastructure.

9. Legislation and related documents

9.1. Legal Acts

- General Data Protection Regulation;
- Data Protection Act 1998;
- Freedom of Information Act 2000;
- Environmental Information Regulations;
- Access to Health Records Act 1990;
- Regulation of Investigatory Powers Act;
- Health and Social Care Act 2012;
- Human Rights Act 1998.

9.2. Supporting Documents

- NHS Information Governance: Guidance on Legal and Professional Obligations;
- NHS Code of Confidentiality;
- Information Security Management: NHS Code of Practice April 2007;
- Caldicott Guardian Manual 2017;
- NHS Information Risk Management;
- NHS Records Management Code of Practice 2016; The Information Governance Toolkit;
- Caldicott Reports