



Code of Practice on confidential personal information

December 2010

Contents

1. Introduction	2
The Care Quality Commission	2
The purpose of this Code of Practice	2
Our functions and powers	3
What is confidential personal information?	5
2. The principles	6
3. How we will decide what actions are 'necessary' in relation to confidential personal information	8
The necessity test	8
Mental capacity	10
4. Obtaining confidential personal information	11
Confidential personal information volunteered by the person to whom it relates	11
Confidential personal information volunteered by a third party	12
Confidential personal information obtained when using our powers, or where the information is otherwise required by law	13
5. Using confidential personal information	14
6. Secure holding and handling of confidential personal information	16
7. Retention and disposal of confidential personal information	17
8. Disclosing, sharing or publishing confidential personal information	18
Sharing information with, or disclosing information to, other organisations	18
Publishing information	19
Access to information	20
9. Governance of this Code	21
10. Keeping this Code under review	22
Appendix: The legal framework	23

1. Introduction

The Care Quality Commission

- 1.1 The Care Quality Commission (CQC) is the independent regulator of health and adult social care services in England. We were established by the Health and Social Care Act 2008 and replaced the former Commission for Social Care Inspection, Healthcare Commission and Mental Health Act Commission.
- 1.2 Our values are to:
 - Put the people who use health and social care services first, be informed by what they tell us and stand up for their rights and dignity.
 - Be independent.
 - Be expert and authoritative, basing our actions on high quality evidence.
 - Be a champion for joined-up care across services.
 - Work with service providers and the professions to agree definitions of quality.
 - Be visible, open, transparent and accountable.
- 1.3 For further information about the Care Quality Commission and what we do, you can call our Customer Services team on 03000 616161, send an email to enquiries@cqc.org.uk or visit our website at www.cqc.org.uk

The purpose of this Code of Practice

- 1.4 The Health and Social Care Act 2008 requires us to publish a code that sets out the practice we will follow in obtaining, handling, using and disclosing confidential personal information.
- 1.5 This Code of Practice fulfills that requirement. We intend it to be used in two main ways:
 - By our staff, to set out how we will work and to provide a point of reference against which our practice can be judged. The Code will help us to continually develop policies, processes and training. These will, in turn, generate detailed guidance to our staff on issues relating to confidential personal information.
 - By our stakeholders (people who use services, carers, the public, providers of health and social care, and other regulatory bodies), to find out about the principles that they can expect us to follow, and to be reassured about our use of confidential personal information.
- 1.6 As the regulatory body within health and social care, we have a role in promoting good practice and we intend to use this Code to contribute to that role.

Our functions and powers

- 1.7 Our functions (the jobs we were set up to do) include the registration of health and social care providers to ensure that essential standards of quality and safety are being met; reviewing and investigating the quality of the services they provide; and protecting the interests of people whose rights are restricted under the Mental Health Act 1983.
- 1.8 Our main objective in performing our functions is to protect and promote the health, safety and welfare of people who use health and social care services.
- 1.9 Schedule 9 of the Health and Social Care Act 2008 allows us to help other public authorities to carry out their functions. This may include sharing confidential personal information with them where we think it is appropriate and in the public interest to do so.
- 1.10 We have a specific range of 'regulatory functions' and, to enable us to exercise these functions, we have extensive powers, including:
 - Entering and inspecting premises that are, or that we reasonably believe to be, 'regulated premises' (premises or vehicles that are used to 'carry on' a regulated care activity, or owned or controlled by an NHS body or local authority, or used – or proposed to be used – to provide NHS care or adult social services).
 - Accessing or obtaining documents or records (including those held on computer) in the course of an inspection.
 - Requiring any information, documents or records that we think is necessary for the exercise of our regulatory functions from:
 - Any English NHS body.
 - Any person providing health care commissioned (purchased or arranged) by the NHS.
 - Any English local authority.
 - Any person providing adult social care services commissioned by an English local authority.
 - Any person who 'carries on' or manages a health or social care activity of a type regulated by CQC.
- 1.11 Section 60(2) of the Health and Social Care Act 2008 defines these regulatory functions as:
 - The registration of health and social care activities, including:
 - The registration of providers and managers.
 - Assessing their compliance with registration regulations.
 - Enforcement action and prosecutions for offences under the Act or for failure to comply with regulations.
 - Providing/publishing registers of registered providers.
 - Receiving notifications of certain matters as required by the Act.

- Carrying out reviews and investigations of health and adult social care services provided or commissioned by NHS bodies and local authorities, and publishing reports of the assessments.
 - Conducting studies of the economy, efficiency and effectiveness with which NHS bodies and local authorities commission, manage or provide health and adult social care services, including comparing the performance of different commissioning organisations and providers, and publishing the results of these studies.
 - Carrying out and publishing special reviews and studies that look at themes in health and social care, by focusing on services provided, pathways of care or the experience of care received by particular groups of people. These reviews and studies are designed to help us make recommendations for improving the care or the management of NHS bodies or local authorities. Further information is available on our website at www.cqc.org.uk/reviewsandstudies.cfm.
- 1.12 We cannot use our powers under the Health and Social Care Act to inspect premises and obtain information for any other purpose.
- 1.13 We also have some functions and powers under other Acts.
- 1.14 Another function is to keep the use of the Mental Health Act under review and to ensure that it is being used properly – in particular, the powers of detention under that Act.
- 1.15 To help us do this, we have powers under the Mental Health Act to visit and interview detained patients, and to access records relating to their detention and treatment, or to access or obtain other information that we reasonably require.
- 1.16 We are also an 'enforcing authority' under the Health and Safety at Work Act in relation to the Ionising Radiation (Medical Exposure) Regulations 2000 (IR(ME)R).
- 1.17 Our role is to ensure that the medical use of ionising radiation is carried out in accordance with the regulations (and the 2006 amendment), to minimise the risk to patients.
- 1.18 In undertaking our responsibility as the 'enforcing authority' for the IR(ME)R regulations, we have powers under the Health and Safety at Work Act to enter premises, interview staff and access or obtain information to check compliance with the regulations, and to investigate notifications of incidents relating to medical ionising radiation (which certain care providers are required to submit to us).
- 1.19 We will apply the same principles to the access, use and disclosure of information in relation to our functions under the Mental Health Act and the Health & Safety at Work Act/IR(ME)R as we do to the to the access, use and disclosure of information in relation to our regulatory functions under the Health and Social Care Act 2008.

What is 'confidential personal information'?

- 1.20 The Health and Social Care Act defines 'confidential personal information' as information that "is obtained by the Commission in terms or circumstances requiring it to be held in confidence and relates to and identifies an individual".
- 1.21 Confidential personal information is likely to include (but is not limited to) information about a person's:
- Physical or mental health.
 - Social or family circumstances.
 - Financial standing and financial details.
 - Education, training and employment experience.
 - Religious beliefs.
 - Racial or ethnic origin.
 - Sexuality.
 - Criminal convictions.
- 1.22 The information may relate to people who use services, their families, carers or representatives, registered providers, health and social care staff, our own staff, or any other person who has contact with CQC. Although we acknowledge that some information is more sensitive than others (for example, information about a person's sexual health is more likely to be sensitive than information about a broken leg, as disclosure of that information is more likely to cause damage or distress to the person to whom it relates), we will apply the same principles and standards of care to all confidential personal information that we hold.
- 1.23 It is a criminal offence under the Health and Social Care Act 2008 for anyone to disclose confidential personal information that has been obtained by CQC, other than in certain circumstances. We intend this Code of Practice to help our staff ensure that they only disclose confidential personal information where it is lawful to do so.

2. The principles

- 2.1 We have translated the various laws (see appendix) into a set of principles that represent our approach to obtaining, handling, using and disclosing confidential personal information.
- 2.2 Our main objective is to protect and promote the health, safety and welfare of people who use health and social care services.
- 2.3 We have developed the following Principles to ensure that we give the fullest possible consideration and protection to people's privacy and dignity, without restricting our powers or our ability to achieve this objective.

2.4 **Principle 1**

We will only obtain confidential personal information where it is necessary to do so for the purpose of exercising our functions.

Principle 2

To ensure that we are not restricted in our ability to protect and promote the health, safety and welfare of people who use health and social care services, we will not seek consent where it is *necessary* to obtain, use or disclose confidential personal information to perform our *regulatory* functions, or for our functions under the Mental Health Act or Health and Safety at Work Act. However, in these circumstances, we will take all practical steps to involve those people in any decision to access their information. When obtaining confidential personal information for other purposes, we will seek consent, wherever it is possible and practicable to do so.

Principle 3

Wherever it is possible and practicable to do so, we will keep individuals informed about how, why and when we use and disclose their confidential personal information, and we will listen and give consideration to their views and concerns when making decisions relating to this information.

Principle 4

We will use only the minimum necessary confidential personal information. We will use anonymised information wherever possible, and we will securely dispose of confidential personal information when it is no longer needed.

Principle 5

In all cases, we will hold and handle confidential personal information securely and sensitively, and we will actively seek to minimise any risk of damage or distress that may be caused to the individuals to whom the information relates.

Principle 6

We will only share, disclose or publish confidential personal information where it is lawful to do so, where it is in the significant public interest to do so, and where the recipients of the information have a genuine 'need to know'.

Principle 7

We will obtain, handle, use and disclose information relating to deceased people in accordance with the same principles that we apply to information about living people, with sensitivity to their families and friends, and with consideration of any previously recorded wishes of the deceased.

Principle 8

We will comply with, and keep up to date with, the law, and have regard to changing issues of ethics and best practice regarding confidential personal information, by regularly reviewing and updating this Code of Practice.

Principle 9

We will be open and transparent in our arrangements and processes for obtaining, handling, using and disclosing confidential personal information.

3. How we will decide what actions are 'necessary' in relation to confidential personal information

- 3.1 We may only use our powers to obtain confidential personal information when doing so is 'necessary' to perform our regulatory functions, or for our functions under the Mental Health Act or Health and Safety at Work Act, as explained in section 1 of this Code.
- 3.2 We also rely on conditions under the Data Protection Act 1998 that allow us to process personal information, where doing so is 'necessary' to carry out our functions under various Acts.
- 3.3 At various points within this Code we refer to making decisions as to whether certain actions in relation to confidential personal information are 'necessary'.
- 3.4 It is therefore important to establish how we will decide whether it is 'necessary' to obtain, use or disclose confidential personal information in any particular case.

The necessity test

- 3.5 To make a decision as to whether it is necessary to obtain, use or disclose confidential personal information, we will consider two factors:
- 3.6 Firstly: Whether obtaining, using or disclosing the information is a necessary step for us to perform a particular function – for example, because it would not be possible or practicable, or would require significant and disproportionate extra cost or effort, to perform the function without doing so. We must act in a way that causes minimum interference with the privacy and rights of people who use care services; and this requires us to ask ourselves whether there are other ways of achieving our aim that would minimise such interference.
- 3.7 Secondly: Whether it is necessary and in the public interest to perform the function in the particular circumstances. This means that we will consider whether the public interest served by performing the function justifies any potential impact on people's privacy.
- 3.8 This second factor may require us to carefully consider and balance different issues, including:
 - Whether the person has given consent.
 - Any objections, concerns or opinions expressed by them (or their family, carer or representative).
 - The general interest in maintaining trust in the confidentiality of health and social care services and the work of CQC.

- The sensitivity of, and potential damage that could be caused by the use or disclosure of, the information.
 - The public interest to be served by performing the function – in particular, the extent to which performing it will protect the health, wellbeing, and legitimate rights and interests of others.
- 3.9 As an example: CQC must consider a range of issues before deciding to prosecute a provider for a breach of regulations. One of those considerations should be the potential impact on people's privacy. We may decide that a prosecution would not be justified if it required us to obtain, use and disclose confidential personal information about people who use a service in a way that would have a very significant impact on their privacy and dignity. Of course, we have an overriding duty to protect the health and welfare of people who use services but, in the circumstances described, we may decide that this duty could be best met by using one of our range of other enforcement powers to protect the privacy of those people.
- 3.10 Where we believe it is necessary to obtain, use or disclose confidential personal information to perform our regulatory functions, we will notify the people to whom that information relates (if it is possible and practicable to do so) and will advise them how and why we intend to access the information. We will also advise them how we intend to use the information and who, if anyone, we may share it with. We will give them an opportunity to raise any objections to this – either verbally or in writing, as appropriate. We will record any objections raised and consider them when deciding whether the public interest justifies the access and use of the information. We will take all reasonable steps to let those people know the outcome of this decision.
- 3.11 If a person wishes to appeal or complain about our decision to obtain, use or disclose their confidential personal information, we will handle this in accordance with our corporate complaints process. In the first instance, the matter will be referred to the line manager of the person who has made the decision to obtain, use or disclose the information for review, and the complaint may be escalated further if a satisfactory outcome is not reached.
- 3.12 If it is possible to delay obtaining, using or disclosing the information, without prejudicing our ability to carry out our regulatory functions, we will do so until the appeal or complaint has reached its conclusion.
- 3.13 Details of our corporate complaints process is available at:
www.cqc.org.uk/contactus/howtoraiseaconcernorcomplaint/howtocomplainaboutcqc.cfm
- 3.14 Decisions of 'necessity' made by our staff must be recorded and will be subject to regular audit. Our policies, guidance and training – and line-management supervision – will support our staff in making these decisions.

Mental capacity

- 3.15 When we are considering issues relating to seeking consent – or of notifying people and considering any objections – to obtain, use or disclose their confidential personal information, we must consider the mental capacity of those people and ensure that they are given any necessary support to make any decisions about their own lives.
- 3.16 A person lacks capacity to make a particular decision if they cannot either:
- Understand information relevant to the decision, or
 - Remember the information long enough to make the decision, or
 - Weigh up information relevant to the decision, or
 - Communicate their decision – by talking, using sign language, or by any other means.
- 3.17 If there are doubts about a person's capacity to make a decision, we must still help them to make it as independently as possible. This will include:
- Making sure that the person has all the relevant information they need to make the decision. If there are choices, this includes information about the alternatives.
 - Explaining or presenting the decision in a way that is easier for them to understand. For example, some people will find it easier to understand if staff use pictures, photographs, videos, tapes or sign language.
 - Discussing the matter at times of the day or in places where the person will better understand. For example, it is not the right time to ask someone to make a decision after they have taken medication that makes them drowsy.
 - Asking someone to become involved who may be better able to help the person understand, for example a relative, friend or advocate who knows them well.
- 3.18 Where a person is assessed as lacking capacity, decisions must be made in that person's best interests, in accordance with the Mental Capacity Act 2005.
- 3.19 Our policies, procedures and guidance relating to circumstances where we may wish to obtain, use or disclose the personal information of people who lack the capacity to consent (for example, during a site visit) provide guidance to staff on how to decide whether a person lacks consent, and how to proceed.

4. Obtaining confidential personal information

4.1 We can obtain confidential personal information in three ways:

- When it is volunteered by the person to whom the information relates,
- When it is volunteered by third parties who have confidential personal information in their possession, and
- When we obtain it while using our statutory powers, or where a service provider is otherwise required by law to provide information to us.

Confidential personal information volunteered by the person to whom it relates

4.2 Examples would include:

- When a person who uses services contacts our helpline to express concerns about the treatment or services he has received from a provider of health or social care. (We do not have powers to investigate complaints against care providers – other than in relation to our powers under the Mental Health Act – or to offer remedy in such circumstances. However, we may use information obtained in this way to perform our statutory functions – for example, by using the information received from a person who uses services to assess those services and/or as evidence to support enforcement action.)
- When a person responds to an invitation from CQC to provide an opinion in relation to a provider of health or social care that is being assessed.
- When a person who uses services or a member of care staff agrees to be interviewed as part of an inspection or investigation.
- Confidential information, such as information about criminal convictions, provided in applications and supporting documentation as part of an application to register as a care provider or manager.

4.3 Where confidential personal information is volunteered to us by the person to whom the information relates, we will assume that they wish us to maintain their confidentiality, unless they agree or indicate otherwise.

4.4 We will take all reasonable steps to ensure that we fully inform people of the purposes for which we will use their information, and of their legal rights before, or at the time that, they provide their personal information to us.

4.5 There may be occasions where we have to use this confidential personal information without consent. We will only use confidential personal information without consent where it is lawful and in the overall public interest to do so. This may include circumstances where it is necessary to use the information to perform our regulatory functions. In doing so, we will be mindful of any damage or distress that the use or

disclosure of the information may cause to the person(s) and to any objections that they have made to its use, and we will balance this against the public interest that will be served by that use or disclosure (see section 3 of this code for details of how we will make this judgement).

Confidential personal information volunteered by a third party

4.6 Examples would include:

- Confidential personal information volunteered to us by other regulators, professional bodies and law enforcement agencies. Confidential personal information volunteered in these circumstances will often be provided in the expectation that we will use that information to perform our regulatory functions.
- When a relative or carer of a person who uses services contacts us on their behalf, to express concerns about the treatment or services received from a provider of health or social care.
- When a member of care service staff volunteers information about that service to us, that is 'whistleblowers'.
- References or supporting information received to support an application to register as a care provider or manager.
- Information supplied by providers as evidence that they are complying with regulations, for example, staff training records or a controlled drug register.

4.7 Where confidential personal information has been provided by a third party, it may not be reasonable or practicable for us to obtain consent to use or to disclose the information from the person to whom it relates, or to advise them that we have received the information. For example, if the relevant person is incapable of providing their consent to use or disclose the information due to advanced dementia (in accordance with assessment against the provisions of the Mental Capacity Act), or if the information provided by another public body relates to a very large number of people.

4.8 We will take any reasonable and proportionate steps to inform people that we have their personal information, why we have it, and what we intend to do with it.

4.9 We will assume that the person(s) to whom the information relates wishes to have their confidentiality maintained, unless they agree or indicate otherwise.

4.10 As described above, circumstances may lawfully permit us to use or to disclose that information without consent or notifying the person(s). This may be because we consider that doing so is necessary to carry out our functions and is in the overall public interest. In doing so, we will be mindful of any damage or distress that using or disclosing the information may cause to the person(s) and we will balance this against the public interest that will be served by that use or disclosure. (See section 3 of this Code for details of how we will make this judgement.)

Confidential personal information obtained when using our powers or where the information is otherwise required by law

4.11 As stated previously (in section 1 of this Code), the Health and Social Care Act 2008 and other legislation provide us with extensive powers to:

- Inspect, take copies, seize and remove information from premises we are inspecting, and
- Compel certain people to provide us with information.

4.12 We will use our powers to obtain information only when it is necessary for the purposes of our regulatory functions. (See section 1 of this Code for an explanation of our regulatory functions, and section 3 for details of how we will make this judgement.)

4.13 Consequently, we will not seek the prior consent of relevant people in these circumstances – because refusal would prejudice our ability to properly discharge our regulatory functions.

4.14 We will not use our powers to obtain confidential personal information where the task in question can be achieved, practicably, using less intrusive means. For example, where we are able to use anonymised information instead.

4.15 Where obtaining confidential personal information is necessary to carry out our regulatory functions, we will ensure that we use our powers responsibly, proportionately and in accordance with the principles of this Code.

4.16 When making the decision to use our powers to obtain information, we will be mindful of any reasonably foreseeable damage or distress that this may cause to the person(s), and we will balance this against the public interest that will be served by obtaining and using the information. (See section 3 of this Code for details of how we will make this judgement.)

4.17 We will not obtain more confidential personal information than is necessary for the specific task in question. We will record the reasons for obtaining confidential personal information in writing and they will be subject to regular audit by our Information Governance team and the Audit and Risk Committee. This record will be made by the member of our staff who is responsible for the decision. Where and how they make and/or keep the record will depend upon the function being exercised, and instructions on this will be included in the policy/guidance for that activity.

4.18 We will inform the relevant person(s) that we have obtained their confidential personal information as part of our regulatory functions unless it is impractical and disproportionate, or would prejudice our ability to discharge our functions, to do so. We will develop and publish guidance to assist our staff in making this judgement.

4.19 Once we have obtained the information, we will decide how to use it in the same way as we would for information that has been voluntarily provided to us by third parties (as described above).

5. Using confidential personal information

- 5.1 We use confidential personal information to assess whether service providers are complying with the requirements of regulations. These regulations govern the quality and safety of services. We also use this information to understand whether the care experienced by people who use services meets the essential standards set out by the regulations. To do this, we sometimes need to look in detail at the care that people actually receive. This allows us to understand their experiences and to check that service providers comply with the law.
- 5.2 Where possible, we use information that is anonymous or aggregated to help make our decisions. For example, if we are checking that medication has been given accurately and on time within a care service (as part of our monitoring of compliance with regulations), we may ask to look at that organisation's audit of medicines administration. If that was not satisfactory – or none existed – we would then look further, which could involve seeing people's details. Examples of such further investigations might be to examine incident records to look for medicines errors, or to check controlled drugs registers. If these gave any cause for concern, we may then need to look at individual personal records, such as treatment or care plans, to ensure that we gather the evidence we need.
- 5.3 We may also use confidential personal information when undertaking more detailed studies of particular issues within care. Again, the use of this information allows us to understand the experiences of people who use these services, and this ensures that the findings and conclusions of our studies reflect the outcomes being achieved within that service.
- 5.4 Overall, checking confidential personal information helps us to monitor service providers' compliance with the law, drive improvement, stamp out bad practice, and produce information that people who use services, the public and other regulators can use to inform decisions and make choices.
- 5.5 We also use confidential personal information to perform our function of monitoring the use of the Mental Health Act and of protecting the rights of people who are detained under that Act, and for our functions of ensuring compliance with IR(ME)R and investigating incidents in relation to the medical use of ionising radiation.
- 5.6 We will tell the relevant person(s) how and why their confidential personal information has been used, unless it is impractical and disproportionate, or would prejudice our ability to discharge our functions, to do so. We will develop and publish guidance to help our staff to make this judgement.
- 5.7 Where we have used our powers to obtain confidential personal information to carry out our regulatory functions, we will not normally use that information for purposes other than to carry out our regulatory functions (unless it is suitably anonymised first).

- 5.8 If we think it is necessary to do so, we may re-use any information that we have obtained for whatever purpose, to carry out our regulatory functions. For example, if we were conducting an interview to decide whether to register a person as a manager of a care service and, in the course of that discussion, they told us about an issue of unsafe practice at an NHS hospital, we may decide that it is necessary to use that information in relation to the regulation of the NHS trust. In making this decision, we will follow the steps in section 3 of this Code.
- 5.9 However, if we have used our powers to obtain confidential personal information, and we subsequently propose to re-use that information for purposes that are not necessary to carry out our regulatory functions (other than in anonymised form), we will only do so with the person's consent. The exception would be when we are lawfully sharing information with other public authorities to enable them to carry out their own public functions (in which case, we will follow the principles set out in section 8 of this Code), or where the disclosure is required by law (for example, to comply with a court order).

6. Secure holding and handling of confidential personal information

- 6.1 We handle confidential personal information in accordance with the requirements of the Data Protection Act 1998, the Security Policy Framework and the Government 'Mandatory Minimum Measures' (www.cabinetoffice.gov.uk/resource-library/security-policy-framework).
- 6.2 Serious breaches of information security must be reported to the Department of Health and the Information Commissioner's Office, and will also be reported in our annual report (which is presented to Parliament and published each year).
- 6.3 We are also required to make an assessment as to whether we should notify anyone who is affected of any breach of security involving their personal information. Other than in exceptional circumstances, we will notify any person if we lose or inappropriately disclose their personal information.
- 6.4 Electronic information is held on secure systems. Portable media devices (such as laptops and hand-held IT devices) are encrypted and, where practicable, information is stored on secure servers, rather than the devices themselves.
- 6.5 Where confidential personal information is held on paper, it is stored in locked cabinets, or in other secure storage, and in premises where access is restricted.
- 6.6 We have a range of Information Assurance policies that staff must follow. If we find that a member of staff (or another person working for CQC) has deliberately and inappropriately accessed or misused confidential personal information, we will take action. This could include disciplinary action, ending a contract, or bringing a prosecution.
- 6.7 We assess ourselves against the NHS Connecting for Health Information Governance Toolkit to ensure that our policies and procedures meet appropriate standards (www.igt.connectingforhealth.nhs.uk/).
- 6.8 We will only share confidential information with other bodies – such as other regulators – where there is assurance that the information will be handled with an appropriate level of security.
- 6.9 Our Director of Intelligence is designated as the Care Quality Commission's Senior Information Risk Owner and has responsibility for ensuring that we understand and manage any risks relating to confidential personal information.

7. Retention and disposal of confidential personal information

- 7.1 We will ensure that we do not retain confidential personal information for longer than we need to.
- 7.2 In some cases, we will receive confidential personal information that is not needed to carry out our functions. In these circumstances, we will not retain this information beyond the point where we confirm that the information is not required.
- 7.3 Where we receive unsolicited confidential personal information from a registered service, an NHS body or a local authority, without good cause and in breach of the Data Protection Act or the common law duty of confidentiality, we may consider this as an indication of poor governance within that organisation when making our regulatory judgements. We will also assess whether it is appropriate to report the matter to the Information Commissioner's Office.
- 7.4 Where appropriate and practicable, we will offer to return confidential personal information once it is no longer required – for example, returning original documents sent by a person who uses registered services.
- 7.5 Where it is not appropriate to return the confidential personal information to its source, we will dispose of the information by deleting it securely from computer systems and portable media (such as computer disks and memory sticks) and by secure physical destruction of 'hard copy' documents (for example, shredding or pulping paper records).
- 7.6 We will hold and publish a Records Retention and Disposal Schedule, which will set out the types of records (including confidential personal information) that we hold, and will set time limits for their disposal.
- 7.7 It should be noted that records often need to be retained after the completion of the original 'primary' purpose for which they were created or obtained where there are legal, regulatory or compliance issues that require us to do so. For example, we would retain evidence used to take enforcement action against a registered provider beyond the completion of that action for 'secondary' purposes that may arise relating to possible complaints or legal challenges, or internal audit etc. These secondary uses of information are included in the retention limits that are set within the Retention and Disposal Schedule.

8. Disclosing, sharing or publishing confidential personal information

Sharing information with, or disclosing information to, other organisations

- 8.1 As the regulator of health and adult social care in England, we have a responsibility to protect and promote the rights of people who use health and social care, in particular, the rights of children and vulnerable adults. This will often mean cooperative or joint working with other public bodies, both in and outside of the health and social care sector.
- 8.2 Inevitably, working with other public bodies has implications for how confidential personal information is used, particularly, the circumstances under which it may be disclosed or shared. The Health and Social Care Act 2008 recognises the significance of information sharing to our regulatory functions and has provided us with express powers of disclosure.
- 8.3 We may exercise our statutory powers to disclose information in the following circumstances:
- When it is required by law or the order of a court.
 - When it is necessary or expedient to protect the welfare of any person (for example, safeguarding).
 - When it is necessary or expedient to enable another public body to carry out its statutory functions.
 - When it helps us to carry out any of our functions.
 - When it is in connection with the investigation of a criminal offence or criminal proceedings.
- 8.4 Other than where a disclosure is required by law or by order of a court, we will only make a disclosure where we consider that the balance of public interest favours disclosure of the information. In making this judgement, we will consider the potential impact on people's privacy (see section 3 of this Code for details of how we will make this judgement).
- 8.5 When sharing confidential personal information in this way, we will notify the people to whom that information relates, if it is possible and practicable to do so, and if doing so will not prejudice the purpose of that information sharing. For example, we may decide to share confidential personal information with the police, without notifying the person to whom the information relates, in circumstances where informing them would interfere with the police's ability to investigate criminal activity.

- 8.6 We will only share confidential personal information where it is lawful to do so, and where we are assured that the information will be handled securely and with appropriate confidentiality.
- 8.7 Where we regularly share information (including personal information) with other bodies, we will set up and publish written agreements with those bodies to govern why, how and when the sharing will take place – including ensuring that the method of transferring the information will be secure. These agreements (memoranda of understanding, joint working protocols and information sharing agreements) are available on our website at:
www.cqc.org.uk/aboutcqc/howwedoit/workinginpartnership/jointagreements.cfm.
- 8.8 We may also share confidential personal information with private or voluntary organisations who we have engaged to work on our behalf. For example, we may employ a private sector data management company to contact providers and check that our data about them is accurate, or may ask external organisations with special insight or first-hand experience of particular care-related issues to undertake work on our behalf. We will only do this where there is appropriate assurance (that meets government standards) that the data will be kept secure and will not be misused. We will only share the minimum amount of confidential personal data required for the purpose.
- 8.9 We will not pass confidential personal information to private organisations for the purpose of, or in circumstances where it could be used for, direct marketing.

Publishing information

- 8.10 We are required by law to publish some information, for example reports about inspections that we have performed and information about some decisions that we have made.
- 8.11 In other circumstances, we choose to publish information as a way of helping us to perform our functions. For example, we may publish information to explain a regulatory decision that we have taken, to help people to make informed choices about the care services that they use.
- 8.12 We will always be careful not to publish confidential personal information – particularly when the information relates to people who use services – but it will sometimes be necessary to do so in order to perform our statutory functions. For example, in exceptional circumstances, if a very small number of people use a service, we may include information in an inspection report that could identify them – if it is directly relevant to a judgement we have made, or action that we have taken, in relation to that service. (See section 3 of this Code for details of how we will make this judgement.)
- 8.13 Or we may consider it necessary to publish confidential personal information about the people that we register and whose services we regulate. For example, we may consider it necessary to publish information about a registered manager's conviction for a criminal offence, if this is fundamentally relevant to a judgement or decision that we make about them or their service – such as a decision to cancel registration, or to apply a condition of registration.

- 8.14 In such circumstances, we will notify the relevant people in advance, listen to – and give careful consideration to – any objections that they raise, and will take whatever steps we can to minimise the impact on their privacy.

Access to information

- 8.15 There is a public right of access to information held by CQC under the Freedom of Information Act 2000. This right of access is limited by a range of exemptions, some of which allow us to refuse to disclose confidential personal information.
- 8.16 People whose personal information we hold have a right to access this information under the Data Protection Act 1998. This allows them to check that the information we hold is accurate, and to know where we have obtained the information from.
- 8.17 Requests for information under the Freedom of Information Act 2000 or the Data Protection Act 1998 can be sent to information.access@cqc.org.uk or to the Information Governance Team, Care Quality Commission, Citygate, Gallowgate, Newcastle upon Tyne, NE1 4PA.

9. Governance of this Code

- 9.1 This Code establishes the principles by which the Care Quality Commission will obtain, use and dispose of confidential personal information. We will have (and publish) a range of more detailed policies and procedures – developed to comply with the principles of this Code – to cover various aspects of our practice. All of our staff will be trained in, and required to comply with, those policies and procedures. This compliance will be continuously monitored by line-management arrangements.
- 9.2 We will monitor and report on compliance with this Code of Practice through our Audit and Risk Committee.
- 9.3 Where we wish to obtain, use or disclose confidential personal information about people who use services in a way that we have not previously used, or for a new purpose (for example, if we were to introduce a new methodology or policy for obtaining and using personal information) we will first seek the approval of our Caldicott Guardian (a member of our board with responsibility for ensuring that the use of such information is justified, necessary, kept to a minimum, restricted to those with a 'need to know', and that all staff involved understand their responsibilities and comply with the law).
- 9.4 Any person who is concerned about how we use confidential personal information may contact the Information Governance Manager by email on information.access@cqc.org.uk, by phone on 03000 616161, or by post to Information Governance Manager, Care Quality Commission, Citygate, Gallowgate, Newcastle upon Tyne, NE1 4PA.
- 9.5 When responding to any concern, the Information Governance Manager will advise the person of any further right of appeal – for example, how to seek a judgement from the Information Commissioner's Office as to whether we have complied with the Data Protection Act.

10. Keeping this Code under review

- 10.1 In preparing this Code, we have consulted with people who use registered services, their families and carers, registered providers, the National Information Governance Board for Health & Social Care, and a range of other public bodies.
- 10.2 We welcome comments from all interested parties about the way we obtain, handle, use, or disclose confidential personal information. Comments should be directed to the Information Governance Manager at the address above.
- 10.3 We are required to keep this Code under review and we will revise it as appropriate, taking into account any comments, complaints and changes in the law about the way that we obtain, handle, use and disclose confidential personal information.
- 10.4 We will next review this Code no later than April 2013.

Appendix: The legal framework

We are subject to a range of legislation and legal rules that govern how we obtain, handle, use or disclose information.

Below is a brief overview of the main legislation in this area, with links to some of the key sections.

Health and Social Care Act 2008

The Health and Social Care Act gives us extensive powers to obtain, use and disclose information, documents and records (which would include confidential personal information). The Act also makes it a criminal offence if a person knowingly or recklessly discloses confidential personal information held by CQC during the lifetime of the person to whom the information relates, unless the disclosure is made in circumstances that the Act permits (referred to as 'defences').

Links on Legislation.gov.uk:

[Health and Social Care Act 2008](#)

[Our regulatory functions'](#) (Section 60)

[Powers of entry and inspection](#) and [powers to require documents and information](#) (Sections 62 and 64)

[Offence of 'disclosure of confidential personal information'](#) and [defences](#) (Sections 76 and 77)

[Permitted disclosures](#) (which will not be prohibited or restricted by common law) (Section 79)

Requirement to have a [code of practice on confidential personal information](#) (Section 80)

Mental Health Act 1983

One of our roles as a regulator is to keep the use of the Mental Health Act under review and check that it is being used properly. Our Mental Health Act Commissioners perform this work by visiting all places where patients are detained under the Mental Health Act, and meet with them in private.

We have powers to visit and examine detained patients in private, and to access records relating to their detention and treatment, or other information that we reasonably require.

We may also meet patients who are on a Community Treatment Order or under Guardianship, and we have a right to access such patients' records.

Links:

[Mental Health Act 1983](#)

The role of CQC as the 'regulatory authority' in England (included in Section 145).

Our powers to enter premises, visit and interview detained patients, and to require the provision of records (Section 120).

Health and Safety at Work Act 1974 and the Ionising Radiation (Medical Exposure) Regulations 2000

We have a role as an 'enforcing authority' to ensure that the medical use of ionising radiation is carried out in accordance with the 2000 regulations, to minimise the risk to patients and healthcare staff.

Ionising radiation is used in medical settings to diagnose – for example X-rays (including dental X-rays) and CT scans – and for therapeutic purposes – such as using radiation to treat disease.

Our staff have powers under Section 20 of the 1974 Act to, among other things, enter premises, take measurements or photographs, interview people, and to access and/or obtain records, documents and information.

Links on Legislation.gov.uk:

[Health and Safety at Work Act 1974](#)

[Powers of inspectors](#) (Section 20)

[Ionising Radiation \(Medical Exposure\) Regulations 2000](#)

We must not act beyond the powers conferred on us by the above pieces of legislation. We must exercise the powers only for the purpose of carrying out our functions or for purposes that are 'reasonably incidental' to those functions.

In exercising our powers, CQC must also comply with the following:

Human Rights Act 1998

The Human Rights Act implements the European Convention of Human Rights into UK law. The Act requires public authorities to give effect to the Convention rights when carrying out their statutory functions. Article 8 establishes a right to 'respect for private and family life', which includes the right of individuals to have their information kept private and confidential. Any action by a public authority that interferes with this right must be proportionate and necessary to support legitimate aims that are specified by the Act.

The most relevant grounds on which CQC may set aside an individual's right to privacy under the Act are where we consider it is necessary to do so to prevent disorder or crime, to protect health, or to protect the rights and freedoms of others.

Links on Legislation.gov.uk:

[Human Rights Act 1998](#)

[Right to respect for private and family life](#) (Article 8)

Data Protection Act 1998

The Data Protection Act regulates the processing of personal data. 'Personal data' is information that relates to, and is capable of identifying, living people (for example name, address, date of birth or reference numbers), and which is (or is intended to be) recorded in a structured manner on computers or paper files.

The term 'processing' covers a broad range of activities in relation to personal data, including obtaining, holding, using or disclosing.

Organisations must process personal data in accordance with eight data protection principles. For example, the first principle requires fair and lawful processing. The seventh principle requires data to be processed securely. The Act also gives rights to individuals to have a degree of control over how personal information relating to them is used – most notably, the right of access.

Links on Legislation.gov.uk:

[Data Protection Act 1998](#)

[Definitions of personal data and processing](#) (Section 1)

[Right of access to personal data](#) (Section 7)

[Right to prevent processing that is likely to cause damage or distress](#) (Section 10)

[Exemption to allow disclosure for the purposes of crime prevention or detection, or the apprehension and prosecution of offenders](#) (Section 29)

[Exemption to allow disclosures required by law or made in connection with legal proceedings](#) (Section 35)

[The Data Protection Principles](#) (Schedule 1)

[Conditions relevant to allow the processing of personal data](#) (Schedule 2)

[Conditions relevant to allow the processing of sensitive personal data](#) (Schedule 3)

Freedom of Information Act 2000

As a public authority, CQC is subject to the Freedom of Information Act. The Act is designed to encourage transparency and accountability in the public sector and seeks to

achieve this by allowing the public to access recorded information held by, or on behalf of, public authorities.

Much of the information we hold will be accessible under the Act. Our Publication Scheme, which is available on our website, is one method by which people can access information. The other is by making a written request to us. The Act provides a number of exemptions from disclosure, including where disclosure would breach the Data Protection Act or a reasonable expectation of confidentiality.

We have produced a guide explaining the information that we make available under our Publication Scheme. To see a copy, click the link below or write to the Information Governance Manager, Care Quality Commission, Citygate, Gallowgate, Newcastle upon Tyne, NE1 4PA.

www.cqc.org.uk/freedomofinformation.cfm

Links to the Act (on Legislation.gov.uk):

[Freedom of Information Act 2000](#)

[General right of access to information held by public authorities](#) (Section 1)

[Exemption from disclosure of personal information](#) (Section 40)

[Exemption from disclosure of information provided in confidence](#) (Section 41)

[Exemption from disclosure relating to obtaining information from confidential sources](#) (Section 30)

Environmental Information Regulations 2004

Access to information relating to, or affecting, the environment is handled under the Environmental Information Regulations. These aim to encourage public participation in environmental matters. The Regulations operate in a very similar way to the Freedom of Information Act – personal data and confidential information are given similar levels of protection.

Links on Legislation.gov.uk:

[Environmental Information Regulations 2004](#)

[Exemption from disclosure of personal data](#) (Regulation 13)

Access to Health Records Act 1990

The Access to Health Records Act 1990 has been largely superseded by the subject access provisions of the Data Protection Act 1998. However, the provisions relating to access to the health records of deceased people are still in force.

The Act allows a patient's personal representative, or any person who may have a claim arising out of the patient's death, to seek access to their health records.

This Act only applies to CQC when a health professional, acting in that capacity on our behalf, has made records relating to the health of an identifiable individual who has since died.

This would most likely occur through the work of the Second Opinion Appointed Doctor (SOAD) service, which we manage. We are responsible for reviewing the detention of people under the Mental Health Act who either refuse the treatment prescribed to them or are assessed as lacking the capacity to understand and therefore incapable of deciding whether to give or withhold consent. The role of the SOAD is to decide whether the treatment recommended is appropriate.

[Access to Health Records Act 1990](#)

[Definition of a health record](#) (Section 1)

[Right of access to health records](#) (Section 3) – Section 3(1)(f) relates to the records of deceased patients

National Health Service Act 2006

Section 251 of the National Health Service Act established a regulated legal process by which the common law duty of confidentiality may be set aside to allow confidential patient information to be used for medical purposes where consent is not practicable and it is not possible to use data that does not identify a person. The provision recognises the importance of patient information to the activities of the NHS and the problems that might arise if the use of patient information depends on the consent of relevant individuals.

The medical purposes specified in the Act include preventative medicine, medical research, and the management of health and social care services.

Applications for approval are administered by the [National Information Governance Board for Health and Social Care](#)'s Ethics and Confidentiality Committee, on behalf of the Secretary of State.

The Health and Social Care Act 2008 gives us specific powers to obtain and use information to carry out our regulatory functions. As a result, we are not usually required to obtain approval from the National Information Governance Board for Health & Social Care if we need to obtain, use or disclose patient information without consent in relation to these functions.

Where our powers are not enough to support the use of patient information without consent – because the use is not necessary to carry out a regulatory function – we will seek consent. If consent is not practicable, we will seek approval under the Section 251 process.

In accordance with the Health and Social Care Act 2008, we have consulted with the National Information Governance Board for Health and Social Care in the development of this Code of Practice.

Links on Legislation.gov.uk:

[National Health Service Act 2006](#)

[Control of patient information](#) (Section 251)

Public Interest Disclosure Act 1998

The Public Interest Disclosure Act protects the employment rights of staff (including trainees and temporary staff) who raise concerns about their place of work.

CQC is a body prescribed by the Act to receive complaints about the services that we regulate, in circumstances where the employee does not feel able to raise the matter directly with their employer.

The Act does not, in itself, convey any right of access to information or duty of confidentiality on CQC.

When we receive a disclosure under the Act – sometimes known as 'whistleblowing' – we assume that the person making the disclosure wishes to have their confidentiality maintained, unless they indicate or agree otherwise.

However, it may not always be possible for us to preserve that person's confidentiality if we act in the overall public interest (that is, take appropriate action to protect people who use services). The Act provides employment protection for whistleblowers in circumstances where their confidentiality cannot be preserved.

Link on Legislation.gov.uk:

[Public Interest Disclosure Act 1998](#)

Disability Discrimination Act 2005

The Disability Discrimination Act makes it unlawful for a public authority, such as CQC, to discriminate against a person with a disability in carrying out its functions.

The Act also places a general duty on public authorities to eliminate discrimination, promote equality of opportunity, and encourage participation in public life by people with disabilities.

Compliance with this Act may require our staff to make appropriate adjustments, or take additional steps, to ensure that people with disabilities are not disadvantaged in issues such as making decisions about how their confidential personal information may be used, or in making requests for information from CQC.

Link on Legislation.gov.uk:

[Prohibition against public authorities discriminating against a person with a disability](#) (Section 21B)

[General duty to eliminate discrimination and promote equality](#) (Section 49A)

Common law

This is the body of law developed by judges through decisions of courts and tribunals. It is built up over time and based on case law.

CQC must have regard to the common law duty of confidentiality – that information provided in confidence should not generally be disclosed to others without the consent of the individual.

Confidentiality can be overridden by legislation or where there is sufficient public interest to justify it. The public interest test involves making a balanced judgement that takes into account the strong public interest in maintaining trust in the confidentiality of services, the public interest in favour of disclosure, and the private interests of any individuals involved. The nature and extent of the disclosure will be a key factor in arriving at a balanced and proportionate judgement.

Recent case law indicates that the common law duty of confidentiality generally continues to apply after the death of a person. It is also important to bear in mind that clinical records often contain third party information relating to living people and they too are owed a duty of confidence.

© Care Quality Commission 2010

Published December 2010

This publication may be reproduced in whole or in part in any format or medium for non-commercial purposes, provided that it is reproduced accurately and not used in a derogatory manner or in a misleading context. The source should be acknowledged, by showing the publication title and © Care Quality Commission 2010.

How to contact us

Phone: 03000 616161

Email: enquiries@ccq.org.uk

Registered Office:
Care Quality Commission
Finsbury Tower
103–105 Bunhill Row
London EC1Y 8TG

Please contact us if you would like a summary of this document in another format or language.

