Information Governance Policies

May 2018

Contents

INFORMATION GOVERNANCE POLICY

May 2018

Purpose

This policy defines the Care Quality Commission's (CQC) approach to Information Governance. It provides assurance that our practices comply with legislation and CQC's business requirements, and that information risks are appropriately recognised and managed.

The aims of this policy are:

- To ensure that information (including information about identifiable people and other confidential information) are:
    - Held securely
    - Obtained fairly and lawfully
    - Recorded and managed accurately and reliably
    - Used effectively and ethically
    - Shared and disclosed appropriately and lawfully.
- To ensure that information risks are identified and managed,
- To ensure that all CQC staff recognise and meet their own responsibilities and accountabilities in relation to the processing of information, and
- To maximise the value of CQC's organisational information assets, through their effective and lawful management.

Policy Statement

Information is vital to CQC's role as the independent regulator of health and adult social care in England.

Only by the effective obtaining, use and sharing of information can CQC meet its purpose to ensure that health and social care services provide people with safe, effective, compassionate, high quality care and to encourage services to improve.

Failure to adequately protect and manage information would create an unacceptable risk to the privacy of people who use those services and to the privacy of other people whose information CQC may obtain and use. Failure to identify and meet our obligation of confidentiality may also create significant risks to the effectiveness of CQC's regulation, the rights and legitimate interests of providers of services, and public trust in CQC as a regulator.

CQC will maintain an ‘Information Governance framework’ to provide a structured and effective set of controls and measures for the handling of information.

This framework will include:

- A suite of policies covering key areas of Information Governance
- A structure of established accountabilities and responsibilities
- Guidance, processes and training for our staff, and for others who access or process information on CQC’s behalf.

Effective information governance is a vital element of meeting the priorities identified in *Shaping our future: CQC’s strategy for 2016 to 2021*:

1. **Encourage improvement, innovation and sustainability in care** by supporting the lawful and fair publication of information.
2. **Deliver an intelligence-driven approach to regulation** by supporting innovation and improvement in how CQC obtains and analyses information to generate intelligence, and by ensuring that these innovative uses of information are lawful, fair and appropriate and operated within effective controls and protection.
3. **Promote a single, shared view of quality** by supporting the appropriate and effective sharing of information with strategic partners
4. **Improve efficiency and effectiveness** by protecting public and stakeholder trust in CQC and therefore maintaining willingness to share information with us.

Scope

Information governance is the process by which an organisation obtains and provides assurance that it is complying with its legal, policy and moral responsibilities in relation to the processing of information.

CQC considers that the following areas fall under the scope of information governance:

- Data protection
- Information Security
- Information access (including Freedom of Information)
- Knowledge and Information Management (including record management and data quality)
- Confidentiality

All employees and agents of CQC are required to comply with this policy, and with the policies and processes that sit under it as part of the information governance framework.

Responsibilities

The following overarching responsibilities apply to all parts of the Information Governance Policy. Additional responsibilities are listed under the relevant parts of this policy.

Role	Responsibility
All staff (including those in roles below)	Processing information, managing records, and complying with security standards and requirements in line with this policy, as well as other related policies and guidance to comply with legislative and business requirements.
The Chief Executive Officer (CEO) and the Board of Directors	Ensuring that systems are in place to support compliance with information law, access and management of records, information security and continuity of service.
Executive Team (ET)	Approving and signing off relevant policies.
Senior Information Risk Owner (SIRO)	Ownership of the Information Governance Policy. Responsibility for 'managing information risk across the organisation and for ensuring that the data and information assets of CQC are identified, processed, transmitted, stored and used in line with the principles of good information governance and in compliance with CQC's legal, statutory and organisational requirements.' (CQC, Corporate Governance Framework) See also Scheme of Delegation
The Caldicott Guardian	Providing advice and oversight to ensure that confidential personal information relating to people who use the services we regulate is obtained, used, handled and shared in accordance with the

	Caldicott Principles.
Data Protection Officer (DPO)	To carry out the tasks under Article 39(1) of GDPR, to: a) Inform and advise on compliance with GDPR. b) Monitor compliance with GDPR. c) Provide advice as regards data protection impact assessments. d) Cooperate with the ICO. e) Act as contact point with the ICO on issues relating to processing. To carry out these tasks with due regard to risks relating to the processing of personal data.
Information Governance Group (IGG)	Providing advice to the CQC Executive team, via the SIRO, on policies, systems, guidance, methodologies and training for information governance. Producing and signing off guidance and training materials on information governance issues. Maintaining and overseeing CQC's information risk register.

Associated policies

CQC will establish and maintain the following policies under our information Governance framework:

- Data protection policy
- Information security policy
- Freedom of Information policy
- Knowledge and information management (KIM) policy
- Code of Practice on Confidential Personal Information

DATA PROTECTION POLICY

May 2018

Purpose

This policy defines the Care Quality Commission's (CQC) approach to processing personal data. It provides assurance that our practices comply with legislative and business requirements.

Policy Statement

CQC will process personal data in accordance with the requirements of data protection law (see definitions, below).

The processing of personal data is vital to CQC's role as the independent regulator of health and adult social care in England.

The effective obtaining, use and sharing of personal data is often necessary for CQC to meet its purpose of ensuring that health and social care services provide people with safe, effective, compassionate, high quality care and to encourage services to improve.

Failure to adequately protect and manage personal data would create an unacceptable risk to the privacy of people who use those services and to the privacy of other people whose personal data CQC may have access to, obtain and use.

Scope

This policy applies to all processing of personal data by or on behalf of CQC.

This includes the processing of personal data relating to people who use the services we regulate, registered persons and their staff, our own employees and agents, and any other persons whose personal data we process.

The scope of this policy includes the processing of personal data by third parties acting on behalf of CQC.

This policy should be read alongside the ‘associated policies’ listed at the end of the document. In particular, it should be read alongside CQC’s Code of Practice on Confidential Personal Information.

Definitions

Personal data is any information processed by CQC which identifies and relates to a living person. This includes information which directly identifies a living person, but also to information which is not directly identifiable but which could be linked back to the person by reference to other information which is held by CQC, is likely to come into the possession of CQC, or which CQC has powers to obtain.

Special category personal data is personal data which reveals or relates to physical or mental health (including health and care needs, treatment or the use of care services), racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, sex life or sexual orientation. It also includes the processing of genetic data or biometric data (e.g. fingerprints, DNA samples, iris scans).

Processing means any operation, action on, or interaction with personal data, whether carried out by a person or by automated means.

Processing includes, but is not limited to: access to, obtaining, recording, organisation or structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, sharing, publication, restriction, erasure or destruction of personal data.

Data protection law is any legislation (including Act, regulation or statutory instrument) currently in force which directly applies to the processing of personal data by CQC.

The principle legislation at the time of publication of this policy are the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Data subjects are the people to whom personal data relates.

Privacy notices are information that is communicated to data subjects to inform them of how and for what purpose(s) their personal data will be processed by CQC, and which provide them with further information prescribed under data protection law, including information of the security and retention of the data, and on the data subject’s rights.

Data Protection Principles

In accordance with data protection law, CQC will ensure that all processing of personal data is carried out in accordance with the principles relating to the processing of personal data (under Article 5 of GDPR).

These '**Data Protection Principles'** require that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner.

2. Collected only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form which permits the identification of data subjects for no longer than is necessary.

6. Kept secure, with appropriate measures to protect against unauthorised or unlawful processing, accidental loss, destruction or damage.

CQC will maintain appropriate records to demonstrate compliance with the data protection principles.

Lawful bases for processing

CQC will only process personal data or special category personal data, where we have identified that a lawful basis for doing so is engaged under data protection law. We will maintain records of the lawful bases relied upon for the processing of personal data.

Consent

Consent is one lawful basis for processing personal data. Explicit consent is one lawful basis for processing special category personal data.

For consent to be valid, it must be informed and freely given. Consent must be indicated by a positive action, and cannot be implied from failure to respond, object

or opt out. Consent may be withdrawn at any time and CQC must ensure that withdrawing consent is as easy as giving consent.

CQC will not rely upon consent as the *only* lawful basis for processing for the purpose of exercising our statutory functions.

Where CQC does rely upon consent as a lawful basis for processing, we will maintain records as evidence of consent.

Other requirements of data protection law

CQC will also comply with the other requirements of data protection law, which include (but are not limited to):

Providing privacy notices to inform data subjects as to how and why we may process their personal data, and as to their rights.

CQC will produce and publish 'privacy notices' which we shall make available on our website and, where appropriate, in other CQC publications.

Where we collect personal data directly from data subjects (e.g. on forms, webforms or surveys, or when asking for information in person or via electronic communications) we will provide a privacy notice at the point of collection.

Where we collect personal data via a third party, we will ensure that a privacy notice is communicated to the data subject to the extent that it is proportionate and reasonable in the circumstances to do so.

Complying with the rights of data subjects.

CQC will ensure that there are processes in place to comply with the rights of data subjects. These include:

Right of data access: CQC will have a process to manage and respond to requests from data subjects for access to their own personal data and for information as to how and for what purpose(s) it is being processed by CQC.

Right to data portability: Where processing is based upon the lawful basis of consent, or for the performance of a contract with the data subject, CQC's process for responding to requests from data subjects

for access to their own personal data will allow for the data subject to receive the relevant data in a structured and machine-readable format.

Right to erasure ('right to be forgotten'), right to restriction of processing, and right to object to processing: CQC will have a process to manage and respond to requests from data subjects that we should erase their personal data. CQC will have a process to manage and respond to requests from data subjects for the restriction of processing of personal data concerning him or her in specified ways or in specific circumstances. CQC will also have a process to manage and respond where a data subject objects to the processing of their personal data by CQC, on grounds relating to his or her personal situation.

These processes will recognise that these rights are qualified, and may be refused where CQC needs to continue processing the personal data for legitimate reasons (with a lawful basis), including where it is necessary and in the public interest to do so for the exercise of our functions or in relation to legal claims.

Right to rectification: CQC will have a process to manage and respond to requests from data subjects for the rectification of inaccurate personal data concerning him or her.

Rights in relation to automated decision making, including profiling: CQC will not use automated processing, without meaningful human input, to profile individuals or make decisions which significantly affect those data subjects, other than with the explicit consent of the data subject or where the processing is explicitly laid down in law. If CQC proposes to undertake such automated processing, this will be clearly communicated in published privacy notices.

Data protection by design and default, and data protection impact assessment (DPIA).

CQC will ensure that any new process or change which is likely to result in a high risk to privacy, or to the rights and freedoms of data subjects, is first subject to a DPIA.

This DPIA will include steps to establish the lawful basis for processing, and to understand and mitigate the likely risks.

The DPIA shall also ensure that the processing of personal data is minimised, and that appropriate technical and organisational measures are integral to the design and operation of systems and processes that involve processing of personal data.

Only transferring personal data outside of the UK or European Economic Area (EEA) where we have adequate assurance that it is lawful to do so and that appropriate protections are in place.

Where possible and practicable, CQC will process personal data within the UK/EEA. CQC will only process personal data outside of the UK/EEA where we have undertaken a DPIA and are satisfied that the personal data is afforded equivalent levels of protection as it would if processed within the UK/EEA, and that the transfer is lawful.

Notification of data breaches.

CQC will have a process under our Information Security Policy to ensure that data protection breaches are reported to the Information Commissioner's Office, and notified to data subjects, as required under data protection law.

Appointing a Data Protection Officer (DPO) and providing adequate resource for the DPO to perform his role.

CQC will appoint and maintain a DPO, and will provide the DPO with the resources required to effectively fulfil this statutory role.

Caldicott Principles

The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel was chaired by Dame Fiona Caldicott and it set out Principles that organisations should follow to ensure that personal data relating to people who use services is protected and only used when it is appropriate to do so. The Principles were extended to adult social care records in 2000 and further revised in 2013.

CQC will comply with the Caldicott Principles when processing personal data relating to people who use health and adult social care services. The Principles are:

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential personal data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Confidential personal data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for people who use care services to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of confidential personal data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of confidential personal data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to confidential personal data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling confidential personal data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient and service-user confidentiality.

Principle 6 - Comply with the law

Every use of confidential personal data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

CQC will have a Caldicott Guardian who will advise on, and monitor compliance with, the Caldicott Principles within CQC.

Confidential personal information (CPI)

Personal data that has been obtained by CQC on terms or in circumstances requiring it to be held in confidence is 'confidential personal data' (CPI) as defined by section 76 of the Health and Social Care Act 2008.

It is a criminal offence for any person to disclose CPI within the lifetime of the data subject, other than where a 'defence' to permit disclosure is met under section 77 of the same Act.

CQC is required to publish a Code of Practice on Confidential Personal Information ('The Code'), setting out the practice we will follow when obtaining, handling, using and disclosing CPI.

CQC will publish the Code and keep it under review to ensure that it is, and remains, compliant with data protection law and this policy. The Code will be the principle guide for CQC staff and agents in making any decisions about the processing of CPI.

Responsibilities

The following overarching responsibilities apply to all parts of the Data Protection Policy. Additional responsibilities are listed under the relevant parts of this policy.

Role	Responsibility
All staff (including those in roles below)	Processing personal data in accordance with this policy - as well as other related policies, processes and guidance - to comply with data protection law and to appropriately protect the privacy, rights and freedoms of data subjects.
The Chief Executive Officer (CEO) and the Board of Directors	Ensuring that systems are in place to support compliance with data protection law. Ensuring that CQC has an appropriate DPO, Caldicott Guardian and SIRO in post, and

	to ensure that they have adequate resources, freedom and authority to perform those roles.
Executive Team (ET)	Approving and signing off relevant policies and processes. Ensuring that policies, processes and systems established or adopted by CQC are compliant with data protection law.
Data Protection Officer (DPO)	To carry out the tasks under Article 39(1) of GDPR, to: • Inform and advise on compliance with GDPR. • Monitor compliance with GDPR. • Provide advice as regards data protection impact assessments. • Cooperate with the ICO. • Act as contact point with the ICO on issues relating to processing. To carry out these tasks with due regard to risks relating to the processing of personal data.
Senior Information Risk Owner (SIRO)	Responsibility for 'managing information risk across the organisation and for ensuring that the data and information assets of CQC are identified, processed, transmitted, stored and used in line with the principles of good information governance and in compliance with CQC's legal, statutory and organisational requirements.' (CQC, Corporate Governance Framework) See also Scheme of Delegation
The Caldicott Guardian	Providing advice and oversight to ensure that personal data relating to people who use the services we regulate is processed in accordance with the Caldicott Principles.
Information Governance Group (IGG)	Providing advice to the CQC Executive team, via the SIRO, on policies, systems, guidance, methodologies and training on data protection.

	Producing and signing off guidance and training materials on data protection issues. Maintaining and overseeing CQC's information risk register.
Information Rights Manager	Providing advice and promoting good practice across the organisation in relation to processing personal data in accordance with data protection law. Developing policies, guidance and training. Advising and supporting on the completion and sign-off of DPIAs. Managing and overseeing the work of the Information Access Team
Information Access Team	Recording, coordinating and responding to subject access requests.

Monitoring compliance

The Information Rights Manager will provide reports on compliance with data protection law and with this policy, when appropriate, using measures agreed with the ET and IGG. These reports will be presented to the DPO, Caldicott Guardian and SIRO at IGG meetings and key issues of compliance and performance will be reported to ET.

The DPO may report to ET or the Board on any aspect of compliance with GDPR. In accordance with Article 38(3) of GDPR, the DPO will not be instructed or restricted in the performance of their tasks.

Associated policies

- Information governance policy
- Information security policy
- Freedom of Information policy
- Knowledge and information management (KIM) policy
- Code of Practice on Confidential Personal Information

INFORMATION SECURITY POLICY

May 2018

Purpose

The Information Security Policy ("The Policy"), and the Information Security Standards ("the Standards") that sit under it, detail the high level security principles for the Care Quality Commission (CQC) and establish the framework under which each of the Standards should be interpreted, managed and applied. These documents have been produced in line with the requirements and guidance contained in ISO27001 and ISO27002:2005.

The overall purpose of the Policy is to provide an overview of CQC information security requirements. The overall purpose of the Standards is to provide a detailed reference document which may be used to address specific queries on information security.

The Policy and Standards apply, and will be available to, all staff working in the Commission in whatever capacity. They are also relevant as evidence of established information security practices during internal or external audit processes. Relevant sections of the Policy and Standards may also be used as a reference point in negotiating or agreeing contracts with external suppliers.

The measures and controls detailed within the Policy and Standards set the security goals within CQC in line with the security strategy to achieve compliance with ISO27001. To this end the policy details the intention of CQC to comply with the ISO standard, it does not provide a summary of the current state of security controls in place at any given time.

The purpose of detailing the ISO27001 compliant controls in this policy document is to set the standard that CQC aims to achieve and to provide the detail required by the business units and, where applicable, 3rd party suppliers to ensure that both existing and planned systems comply, or work incrementally towards compliance with, ISO27001.

Scope

The Policy and Standards have been developed for use across the whole of CQC and comply with the requirements of widely recognised good information security practice. They will:

- Assist staff to apply the correct level of security control to their day to day activities in line with good practice and applicable regulation and legislation.
- Assist with the development and commissioning of new processes and systems by detailing the required security settings and standards.
- Be formatted, controlled and distributed in line with CQC requirements.

The Policy and Standards will be available, as the correct up to date version, on the intranet to all staff.

Any departments or staff who have a requirement to store or otherwise use hard copies of the Policy and Standards should ensure that they frequently check that they have the latest version of the policy and refer any queries to the information security team. They should also ensure that any old, outdated versions of this document are destroyed and replaced as necessary.

Policy Statement

As the regulator of health and adult social care standards in England, the CQC aims to demonstrate the same standards of information security as we expect the services that we regulate to apply.

The importance of information security

Information can be defined as useful data for a particular analysis, decision or task. Information must always be protected appropriately irrespective of how it is stored, presented or communicated.

The main aims of information security are to preserve:

- **Confidentiality:** ensuring that information is accessible only to those who are authorised to have access.
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods.
- **Availability:** ensuring that authorised users have access to information when needed.

It also aims to support the requirements of:

- **Accountability:** accounting for the actions of individuals by monitoring their activities.
- **Non-Repudiation:** legally acceptable assurance that transmitted information has been issued from and received by the correct, appropriately authorised, individuals.

CQC has a responsibility to securely manage its information assets, the information made available to it by providers and the people who use providers' services, as well as that provided by its own employees, contractors, and business partners. CQC has a responsibility to protect that information from unauthorised disclosure, loss of integrity or loss of availability.

All parts and agents of the organisation are responsible for making sure that information is protected adequately in accordance with the Policy and Standards.

CQC recognises the sensitive nature of the information that the organisation holds and processes, and the serious potential harm that could be caused by security incidents affecting this information.

CQC will therefore give the highest priority to information security. This will mean that security matters will be considered as a high priority in making any business decisions. This will help ensure that CQC will allocate sufficient human, technical and financial resources to information security management, and will take appropriate action in response to all violations of Security Policy.

CQC will use this Security Policy and the Standards as the basis for an organisation-wide strategy to set the correct level of information security.

The security efforts will be:

- **Coordinated:** security measures will be based on a common framework provided by the Policy and Standards, and all staff will be involved in maintaining compliance with the security policy.
- **Proactive:** we will detect, identify and manage vulnerabilities, threats, and security gaps to prevent security incidents as far as we possibly can.
- **Supported at the highest level:** senior management are actively committed to information security and give their full support to implementing the required security controls that are identified through a continuous risk assessment process.

These security efforts will be structured and directed by the Security Policy, which covers all aspects of information security within CQC's business operations.

Responsibilities

Party	Key Responsibilities
All staff (including those in the roles below)	All staff will adhere to this Policy and the Standards. They will raise any issues of non-compliance, information risk or incidents with their line manager and the security team.
The Chief Executive Officer (CEO) and the Board of Directors	Ensuring that systems are in place to support appropriate information security measures
Senior Information Risk Owner (SIRO)	Responsibility for 'managing information risk across the organisation and for ensuring that the data and information assets of CQC are identified, processed, transmitted, stored and used in line with the principles of good information governance and in compliance with CQC's legal, statutory and organisational requirements.' (CQC, Corporate Governance Framework) See also Scheme of Delegation.
Information Governance Group	Approval, review and oversight of The Standards. Oversight, guidance and approval of the information risk and incident management processes. Providing advice to the CQC Executive team, via the SIRO, on policies, systems, guidance, methodologies and training for information security.
Information Security Manager	Definition, implementation, monitoring and management of the Information Security Management System (ISMS) and information security policy documents. Organisation, management and participation in any joint information security committees with the Department of Health, 3rd party ICT providers and other external organisations.
Data Protection Officer (DPO)	To carry out the tasks under Article 39(1) of GDPR, to: • Inform and advise on compliance with data

	protection law. • Monitor compliance with data protection law. • Provide advice as regards data protection impact assessments. • Cooperate with the ICO. • Act as contact point with the ICO on issues relating to processing. To carry out these tasks with due regard to risks relating to the processing of personal data.

Monitoring Compliance

Monitoring compliance and effectiveness of the Policy and Standards will be carried out in a number of ways:

- The Information Security Manager will provide reports on compliance with the Policy and Standards, when appropriate, using measures agreed with the ET and IGG. These reports will be presented to the DPO, Caldicott Guardian and SIRO at IGG meetings and key issues of compliance and performance will be reported to ET.
- Review of effectiveness during the information and compliance status reviews, which are part of the annual Data Security Toolkit submissions
- External audits commissioned in line with Department of Health and Social Care directives to check compliance with recognised security standards.
- Internal, targeted audits of specific information security areas. These will be triggered by the risk management process, incident management or areas of concern highlighted by staff or senior management of CQC.

All compliance monitoring, audits and reporting will be included on the agenda of the IG Group meetings and minutes along with any actions and responsible owners.

Associated policies

- Information governance policy
- Data Protection policy
- Freedom of Information policy
- Knowledge and information management (KIM) policy
- Code of Practice on Confidential Personal Information

FREEDOM OF INFORMATION POLICY

May 2018

Purpose

This policy defines the Care Quality Commission's (CQC) approach to complying with the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations (EIR).

Policy Statement

CQC recognises the importance of transparency and openness, and the public interest served through access to information held by public authorities.

CQC will comply with the requirements of FOIA and EIR, to make information that it holds publicly available whilst protecting personal data and other information where there is a legitimate and lawful basis for non-disclosure.

It will meet these statutory responsibilities by:

- Maintaining and publishing a **publication scheme**, following a scheme approved by the Information Commissioner,
- Making information publicly available in accordance with the publication scheme and other government requirements on transparency (by publication on CQC's website – www.cqc.org.uk – where appropriate),
- Responding to requests for information within the statutory deadline (20 working days),
- Providing any requested information that is held by CQC - except where a relevant exemption from disclosure applies and (where relevant) where there is an overriding public interest in withholding the information from disclosure,
- Implementing and operating a process of Internal Review, to allow for the consideration of any complaint relating to our compliance with FOIA or EIR, and
- Explaining the application and reason for applying any exemption, of the right to an Internal Review of any decision to withhold information, and of the further right of appeal to the Information Commissioner.

Scope

This policy applies to all information held by or on behalf of CQC, other than information held by CQC solely on behalf of another party.

Information held on behalf of CQC will include information held by third parties acting under CQC's instruction. It will also include information held by CQC staff outside of its systems and property, where that information is being processed for the purposes of CQC's activities..

This policy should be read alongside the 'associated policies' listed at the end of the document.

Responsibilities

The following overarching responsibilities apply to all parts of the Freedom of Information Policy. Additional responsibilities are listed under the relevant parts of this policy.

Role	**Responsibility**
The Chief Executive Officer (CEO)	Ensuring that systems are in place to support compliance with the FOIA and EIR.
Executive Team (ET)	Approving and signing off relevant policies and processes.
Senior Information Risk Owner (SIRO)	Responsibility for 'managing information risk across the organisation and for ensuring that the data and information assets of CQC are identified, processed, transmitted, stored and used in line with the principles of good information governance and in compliance with CQC's legal, statutory and organisational requirements.' (CQC, *Corporate Governance Framework*)

Information Governance Group (IGG)	Providing advice to the CQC Executive team, via the SIRO, on policies, systems, guidance, methodologies and training on FOIA and EIR. Producing and signing off guidance and training materials on FOIA and EIR. Maintaining and overseeing CQC's information risk register.
Information Rights Manager	Providing advice and promoting good practice across the organisation in relation to FOIA and EIR. Developing policies, guidance and training. Maintaining CQC's Publication Scheme. Managing and overseeing the work of the Information Access Team.
Information Access Team	Recording, coordinating and responding to requests for information under FOIA and EIR. Ensuring that responses are signed off in accordance with CQC's Scheme of Delegation.
All staff (including those in roles above)	To maintain appropriate records in accordance with CQC policies and procedures. To assist as required in locating, extracting and reviewing information for the purpose of responding to FOIA and EIR requests.

Monitoring compliance

The Information Rights Manager will provide reports on compliance with FOIA, EIR and with this policy, when appropriate, using measures agreed with the IGG. These

reports will be presented to the SIRO at IGG meetings and key issues of compliance and performance will be reported to ET.

Associated policies

- Information governance policy
- Data Protection policy
- Information security policy
- Knowledge and information management (KIM) policy
- Code of Practice on Confidential Personal Information

KNOWLEDGE AND INFORMATION MANAGEMENT POLICY

December 2017

Purpose

This policy defines the Care Quality Commission's (CQC) approach to knowledge and information management. It provides assurance that our practices comply with legislation and business requirements.

It sets out a framework under which specific records management policies and procedures exist. This ensures we all follow good practice to control records created internally, or received from external sources. It also provides clarity on the roles, responsibilities and accountabilities to follow the policy requirements.

Policy statement

Records provide vital evidence of business decisions, activities and transactions. They are also essential in ensuring that CQC meets legislative and regulatory requirements. CQC provides, and continually develops, robust practices and processes to meet these requirements.

Effective records management will underpin the priorities detailed in shaping our future: CQC's strategy for 2016 to 2021:

1. **Encourage improvement, innovation and sustainability in care** by linking changes in the business approach to regulation, to our approach to records management.
2. **Deliver an intelligence-driven approach to regulation** by defining standards to ensure a consistent approach to records management that enable us to 'use our information from the public and providers more effectively to target resources'.
3. **Promote a single shared view of quality** by ensuring that the integrity of records is maintained. Records storage protects sensitive information while still enabling data sharing with partners.
4. **Improve our efficiency and effectiveness** by promoting 'digital first' and by managing and disposing of records, once they no longer have a value to the business, to minimise the costs associated with physical and electronic storage.

CQC will provide training and guidance to ensure staff understand their legal responsibilities and can apply best practice in managing records. The key benefits for supporting CQC in this are that records are:

- Captured and stored in the right place.
- Authentic so CQC are confident that records are accurate.
- Accessible in a timely way, by those who need or have a right to see them.

- Protected from unauthorised deletion, changes or access.
- Disposed of appropriately once they are no longer required.

Records should be held in electronic format to meet the requirements of the government's digital strategy and to support easy access. **Therefore, the policies and associated guidance that support this policy are designed to achieve this goal while also supporting management of records that only exist in paper format.**

Scope

This policy principally applies to business related information contained within CQC records that are held in an office, including home offices, and on CQC systems.

For the purposes of this policy although copies of records, such as a paper print outs from systems, are not classed as records the information they contain must be stored and managed in a way that prevents unauthorised access to the information that they contain.

This policy also applies to records stored by contracted 3rd party organisations who hold or process CQC business information.

The policy applies to records in any format, for example electronic files, database entries, paper files, audio recordings, or video recordings. It also applies to anyone who creates or has access to information stored in CQC systems or offices, including home offices.

Definitions

Records management is the practice of managing the records of an organisation throughout their life cycle, from creation or receipt to their eventual disposal or transfer to permanent storage.

A **Record** is information created, received and/or maintained as evidence by CQC in its pursuance of legal obligations or business transactions, regardless of format. Records serve to detail CQC's functions, policies, decisions, procedures, or operations. Copies of records, or parts of them are not records. Templates and blank forms are not records until completed.

An **Information asset** is a record or group of records, defined and managed as a single unit.

Information asset register describes CQC's information assets; it details their owner, use, format, sensitivity, retention period, storage location and if they contain Confidential Personal Information (CPI).

Legislative and best practice framework

CQC will comply with the following legislative and best practice principles for information management.
Legislation:

- The General Data Protection Regulation
- The Data Protection Act 2018
- The Freedom of Information Act 2000.
- The Police and Criminal Records Act 1984 (PACE).
- The Public Records Act 1958.

Best practice:

- Information and Documentation – Records Management ISO 15489.
- Information Security Management ISO 27001.
- Cabinet Office Security Policy Framework.
- The Caldicott Principles.
- Information Governance Toolkit requirements.
- Information Security management NHS Code of Practice 2007.
- Evidential Weight and Legal Admissibility of Electronic Information (BS 10008).

Key principle

Records are a valuable corporate asset and must be managed in a way that recognises this.

This principle of robust records management policies, procedures and practices mean CQC will:

- Meet legal responsibilities.
- Manage records in line with recognised best practice.
- Manage records with a consistent approach to eliminate variation.
- Be able to find and analyse records easily.
- Be confident that records are reliable and accurate.
- Be able to use records to identify poor care in an efficient manner.
- Use records to support regulatory and enforcement activities.
- Prevent loss or unauthorised access of records.
- Reduce paper storage.
- Store records securely.
- Only store records whilst there is a business need.
- Save time and money.
- Make judgements based on accurate records.

Records management policy framework

This policy provides the framework under which all related policies and associated processes sit. The policies support CQCs records management requirements and include four key activities:

Planning

Policies and guidance will be planned and updated to provide support for:

- Maintaining an accurate Information Asset Register,
- Training all staff,
- Changes in legislation or business requirements.

Creation and capture

Policies and guidance support the identification of records and define standards for:

- Naming electronic records,
- Managing paper and handwritten records,
- Scanning paper records to ensure they comply with current legal requirements and best practice when creating electronic records,
- Managing emails which are CQC records.

Storage, maintenance and access

Policies and guidance support record storage and maintenance by defining standards for:

- Protecting sensitive or confidential information,
- Sharing records,
- Version control,
- Storing and maintaining paper,
- Managing records within shared systems, including emerging technologies such as the Cloud.

Retention, review and disposal

Policies and guidance define the processes and methods for managing records at the end of their lifecycle by defining standards for:

- Identifying retention periods for categories of records based on business need and legislative requirements,
- Supporting the secure disposal of records,
- Defining which records need preserving and the procedures associated with this.

Responsibilities

The following list of responsibilities applies to all records management policies. Where additional responsibilities apply to an individual activity, such as email management, these are in the specific policy.

Role	Responsibility
All staff (including those in roles below)	Managing records in line with this policy as well as other related policies and guidance to comply with legislative and business requirements.
The Chief Executive Officer (CEO)	Ensuring that systems are in place to support access and management of records, and continuity of service.
Executive Team (ET)	Approving and signing off relevant records management policies.
Senior Information Risk Owner (SIRO)	Responsibility for 'managing information risk across the organisation and for ensuring that the data and information assets of CQC are identified, processed, transmitted, stored and used in line with the principles of good information governance and in compliance with CQC's legal, statutory and organisational requirements.' (CQC, Corporate Governance Framework) See also Scheme of Delegation
The Caldicott Guardian	Providing 'advice and oversight to ensure that confidential personal information relating to people who use the services we regulate is obtained, used, handled and shared appropriately and lawfully' (CQC Code of Practice-CPI) See also Scheme of Delegation
Information Governance Group (IGG)	Providing advice to the CQC Executive team, via the SIRO, on policies, systems, guidance, methodologies and training for information governance (including records management).
Knowledge and Information Manager	Providing advice and promoting good practice in records management across the organisation, ensuring the development of policies and guidance.
Information Asset Owners (IAO)	Understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. (Cabinet Office) As defined in the Scheme of Delegation part 2. This includes responsibility for ensuring that the systems used to manage information assets in their area have an identified system owner. The system owner is responsible for ensuring appropriate controls are in place and legislative requirements are met. As defined in the IT Systems governance policy.
Information Asset Managers (IAM)	Overseeing the identification and management of records within their teams. Implementing practical processes associated with this policy, advising the IAO of risks and mitigating actions. As

	defined in the Scheme of Delegation part 2.
Information Asset Administrators (KIM Champions)	Day-to-day administration of records, promoting good information management practice. Monitoring and reporting on compliance to the Knowledge and Information Manager and highlighting risks to the IAM. As defined in the Scheme of Delegation part 2.

Monitoring compliance

The Knowledge and Information Manager will provide reports on compliance with this policy, when appropriate. These reports will be presented to the SIRO at IGG meetings as well as being sent to IAOs. The IAO will investigate where compliance is below expected levels, and provide the SIRO with assurance that issues have been resolved.

Associated policies

- Information governance policy
- Data protection policy
- Information security policy
- Freedom of Information policy
- Code of Practice on Confidential Personal Information

CQC Policy Statement on the sensitive processing of personal data for any of the law enforcement purposes under the Data Protection Act 2018

Background

CQC has criminal enforcement powers and the power to prosecute under various legislation. These are:

- Health and Social Care Act 2008
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Care Quality Commission (Registration) Regulations 2009.
- Health and Safety at Work Act 1974

Under the legislation listed above, CQC may prosecute for offences listed under the Act, but also for specific breaches of the Regulations. The above list is not exhaustive.

More details on the action we take is listed in the Enforcement Handbook. CQC is therefore considered a competent authority as per section 30(1)(b) of the Data Protection Act 2018 as we are processing personal data for the "law enforcement purposes".

Where CQC relies on section 35(4) or (5) for a lawful and fair basis for the sensitive processing of personal data for any of the law enforcement purposes, CQC must have an appropriate policy document in place, as per section 42 of the Data Protection Act 2018.

Such a policy document must:

a) explain CQC's procedures for securing compliance with the data protection principles (see section 34(1)) relating to sensitive processing, and

b) explain CQC's policies about the retention and erasure of the personal data being processed, giving an indication of how long such personal data is likely to be retained.

These policies and procedures are detailed below.

(a) CQC's procedures for securing compliance with the data protection principles

Law enforcement personal data will also be Confidential Personal Information as per Section 76 of the Health and Social Care Act 2008 (HSCA 2008).

Under section 80 of the HSCA 2008 the Commission must prepare and publish a code in respect of the practice it proposes to follow in relation to confidential personal information

The published Code of Practice on Confidential Personal Information (COP) defines how CQC will secure compliance with the data protection principles.

Therefore, the procedures for securing compliance with the data protection principles

Principle 1 – This is covered under practice 1, 2 & 3 from page 13 of the COP
Principle 2 – This is covered under practice 1, 2 & 3 from page 13 of the COP
Principle 3 – This is covered under the necessity test from page 9 of the COP
Principle 4 – Where we have law enforcement personal data we will take steps to ensure the accuracy and up to date nature of any law enforcement personal data in line with our Enforcement Policies and Procedures. CQC will have due regard for the source of any personal data and whether it is based on fact or personal opinion. CQC also explains a data subjects right to correction of incorrect or incomplete personal data in our Privacy Statement.
Principle 5 – This is covered under part (b) (see below)
Principle 6 – This is covered under practice 4 from page 25 of the COP

(b) CQC's policies about the retention and erasure of the personal data being processed

CQC will retain information only for as long as is necessary for fulfilling our own regulatory functions or where required to comply with other legal requirements. CQC has a Retention and Disposal Policy and Guidance which supports the retention and destruction process.

CQC's retention and disposal schedule is published on the CQC Website. This details the retention periods currently used by CQC.

Data Protection Act 2018

42 Safeguards: sensitive processing

(1)This section applies for the purposes of section 35(4) and (5) (which require a controller to have an appropriate policy document in place when carrying out sensitive processing in reliance on the consent of the data subject or, as the case may be, in reliance on a condition specified in Schedule 8).

(2)The controller has an appropriate policy document in place in relation to the sensitive processing if the controller has produced a document which—

(a)explains the controller's procedures for securing compliance with the data protection principles (see section 34(1)) in connection with sensitive processing in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, and

(b)explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.

(3)Where personal data is processed on the basis that an appropriate policy document is in place, the controller must during the relevant period—

(a)retain the appropriate policy document,

(b)review and (if appropriate) update it from time to time, and

(c)make it available to the Commissioner, on request, without charge.

(4)The record maintained by the controller under section 61(1) and, where the sensitive processing is carried out by a processor on behalf of the controller, the record maintained by the processor under section 61(3) must include the following information—

(a)whether the sensitive processing is carried out in reliance on the consent of the data subject or, if not, which condition in Schedule 8 is relied on,

(b)how the processing satisfies section 35 (lawfulness of processing), and

(c)whether the personal data is retained and erased in accordance with the policies described in subsection (2)(b) and, if it is not, the reasons for not following those policies.

(5)In this section, "relevant period", in relation to sensitive processing in reliance on the consent of the data subject or in reliance on a condition specified in Schedule 8, means a period which—

(a)begins when the controller starts to carry out the sensitive processing in reliance on the data subject's consent or (as the case may be) in reliance on that condition, and

(b)ends at the end of the period of 6 months beginning when the controller ceases to carry out the processing.