NHS
Bradford District
and Craven
Clinical Commissioning Group

# Information governance framework

The information governance framework sets out the CCG's overall approach to the management of information governance

## Key information

| | |
|---|---|
| Responsible director: | Chief finance officer and SIRO |
| Author: | IG officer, The Health Informatics Service (THIS) |
| Approval body: | Audit and governance committee |
| Date approved: | November 2020 |
| Version: | 1.0 |
| Review date: | November 2022 |

## Version control

| Version no. | Date | Author | Description | Circulation |
|---|---|---|---|---|
| 1.0 | October 2020 | As above | Version approved by audit and governance committee. | CCG wide |

## Contents

Key information ........ 1

Version control ........ 1

1 Introduction ........ 4

2 Scope of the framework ........ 4

3 Associated documentation ........ 5

4 Framework statement ........ 5

5 Objective ........ 5

6 Duties, accountabilities, roles and responsibilities ........ 6

6.1 Governing body ........ 6

6.2 Audit and governance committee ........ 6

6.3 Accountable officer ........ 6

6.4 Senior information risk owner ........ 6

6.5 Information governance lead ........ 7

6.6 Data protection officer ........ 7

6.7 Caldicott guardian ........ 8

6.8 Associate director of digital and technology ........ 8

6.9 Chief clinical information officer (CCIO) ........ 9

6.10 Information asset owners and information asset administrators ........ 9

6.11 Directors, heads of service and line managers ........ 10

6.12 Employees ........ 10

6.13 Outsourced provider of information governance services ........ 11

7 Policy and procedure details ........ 11

7.1 Openness and transparency ........ 11

7.2 Legal compliance ........ 11

7.3 Information security ........ 12

7.4 Clinical information assurance, quality assurance and records management ........ 12

8 Dissemination, implementation and training ........ 13

8.1 Dissemination and review ........ 13

8.2 Training ........................................................................................................ 13

9 Review and monitoring........................................................................................ 13

10 Public sector equality duty.................................................................................. 14

11 Appendices ........................................................................................................ 14

Appendix A: New starter information governance declaration form ..................................... 15

# 1 Introduction

NHS Bradford District and Craven Clinical Commissioning Group recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. The CCG also recognises the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which they process, store, share and dispose of information.

The information governance framework sets out the CCG's overall approach to the management of information governance and should be read in conjunction with the other information governance policies and procedures that can be found on the CCG intranet and website.

# 2 Scope of the framework

2.1 This framework must be followed by all staff who work for, or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, governing body, senior leadership team, students and commissioning support staff working for and behalf of the CCG. The framework 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.

2.2 This framework covers:

All aspects of information within the organisation, including (but not limited to):

- patient/client/service user information
- personnel/staff information
- organisational and business sensitive information
- structured and unstructured record systems - paper and electronic
- photographic images, digital, text or video recordings including CCTV
- all information systems purchased, developed and managed by, or on behalf of, the organisation
- CCG information held on paper, CD, USB/memory sticks, computers, laptops, tablets, mobile phones and cameras

The processing of all types of information, including (but not limited to):

- accessing information
- transmission of information – verbal, e-mail, post, text and telephone
- sharing of information for clinical, operational or legal reasons
- the storage and retention of information
- the destruction of information

2.3 Failure to adhere to this document may result in disciplinary action and/or referral to the appropriate regulatory agencies as appropriate including the police and professional bodies.

2.4 Information governance within member practices and other independent contractor's is the responsibility of the directors/partners. However, the CCG is committed to supporting member practices and other independent contractors in their management of information risk and will provide advice, share best practice and provide assistance when appropriate.

2.5 The CCG is committed to working collaboratively with partners to ensure effective management of information risk across the Bradford District and Craven and West Yorkshire & Harrogate systems

## 3 Associated documentation

This framework should be read in conjunction with:

- IG and data security handbook
- Confidentiality & Data Protection Policy
- Records Management Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Incident Reporting Policy
- Disciplinary Policy
- Anti-Fraud, Bribery and Corruption Policy  Raising Concerns Policy
- Internet and Social Media Policy
- access to records (subject access request) procedure
- freedom of Information procedures
- data protection impact assessment guidance and checklist
- safe transfer guidelines and procedure
- destruction of confidential waste procedure
- incident management, investigation and reporting procedures

## 4 Framework statement

The framework sets out the overarching approach that the CCG will take to ensure they are compliant with the requirements of the Data Protection Act, data protection legislation, records management guidance, information security guidance and other related legislation and guidance, contractual responsibilities and to support the assurance requirements of the ten data security standards of the Data Security and Protection Toolkit.

## 5 Objective

5.1 This framework supports the CCG in its role as a commissioner of health services and will assist in the safe and legal sharing of information with its partners and parties.

5.3 The CCG has established, implemented and maintains a suite of information governance policies and procedures linked to this framework to ensure compliance with the requirements set out in 2.1 above (see Section 9: Associated documents)

# 6 Duties, accountabilities, roles and responsibilities

## 6.1 Governing body

The ultimate responsibility for information governance in the organisation lies with the governing body. The governing body is accountable for ensuring that the necessary support and resources are available for the effective implementation of this framework.

## 6.2 Audit and governance committee

The audit and governance committee has delegated authority from the governing body to discharge its function in respect of information governance.

The audit and governance committee is accountable to the governing body and is responsible for the review and approval of this framework, related work plans and procedures and will receive regular updates on compliance and any related issues or risks.

## 6.3 Accountable officer

The chief officer is the accountable officer for the CCG and has overall accountability and responsibility for information governance and is required to provide assurance, through the annual governance statement that risks to the CCG, including those relating to confidentiality and data protection, are effectively managed and mitigated.

The chief officer is responsible for:

- Defining the organisation's policy in respect of information governance and records management, taking into account legal and NHS requirements
- Ensuring that sufficient resources are provided to support information governance
- Setting and supporting a culture that supports legal and effective information governance

## 6.4 Senior information risk owner

The chief finance officer is the senior information risk owner (SIRO) and has organisational responsibility for all aspects of risk associated with information governance, including those relating to confidentiality and data protection.

The senior information risk owner (SIRO) will:

- Take ownership of the organisation's information risk assessment process and act as advocate for information risk on the governing body
- Ensure that identified information security threats are followed up and incidents managed
- Ensure that the organisation's approach to information risk is effective in terms of resources, commitment and execution and that this approach is communicated to all staff
- Be required to undertake and pass SIRO training annually
- Sign off the annual Data Security and Protection Toolkit submission
- Submit a SIRO annual report to the audit and governance committee

## 6.5 Information governance lead

The information governance lead is the strategic head of assurance, who reports to the strategic director of organisation effectiveness and is supported by the head of corporate governance.

The IG lead works with the IG team (out-sourced) to ensure systems are developed and implemented. The IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG within the CCG. This role includes but is not limited to:

- developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities
- ensuring that there is top level awareness and support for IG resourcing and implementation of improvements
- providing direction in formulating, establishing and promoting IG policies;
- establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives
- ensuring assessments and audits of IG policies and arrangements are carried out, documented and reported as required
- ensuring that the approach to information handling is communicated to all staff and made available to the public e.g. subject access and freedom of information requests; privacy info notice
- ensuring that appropriate training is made available to staff and completed as necessary to support their duties and for NHS organisations
- liaising with other committees, working groups and programme boards in order to promote and integrate IG standards
- monitoring information handling activities to ensure compliance with law and guidance
- providing a focal point for the resolution and/or discussion of IG issues
- ensuring effective liaison with the CCG's data protection officer, in particular relating to data protection impact assessments and data security incidents

## 6.6 Data protection officer

Article 37(5) of the General Data Protection Regulation (GDPR) allows the role of data protection officer (DPO) to be assigned to either a member of staff or to an external contractor, designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

Under data protection legislation, the role of DPO is protected and the organisation must ensure that:

- the DPO reports to the highest management level of the organisation i.e. governing body level
- the DPO operates independently and is not dismissed or penalised for performing their task
- adequate resources are provided to enable DPOs to meet their data protection legislation obligations.

In accordance with their obligations under the data protection legislation, the CCG has appointed a data protection officer (DPO) to support compliance. To complement the role of the out sourced IG service, who provide operational information governance services, the CCG has sourced its DPO through entering into a service level agreement with Audit Yorkshire. The contact details for the data protection officer are published on the CCG's website.

The DPO's tasks are defined in Article 39 of the general data protection regulation (GDPR) as:

- to inform and advise the CCG and its employees about the organisation's obligations to comply with the data protection legislation and other data protection laws
- to monitor compliance with the data protection legislation and other data protection laws, and with the CCG's data protection polices, including managing internal data protection activities
- raising awareness of data protection issues, training staff and conducting internal audits
- to advise on, and to monitor, data protection impact assessments (DPIA)
- to cooperate with the information commissioner's office (ICO)
- to be the first point of contact for the ICO and for individuals whose data is processed (employees, patients etc.)

## 6.7 Caldicott guardian

The caldicott guardian for the CCG is the director of quality and nursing. 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 is supported by the deputy caldicott guardian who is the CCG's associate director of quality & nursing.

The caldicott guardian will:

- ensure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained
- provide leadership and informed guidance on complex matters involving confidentiality and information sharing
- play a key role in ensuring that their organisation satisfies the highest practical standards for handling person-identifiable information. Their main concern is information relating to patients, service users and their care, but the need for confidentiality extends to other individuals, including their relatives, staff and others. Organisations typically store, manage and share personal information relating to staff, and the same standards should be applied to this as to the confidentiality of patient information.
- apply the seven Caldicott principles wisely, using common sense and an understanding of the law.

## 6.8 Associate director of digital and technology

The associate director of digital and technology is supported by the outsourced IT function and will:

- maintain a list of systems which do not support individual login with the risks outlined and what compensating measures are in place
- ensure that technical controls that prevent information from being inappropriately copied or downloaded
- complete data security and protection training suitable to their role
- ensure appropriate access controls are in place to enable line managers to grant access to staff for systems that hold personal and confidential information
- ensure that staff roles are linked to IT accounts and that staff who move in or out of the CCG are reflected by IT accounts administration.
- ensure that all staff understand their activities on IT systems will be monitored and recorded for security purposes
- ensure that any IT/cyber related incidents are investigated via CCG policy and procedures
- ensure that all CCG issued user devices are subject to anti-virus protections, while email services benefit from spam filtering deployed at the corporate gateway
- ensure that all software has been surveyed to understand if it is supported and up to date
- ensure unsupported software is categorised and documented and data security risks are identified and managed
- ensure that supported systems are kept up to date with the latest security patches
- ensure that all networking components have had their default passwords changed
- assist the associate director of contracting to ensure that all IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the national data guardian’s data security standards.

### 6.9 Chief clinical information officer (CCIO)

The chief clinical information officer (CCIO) for the CCG will be a clinically-qualified person who is responsible for:

- acting as the key representative for the CCG  liaising between the disciplines of clinical medicine, IT, information governance and information management
- promoting and supporting the development of, and innovation in, clinical medicine, IT, information governance and information management to enhance the effectiveness and efficiency of patient care
- promoting and supporting legislative compliance and good practice in the development of clinical information systems and initiatives
- assisting where appropriate the CCG, member practices and partners with identifying, assessing, treating and reporting risks and issues relating to clinical information
- providing guidance, leadership and strategic direction in this area within the CCG and across the wider Bradford District & Craven system.

### 6.10 Information asset owners and information asset administrators

Information asset owners (IAOs) are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they are responsible for and that any changes introduced to their business processes and systems undergo a data protection impact assessment (DPIA).

IAOs are responsible for ensuring that their information asset register and data flow mapping is accurate and up to date at all times.

IAOs will also ensure that:

- contracts with third parties providing services to and on behalf of the CCG include appropriate, detailed and explicit requirements regarding confidentiality and data protection to ensure that contractors are aware of their IG obligations
- the CCG maintain a list of its suppliers that handle personal information, the products and services they deliver, their contract details and the contract duration
- the CCG's suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.
- basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance
- compliance with contractual requirements will be monitored throughout the year and included within the CCG's annual Data Security and Protection Toolkit submission

An information asset administrator (IAA) will have delegated responsibility for the operational use of an information asset. IAOs are responsible for allocating the role of IAA to relevant staff and for ensuring the adequate training of IAAs in operational use of an information asset.

### 6.11 Directors, heads of service and line managers

Directors, heads of service and line managers are responsible for ensuring that they and their staff are familiar with this framework document and its associated guidance. They must ensure that any breaches of the policy are reported, investigated and acted upon in line with the CCG's Incident Reporting Policy.

Line managers are responsible for the request for new accounts, providing a definitive list of access requirements, and ensuring that the IT service desk and systems information asset owners/administrators are notified when a member of staff leaves or moves so that access to systems can be terminated or adjusted.

### 6.12 Employees

Information governance compliance is an obligation for all staff.

All new members of staff must read the IG & data security handbook and sign the declaration form provided in the induction pack (also see Appendix A) at the earliest opportunity.

Staff should note that there is a non-disclosure of confidential information 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 information governance issues.

Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of the computer system is a disciplinary offence, which may result in dismissal or termination of their 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. Under data protection legislation, individuals can personally be fined and/or prosecuted where a data breach is deemed intentional or malicious.

All employees must promptly report any information governance incidents or near misses to the governance team in line with the CCG's incident reporting policy. A sufficiently serious information governance breach must be reported to the information commissioners' office within 72 hours of the breach being identified, it is therefore vital that any information governance incidents are reported promptly.

### 6.13 Outsourced provider of information governance services

The provider will provide a range of IG services as set out in the annual IG work programme which is approved by the audit & governance committee.

## 7 Policy and procedure details

### 7.1 Openness and transparency

- the CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information
- information will be defined and, where appropriate, kept confidential underpinning the principles of caldicott legislation and guidance
- information about the organisation will be available to the public in line with the Freedom of Information Act, Environmental Information Regulations and Protection of Freedoms Act unless an exemption applies. The CCG has established and maintains a publication scheme in line with legislation and guidance from the information commissioner
- there are clear procedures and arrangements in place for handling queries from patients, staff, other agencies and the public concerning personal and organisational information
- integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended
- legislation will be followed and account taken as appropriate of national and local guidelines
- the CCG will undertake annual assessments and audits (through the data security and protection toolkit) of its policies, procedures and arrangements for openness.
- data subjects patients will have ready access to information relating to their own health care under data protection legislation using the CCG's access to records procedure (also known as subject access requests (SARS)). The access to records procedure can be found on the CCG intranet.

### 7.2 Legal compliance

- the CCG regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory requirements will be achieved, monitored and maintained
- the CCG will undertake or commission annual assessments and audits of its compliance with legal requirements as part of the annual assessment against the

data security and protection toolkit standards and in line with changes and developments in legislation and guidance

- the CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise as set out in the principles of the Human Rights Act and in the public interest
- the CCG will establish and maintain policies to ensure compliance with the data protection legislation, Freedom of Information Act, Human Rights Act and the common law of confidentiality and associated guidance
- the CCG will work with partner NHS bodies and other agencies to establish information sharing protocols to inform the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation
- information governance training will be mandatory for all staff. This will include awareness and understanding of the caldicott principles and confidentiality, information security and data protection. Information governance will be included in induction training for all new staff with completion of refresher training on an annual basis thereafter. The necessity and frequency of any further training will be personal development review (PDR) based
- the CCG will work in collaboration with the local counter fraud specialists and other related agencies to support their work in detecting and investigating fraudulent activity across the NHS

### 7.3 Information security

- the CCG has established and maintain policies for the effective and secure management of its information assets and resources
- the CCG will undertake or commission annual assessments and audits of its information and IT security arrangements as part of the annual assessment against the data security and protection toolkit standards and in line with changes and developments in legislation and guidance
- the CCG will promote effective confidentiality and information security practice to its staff through policies, procedures and training
- the CCG has established and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security
- the CCG has appointed a senior information risk owner (SIRO) and assigned responsibility to information asset owners to manage information risk
- the CCG will use pseudonymisation and anonymisation of personal data where appropriate to further restrict access to confidential information
- all new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organisation to address the privacy concerns a data protection impact assessment (DPIA) must be used. Under data protection legislation, data protection impact assessments are mandated for high risk processing.

### 7.4 Clinical information assurance, quality assurance and records management

- the CCG has established 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 of, the quality of information within their services
- wherever possible, information quality should be assured at the point of collection
- the CCG will promote data quality through policies, procedures, user manual and training
- data standards will be set through clear and consistent definition of data items, in accordance with national standards
- the CCG has established a records management policy covering all aspects of records management and consistent with the records management code of practice for health and social care 2016

# 8 Dissemination, implementation and training

## 8.1 Dissemination and review

Following ratification by the audit and governance committee, this framework will be disseminated to staff and placed on the CCG's website.

The framework will be reviewed every two years or in line with changes to relevant legislation or national guidance.

## 8.2 Training

Mandatory information governance training forms part of the staff induction process and it is contractually mandated that all staff complete mandatory information governance in the form of the online data security awareness training annually.

The CCG has established an IG training needs analysis (TNA) that identifies the information governance training needs of key staff groups taking into account role, responsibility and accountability levels and will review this regularly through the PDR processes.

All staff, whether permanent, temporary or contracted, should be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality.

All new members of staff must read and understand the information governance and data security handbook and sign the new user declaration form (Appendix A).

# 9 Review and monitoring

An assessment of compliance with requirements within the data security and protection toolkit will be undertaken each year. The toolkit is subject to review by internal audit on an annual basis.

Reporting on information governance developments, risk, issues and incident is provided to all standard meetings of the audit & governance committee (three per annum).

Monitoring of this framework will also be undertaken as part of the annual IG work programme.

## 10 Public sector equality duty

The Equality Act 2010, available on the GOV.UK website, includes a general legal duty to:

- eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Act
- advance equality of opportunity between people who share a protected characteristic and people who do not share it
- foster good relations between people who share a protected characteristic and people who do not share it

The protected characteristics are:

- age
- disability
- gender reassignment
- marriage or civil partnership (only in respect of eliminating discrimination)
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation

All policies should include a statement that the CCG aims to design and implement services, policies and measures that meet the diverse needs of our service users, population and workforce, ensuring that no one is placed at a disadvantage over others.

In this statement also describe any elements of the policy which aim to reduce any inequalities experienced by any group(s) of people with any of the equality act protected characteristic(s).

Seek advice on this statement, if necessary, from the CCG equality and diversity lead.

## 11 Appendices

Appendix A: New Starter Information Governance Declaration Form

## Appendix A: New starter information governance declaration form

I confirm that I have received the IG & data security handbook and understand that it is my responsibility to read and understand it and to raise any queries or concerns with my line manager or directly with the CCG's information governance service provider (this.informationgovernance@this.nhs.uk).

This booklet has been developed to ensure that users are compliant with, but not limited to, the Data Protection Act 2018 (DPA), General Data Protection Regulation (GDPR), Freedom of Information Act 2000, Human Rights Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patent Act 1988, ISO27001 (formerly BS7799) and the caldicott principles.

It is IMPORTANT to remember that you are accountable for your computer login and that all activity is auditable.  Monitoring of email and internet activity is also carried out.  It is your responsibility to ensure that only you know your password and that if you leave your PC logged in and unattended you must lock your PC (press Ctrl+ Alt + Del) to stop any unauthorised use of your PC.

If you choose to make a note of any login IDs and/ or passwords that you are using, lock them away in a secure place. Keep all passwords secure and DO NOT disclose them to anyone.

You should be aware that inappropriate use, including any violation of this policy may result in the withdrawal of the facility and may result in prosecution, fines and / or disciplinary action, including dismissal, in accordance with the CCG's disciplinary procedures and data protection legislation legislation.

| | |
|---|---|
| Signed: | Date: |
| Name (Please Print): | |
| Job Title: | |
| Team: | |
| Contact Telephone Number: | |

When signed, this declaration will be held on your personal file.

**Line managers to send signed declaration to HR for inclusion in employees' ESR files.**