Code of practice on confidential personal information

September 2016

(reviewed and amended in May 2018 to reflect updates to legislation in 2018)

Contents

Introduction

Purpose of the Code of Practice

This Code establishes the practices that the Care Quality Commission (CQC) will follow to obtain, handle, use and disclose confidential personal information.

We intend this Code to be used in two main ways:

- **By our staff**, as a guide to help them make decisions about confidential personal information. All our staff are required to comply with this Code and receive guidance and training to help them in this.
- **By other interested parties**, such as people who use services, carers, the public, providers of health and social care, and other regulatory bodies, to understand how we use their confidential personal information. The Code will also reassure people when we are requesting information or using our powers to obtain information, and provide a point of reference against which our practice can be judged.

The Code provides clear and easy-to-follow guidance to support our staff in making lawful, ethical and appropriate decisions in relation to confidential personal information. It also tells the public how to access information that CQC holds. The appendix provides links to other, more detailed guidance on key issues. This supports this Code of practice, but is not part of it and we will update this list as appropriate.

What is confidential personal information?

The Health and Social Care Act 2008[a] is the law that created CQC in its current form. It defines confidential personal information as information that is:

"obtained by the Commission on terms or in circumstances requiring it to be held in confidence".

and that:

"relates to and identifies an individual".

This means that the information must say or reveal something private, personal and of meaning about someone, and that it must also reveal who that person is (either by itself, or when combined with other information that we hold). This information may relate to *any person* who has directly or indirectly come into contact with CQC.

a. Section 80(5).

Information that is already publicly or widely known, or that a reasonable person would not expect CQC to keep secret, is not confidential personal information.

Examples of confidential personal information:

- A person's medical or care records, or specific pieces of information about their physical or mental health, condition or treatments.
- Information about a care provider's social or family life.
- Details of a care worker's education, training and experience.
- Information about the sexuality, religious beliefs and racial or ethnic origin of a CQC employee.
- Information that would identify people who have shared information in confidence with us, including people who use the services we regulate, 'whistleblowers', and people we have interviewed in private during inspections.

Examples of information that is not confidential personal information:

- Information relating to a registered manager that we are required to publish on the register on CQC's website.[b]
- Information that does not identify an individual. For example, the number of registered nurses working in a hospital.
- Information about a CQC employee that they should reasonably expect to be available to the public; for example, information about salaries and pay grades that CQC is required to publish.

Of course other information that CQC uses, which doesn't relate to or identify an individual, may need to be handled with a degree of confidentiality. For example, commercially sensitive documents relating to procurement of services or CQC's market oversight function. Such information is not covered by this Code, but we publish an Information Security and Governance Policy that sets out how we protect all types of confidential information. A link to the current version of this policy is included in the appendix of this Code (page 30).

Why CQC needs to obtain and use confidential personal information

Access to confidential personal information plays an essential role in CQC's inspections and the wider regulation of health and social care services in England.

CQC reviews confidential personal information, including information from medical and care records, because at times it is a necessary way of helping us to understand the quality of people's care and to ensure that we achieve our purpose of making sure people receive safe, effective, compassionate, high-quality care, and encouraging services to improve.

b. Under section 38 of the Health and Social Care Act 2008.

For example, we may need to access confidential personal information to allow our inspectors to assess whether:

- providers of care are using care plans to ensure that people receive person-centred care that meets their clinical and personal needs, particularly older people and people with long-term conditions (such as diabetes or dementia), people with a learning disability, and other people who may be vulnerable because of their circumstances
- lessons have been learned from complaints and serious incidents to improve safety and care, and whether care providers have met their 'duty of candour' to explain and apologise for serious mistakes
- the rights of people who have been detained under the Mental Health Act are being respected and protected
- medication records are kept properly
- information has been shared properly (lawfully, effectively and appropriately) between care services
- people are properly involved in decisions about their care, they are asked to give their consent, and their decisions are respected
- safeguarding concerns are being appropriately acted on to ensure that people who may be vulnerable are being protected from abuse and harm.

We also obtain information in a number of other ways, outside of our inspections, to help us to monitor the quality of care, prioritise our work, and identify problems with services that may require us to take regulatory action. We do this in a number of ways, for example:

- We invite people who use services to share their experiences with us.
- We share information locally and nationally with other organisations involved in commissioning, providing and regulating care (for example, local authorities, NHS Improvement, and professional regulators).
- We receive data about the quality of care services from NHS Digital. This data does not usually directly identify individual people who use services, but some data is detailed enough that it may be possible to identify some people. We handle and use this data in accordance with strict agreements with NHS Digital, we ensure that it is kept secure, and we do not try to identify anyone from it.

Where possible, we will use anonymised information or information other than confidential personal information to carry out our work. But looking at, and using, confidential personal information is often the only practical way in which we can carry out our work effectively. For example, it may be difficult and time consuming for a care provider to make anonymised copies of any records we need to see as we request them during an inspection. In other cases, we may need to know whose records we are looking at because we are trying to understand how that person's needs have been met.

Parliament has granted CQC powers to obtain and use confidential personal information, including information in medical and care records, to enable us to carry out this work.

If CQC does not use these powers effectively and appropriately, we may fail in our role of identifying and taking action on poor care, or we may fail to identify and highlight good care.

Whenever we obtain, use, handle or disclose confidential personal information, we are required to comply with a range of legal obligations. In particular, we must ensure that we process personal data in accordance with the data protection laws[c], and that any interference with the privacy of any person is compliant with Article 8 of the Human Rights Act 1998. We must also ensure that we do not unlawfully breach, or require others to breach, the common law duty of confidence.

c. References throughout this Code to 'data protection laws' refer to the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), from 25 May 2018. Before that date, the Data Protection Act 1998 applied.

Our approach to confidential personal information

CQC must have a consistent and lawful approach to obtaining, using, disclosing and handling confidential personal information across all areas of our work.

Our staff also have a personal duty to protect confidentiality, and we must support them to meet this obligation.

To achieve this, we adopt the following practices to the decisions we make about confidential personal information.

PRACTICE 1: Obtaining confidential personal information

We only obtain confidential personal information where it is necessary to do so to enable us to perform our functions. We will obtain only the minimum necessary confidential personal information.

We apply the necessity test (see page 9) to make these decisions.

We have powers that allow us to obtain confidential personal information where it is *necessary* to assist us in performing our *regulatory functions* or other functions where we have legal powers to obtain confidential personal information.[d] These powers mean that we do not need to get a person's consent to obtain this information, but we will take reasonable steps to inform and consult with people when we intend to obtain their information; we will support providers to keep appropriate records so that people can find out if CQC has accessed their information, and we will ensure that our actions are proportionate and justifiable.

For more information, see page 13.

d. For example, our functions under the Mental Health Act 1983, to check that the rights of people detained under that Act are being observed.

PRACTICE 2: Using confidential personal information

As far as it is possible and practicable to do so, we will keep people informed about how, why and when we need to obtain, use and disclose their confidential personal information. We will also consider their views and concerns (and, where appropriate, the views of their families or other representatives) when making decisions relating to this information. We will try to minimise any risk of damage or distress that may be caused to people that the information relates to.

We will apply the necessity test (see page 9) to make these decisions.

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

Where we are considering a significant change in our methods, policies, processes or systems that may affect people's privacy, we will first carry out a Privacy Impact Assessment (PIA).

For more information, see page 20.

PRACTICE 3: Disclosing and sharing confidential personal information

We will only disclose or share confidential personal information where it is 'necessary' to do so to perform our regulatory functions or for another legitimate and lawful purpose. We will only do so where any harm that may be caused by disclosure is outweighed by the possible harm that we are aiming to prevent, or by the public benefit that we are seeking to achieve.

We will apply the necessity test (page 9) to make these decisions.

We will disclose or share anonymised information instead of confidential personal information, wherever it is practicably possible to do so.

We work in collaboration with other public bodies to encourage and facilitate information sharing in the public interest. We will govern these working relationships with formal agreements and take appropriate steps to ensure that any confidential personal information that we share is properly protected and appropriately, fairly and lawfully handled.

For more information, see page 22.

PRACTICE 4: Handling and protecting confidential personal information

In all cases, we will hold and use confidential personal information securely, sensitively and only for as long as necessary.

We will obtain, handle, use and disclose information relating to deceased people with respect to their privacy and dignity, with sensitivity to their families and friends, and with consideration of any previously recorded wishes of the deceased person.

For more information, see page 25.

When we developed this Code of Practice, we took into consideration the *Code of Practice on Confidential Information* from the Health and Social Care Information Centre (HSCIC) (now NHS Digital) and the Department of Health's *Confidentiality: NHS Code of Practice*. We consider that this Code of Practice is consistent with the practices set out in those documents.

We also consider that this Code of Practice is consistent with the *Caldicott Principles* and legal requirements including data protection laws and the Human Rights Act 1998.

We will review this Code of Practice regularly to ensure that we continue to comply, and keep up to date with the law, and to consider the changing public interest, ethics and best practice regarding confidential personal information. If we consider it necessary to revise this Code, we will consult widely before doing so.

We also publish a range of other information that explains how we obtain, use, disclose and handle confidential personal information. This includes the specific guidance and information that is available on our website, as well as printed information leaflets for the public (see the appendix on page 30).

The ‘necessity test’

The necessity test is the foundation that CQC uses to make all decisions about whether we should obtain, use or disclose confidential personal information. This applies whether or not consent is required.

Using this test helps us to make sure that CQC is acting fairly and lawfully by establishing need, assessing competing interests and considering any potential for damage, loss or distress. It enables us to recognise and balance the implications of our actions against the potential harm that may be caused if we do not act.

CQC staff use this test frequently, and it will help others to understand how we are likely to use their information.

The test has two simple stages:

FIRSTLY

We consider whether obtaining, using or disclosing the information is a **necessary step** for us to perform one of the jobs we are required to do by law (CQC’s functions), or whether it is a necessary step for another legitimate aim.

‘Legitimate aims’ are lawful, reasonable and appropriate objectives or outcomes that we are justified in wanting to achieve.

To be ‘lawful’, our aim must be in accordance with the Principles – and meet appropriate lawful bases for processing personal data – under data protection laws, and must be for the purpose of the protection of health, protecting the rights and freedoms of others, or another purpose consistent with Article 8 of the Human Rights Act 1998.

Examples of legitimate aims include: protecting the safety and welfare of people who use services, or assisting other public authorities to perform their own functions.

When deciding whether obtaining, using or disclosing confidential personal information is a ‘necessary step’, we will consider whether it would be reasonably possible or practicable to achieve the intended outcome without using confidential personal information.

As a public body, we must also perform our functions in an effective and efficient way. We may consider it a ‘necessary step’ to obtain, use or disclose confidential personal information where we could achieve the same outcome in other ways, but where doing so would require very significant and disproportionate effort. This is because it is in the public interest to achieve an efficient use of our resources. The second part of the test assesses the public interest in more detail.

SECONDLY

Only where we have established that obtaining, using or disclosing the confidential personal information is a necessary step (see above), we will then consider whether it is necessary **in the overall public interest** in each particular circumstance.

This means that we will consider whether the public interest served by achieving that aim justifies any potential impact on a person's privacy or other rights and interests.

In effect, we are asking ourselves whether our proposed actions are **proportionate and reasonable**. This may require us to carefully consider and balance a range of different issues, which include:

- any objections, concerns, opinions and expectations expressed by the individuals (or their family, carer or representative)
- the sensitivity of the information, and the potential damage that could be caused by using or disclosing it
- the impact on a person's privacy and interests
- the general public interest in maintaining trust in the confidentiality of health and social care services and the work of CQC
- the public interest to be served by CQC pursuing the function or legitimate aim; in particular, we should consider the extent to which our actions will protect the health, wellbeing, and legitimate rights and interests of others
- the effective and efficient use of public resources.

When we use the necessity test it is essential that we are as well-informed as possible about the wishes of the person to whom the information relates, and any potential harm (such as loss of privacy or dignity) that our actions may cause them. Where it is possible to do so, without interfering with our ability to perform our functions, our staff will ask those people for their views and consider these.

In some circumstances, it would require a significant and disproportionate effort to notify people about our access and use of confidential personal information. Doing so in some circumstances may also increase the risk to privacy, or may prevent us from performing our role, or may otherwise cause harm.

For example, we would normally notify and consult with the people whose confidential personal information we are accessing and using if they are present at the service at the time of our inspection and relatively easy to identify and contact, or if we were considering them as a 'case study' and therefore accessing their information repeatedly over a length of time.

On the other hand, if we were reviewing a medication log containing the names of many people, or were checking a selection of records to identify whether a single marker had been added, we would probably consider it disproportionate to obtain the names and contact details of all of those people and write to them individually.

We provide detailed guidance and training to help and support CQC staff to be confident when making decisions using the necessity test. In some situations, there will be a clear and obvious decision, whereas in others the necessity test may produce a finely balanced outcome where it isn't clear if the action is justified.

We support our staff in these circumstances with specialist advice to better protect the rights of individuals whose information we want to use. This advice comes from our 'Caldicott Guardian' (a senior manager with responsibility for ensuring that any information about people who use registered services is obtained, handled, used and shared appropriately) and specialist advisors with appropriate expertise.

Any CQC employee or agent making a decision to obtain, use, or disclose confidential personal information must be able to explain and justify that decision, if challenged to do so.

Mental capacity considerations

CQC must comply with all the requirements of the Mental Capacity Act 2005.

Our powers allow us to access records containing confidential personal information without consent, regardless of the person's capacity, to enable us to perform our regulatory functions.

In circumstances where our powers do not apply and where the person does not have capacity to consent, we will only proceed where an appropriate assessment of the person's best interests has been made. We will consult professionals and those close to the person where appropriate to establish competence and to assess their best interests. We will proceed in accordance with these best interests in a way that minimises the impact on the privacy, rights and freedoms of that person.

Specifically in relation to the guidance in this Code, we will assume that any person has capacity to consent to CQC obtaining, using or sharing their information, unless it is established that this is not the case.

Where a person is not capable of giving their consent, and where no-one is empowered to make decisions on their behalf (for example, under a power of attorney, or guardianship of the court), we will only obtain, use or share their confidential personal information where there is another legal basis for doing so.

Children and young people

When we are asking for or receiving information from a child, or using consent as a basis for using their information, we will consider whether the child clearly understands what is involved and is capable of making an informed decision. We will consult professionals and parents where appropriate to establish the child's competence.

Other than in exceptional circumstances[e], when we use information about children and young people who do not have capacity to consent, we will involve their parent or guardian when making our decision, where it is possible to do so. Where a child is not capable of giving their consent, and where our powers do not permit us to access or use information without consent, we will need to obtain the consent of a parent or someone with parental responsibility.

If we share any information about a child with their parent or guardian, we must comply with this Code. For example, where a child is capable of consent, we would not normally disclose their confidential personal information with a parent without their consent.

Information about children and young people is particularly sensitive and we will treat it with appropriate care.

e. For example, there may be information that a child legitimately wishes to be kept from their parent or guardian (or even where disclosure could place that child at risk), such as information about sexuality or religious beliefs.

PRACTICE 1: Obtaining confidential personal information

Obtaining information by using our powers

To enable CQC to perform certain 'regulatory functions' Parliament gave us specific powers to enter and inspect care services and to obtain information. We also have powers to require the services that we regulate to send information that we need to us.

Once we have considered the necessity test (see page 9) to assess whether it is necessary and proportionate for us to access confidential personal information, it is more preferable to obtain information by using these powers. This is because it provides the clearest legal basis for obtaining the information we need and gives the holder of the records a clear legal basis to disclose it to us.

However, we will also consider whether there are more appropriate ways to obtain the information we need, for example, by accessing information that is already collected by NHS Digital, and therefore minimising the burden to care providers.

Purposes for which we can use our powers

We can use our powers for **regulatory functions** that are in the Health and Social Care Act 2008.[f] These functions include:

- the registration of care service providers and managers
- assessing their compliance with regulations, and taking action (including formal enforcement and legal action) when those regulations are not being met[g]
- carrying out reviews and investigations of health and adult social care services and publishing reports of our findings
- studying the economy, efficiency and effectiveness with which NHS bodies and local authorities (councils) commission, manage and provide health and adult social care services, and publishing the results of these studies
- carrying out and publishing some types of special reviews and studies that look at important themes and issues in health and social care
- monitoring and reporting on the handling of information by the care services that we register and regulate.

f. Section 60(2) – The 2008 Act has been amended by the Health and Social Care Act 2012, and other legislation and regulations, to give CQC some of the functions listed here.

g. Including monitoring the 'duty of candour' and 'fit and proper person' requirements on providers.

We also have some functions under other acts of Parliament with associated powers that allow us to obtain and use information, including confidential personal information. These include:

- Our role of monitoring the use of the Mental Health Act 1983[h] and ensuring that it is being properly used (in particular, how providers use powers of detention and treat people without consent under that Act).
- Acting as an 'enforcing authority' under the Health and Safety at Work Act in relation to the Ionising Radiation (Medical Exposure) Regulations 2017 (IR(ME)R17). Our role is to ensure that the medical use of ionising radiation is carried out in accordance with the regulations to minimise the risk to patients.
- Our responsibility for deciding whether we need to take regulatory action in response to reported health and safety incidents that involve people who use health and adult social care services that are regulated by CQC.

We provide detailed guidance for our staff on using our powers to obtain health and care records. Only people who have been specifically authorised by CQC are allowed to use these powers to access confidential personal information.

Consent when CQC is using its powers

Where we have decided that it is necessary to use our powers to obtain confidential personal information for the above purposes, **we do not need to seek consent to do so**.[i]

However, we will inform people that we intend to obtain or use their confidential personal information (including advising them why we need to do so, how we intend to use that information, and who – if anyone – we intend to share it with) and listen to their views, unless it would require a significant and disproportionate effort to do so.

Where someone does raise objections or concerns about us accessing their confidential personal information, we will take these into account as part of the necessity test. People may tell us directly that they do not want us to use their information in this way, or they may have informed their care provider of their wishes.

We will only access confidential personal information against the expressed wishes of people who use care services in exceptional circumstances. Where we do have to do this, we will inform that person of our reasons for going against their wishes.

When assessing whether it is practical and possible to inform people of our intentions, we will take into account all the relevant circumstances. These will include, but not be limited to:

h. Section 120 of the Mental Health Act 1983.

i. Obtaining information that is necessary to perform our statutory functions engages the lawful basis for processing personal data under paragraph 1(e) of Article 6 of the General Data Protection Regulation (GDPR). It also engages the lawful bases under paragraphs 2(h) and (i) of Article 9 of the GDPR, allowing us to process 'special category' personal data such as health information.

- whether it is possible and reasonably practical to identify and contact those people in light of the resources available to CQC
- whether consultation in itself is likely to cause disproportionate or unwarranted distress or harm to any person; **in exceptional cases** consulting a person about obtaining information may cause serious harm
- whether consultation is likely to prejudice how we perform our regulatory functions, or how we carry out some other investigation or enforcement action.

The greater the sensitivity of the information, or the potential to impact on privacy, the greater the effort we will make to inform people and consult with them about obtaining and using their confidential personal information. Where we cannot consult with people in advance, we will also consider whether it is practical and proportionate to notify them later that we have accessed their confidential personal information. Where we access medical or care records, we will support providers to meet their responsibility to ensure that they maintain a proper note of this in, or with, that record, so that anyone can find out if CQC has looked at their records.

Example 1

During an inspection of a hospital, we decide that we need to check whether medicines records are being kept properly.

In the absence of other evidence, the inspector considers that it is necessary to check medicines records against the individual medical records for a sample of 10 patients. We will only be looking at a small amount of specific information from each medical record and, unless we find serious problems, we will not be taking copies of the records or making copies of information from them.

Locating each patient within the hospital, or obtaining their contact details and writing to them in advance, would significantly delay the checks and therefore the whole inspection. The inspector assesses that it is necessary and proportionate to view the records – the likely impact is low, and the public interest in conducting these checks is high. The inspector makes a note of this decision (and the reasons for it) and proceeds with the review. Hospital staff enter a note on each medical record to show that it has been accessed by CQC.

Example 2

During an inspection of a care home, a CQC inspector speaks to Mary, a resident of the home. Mary says things that cause the inspector to be concerned about whether the service is managing her diabetes properly.

The inspector tells Mary that he is concerned and would like to review her care plan so that he can look into this further.

Mary has some concerns about her privacy, which the inspector discusses with her. He explains his responsibility to maintain confidentiality and why he thinks it is important to look at the records. He explains that he will only look at the parts of Mary's care plan that relate to the management of her diabetes. Mary is reassured by this.

The inspector decides that there is a strong public interest in making sure that the care home manages people's diabetes care properly, and that checking the records for this purpose is proportionate. He tells Mary that he will do this.

Example 3

During an inspection of a GP practice, we decide that we need to check whether people diagnosed with dementia are being properly referred by the practice, and whether their long-term care is being appropriately monitored. The inspector considers reviewing a sample of medical records to investigate this.

The practice has recently been involved in a local audit of these issues and the inspector decides that there is already enough evidence available in the audit report to assess this issue and so it is not necessary to look at people's records.

Providers of care have their own legal responsibility to inform people who use their services, their staff and others about how their confidential personal information may be accessed and used. They should therefore tell people that CQC may look at the records they hold, and should keep a record for their own use of which records we have asked to look at during an inspection.

We also publish information in printed leaflets and on our website that explains in general how we obtain, use and share confidential personal information.

To help support NHS colleagues to meet the requirements of the NHS constitution[j], and to help all providers meet their own legal responsibilities, we will inform providers of the legal basis and reasoning as to why we require access to or information from medical records.

Where we use our powers to access or obtain confidential personal information, people who provide registered services and their staff are obliged to comply, unless they have a 'reasonable excuse' not to.[k] This provides a lawful 'gateway' allowing them to disclose this information to CQC.[l]

Obtaining confidential personal information by other means

There may be circumstances where we consider it necessary to obtain confidential personal information to perform our regulatory functions, but where our statutory powers to require the information do not apply. For example, where we want information held by the police that we consider is relevant to a provider's compliance with regulations.

Where we have determined that this is necessary (using the necessity test on page 9), we can request that information. We will rely on the holder of that information to voluntarily provide it to us. They will be responsible for establishing whether they have consent, or another legal basis, that will allow them to disclose the information to us.

We have formal agreements with key organisations that we work alongside, such as memoranda of understanding, joint working agreements and information sharing agreements, about how we will share and handle information.

When we are seeking information from an organisation but we have no standing agreements in place, we will make a formal request to explain why we think the disclosure of information to CQC is lawful, and in particular how it complies with data protection laws and any other relevant legislation.

In all cases, we will need to establish a lawful basis to obtain confidential personal information.

j. The NHS Constitution states: "You have the right *to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.*"

k. Under sections 63(7) and 64(4) of the Health and Social Care Act 2008.

l. In these, or other circumstances, other lawful gateways may permit disclosure – for example, consent or disclosures made to prevent serious harm.

Lawful basis to obtain confidential personal information where our statutory powers do not apply

Consent

Where we are not using our powers, we will consider whether it is possible and appropriate to ask people for their consent to obtain their confidential personal information.

Consent requires that a person is properly informed as to why their information is being obtained and how it will be used, and for them to positively and freely agree to this.

Failure to object or refuse is not consent. There must be some positive sign of agreement, although this does not necessarily have to be written.

Consent must not be obtained under duress. A person's consent is not valid if they give it because they feel they have no choice, or believe they will be seriously disadvantaged if they refuse.

Consent may also be withdrawn at any time.

Where we are relying on consent, but that consent is withdrawn before we obtain the information, we will not then obtain that information.

If consent is withdrawn after we have obtained the information, CQC will consider whether there is another legal basis to allow us to continue using the information. We will also consider whether it is fair to do so. If not, then we will securely dispose of that information.

Other lawful basis to obtain confidential personal information
In some cases, we may be able to obtain confidential personal information without using our powers and without the need for consent.

For example, if we are performing one of our functions (other than a regulatory function) we may be able to gather confidential personal information where we have formal approval from the Secretary of State for Health to do so. This approval can be granted under section 251 of the National Health Service Act 2006, following an application made to the Health Research Authority. An example of this would be where CQC conducts a survey of people receiving NHS care so that we can report on their experiences, and wishes to obtain contact details for this purpose.

Also, there will be a lawful basis to obtain confidential personal information where it is necessary for the administration of justice or other legal proceedings, or to enable us to protect people from very serious harm, or (for information about our own staff) where we need to fulfil our obligations as an employer. As noted above, we will consider whether using confidential personal information is necessary and proportionate for these purposes before we request it.

Record of CQC's access to health and care records

CQC will work with registered providers to ensure that when we access people's health and social care records, we do it in a way that supports the provider's own legal and governance requirements to maintain an audit trail of access to these records. This will ensure that people who use services will always be able to find out, through their care provider, whether or not CQC has accessed their records.

See the appendix (page 30) for links to CQC's guidance on obtaining confidential personal information, in particular, guidance on the use of our powers to access medical and care records during inspection.

PRACTICE 2: Using confidential personal information

How CQC uses confidential personal information

Most of the data and information that we collect, hold and use is not confidential personal information.

We use other types of information such as statistical information, anonymised records, audit findings and corporate records to monitor and understand the quality of care, and to take action where care providers are not meeting fundamental standards of care required in the regulations.

However, confidential personal information does play an important role in CQC's inspections and the wider regulation of health and adult social care services. At times, we need it to help us understand the quality of people's care and to achieve our purpose of making sure that people receive safe, effective, compassionate, high-quality care, and encouraging services to improve.

We sometimes need to use confidential personal information when using our enforcement powers and when taking action to protect people who use services – for example, using relevant information from people's care records as evidence in court when prosecuting a provider.

We also need to use confidential personal information when performing our roles of protecting the rights of people detained under the Mental Health Act, investigating incidents involving medical radiation, and carrying out in-depth investigations to look at care across the system.

We publish detailed guidance about how we inspect and enforce the regulations, and about the information that we routinely collect and use to monitor services.

If we are considering a change to our processes that may affect how we collect and use confidential personal information, we will conduct a Data Protection Impact Assessment (DPIA) to help us understand and minimise the potential consequences of the change on people's privacy, and to ensure that we identify and manage any risks.

If we collect information when carrying out one of our functions, the law allows us to use it to help us to perform any of our other functions.[m] For example, while checking whether a service is respecting the rights of a person detained under the Mental Health Act, we might find evidence that the service is not meeting the nutritional needs of detained people. We could use this evidence to support the use of our powers under the Health and Social Care Act 2008.

m. Section 78 of the Health and Social Care Act 2008.

However, we will not use confidential personal information for any purpose that is clearly incompatible with the original purpose for which we first obtained it, or in ways that would be unfair to the people whose information it is. For example, if we had obtained the names and addresses of people using a domiciliary care service (receiving personal care in their own homes) so that we could ask them about that care, we would **not** use this information to send them newsletters or contact them in a survey for their views on other matters, unless they had consented to this.

We can only use confidential personal information in ways that are lawful under data protection laws and other relevant legislation.

We are aware of the sensitivity of the information that we hold, particularly where we need to use information about people's health and the care and treatment they receive. We treat this information with respect and care, and we only collect and use it where it is lawful, necessary and proportionate to do so. We use the necessity test (see page 9) to make these decisions.

See the appendix (page 30) for links to CQC's guidance on using confidential personal information.

PRACTICE 3: Disclosure of confidential personal information

How CQC discloses confidential personal information

It is a criminal offence[n] to disclose confidential personal information that CQC has obtained unless it is in circumstances, or for purposes, listed as 'defences' under the Health and Social Care Act 2008.[o]

CQC can lawfully disclose confidential personal information where we can prove that one of the following circumstances applied at the time, or that we reasonably believed that they applied.

- the information had been anonymised
- the disclosure was made with the consent of the individual
- the disclosed information had previously, and lawfully, been disclosed to the public
- the disclosure was made in a way allowed by regulations relating to complaints about health or social care services[p]
- the disclosure was required or permitted by any enactment (Act of Parliament or regulations) or court order
- the disclosure was necessary or very helpful in protecting the welfare of any individual (for example, to protect people from the risk of neglect or abuse)
- the disclosure was made to another person or organisation because it was necessary or useful for them to have it in order to perform their own legal functions under enactment (in summary, to help another public body carry out its own role)
- the disclosure was made in connection with the investigation of a criminal offence
- the disclosure was made in order to enable CQC to perform our own functions.

Where one of the 'defences' listed above is met, and where the disclosure is necessary to enable CQC to perform its regulatory functions, or to enable another statutory organisation to perform its functions, or otherwise to protect and promote the welfare and safety of people using services (as assessed using the necessity test), it is also likely to meet a lawful basis for processing in accordance with data protection laws. These disclosures will not be prohibited or restricted by the common law duty of confidentiality.[q] However, there may be other legal restrictions on disclosure that we will be mindful of.[r]

n. Under section 76 of the Health and Social Care Act 2008.

o. Section 77.

p. Regulations under section 113 or 114 of the Health and Social Care (Community Health and Standards) Act 2003 (c.43)(complaints about health and social care services).

q. Under section 79(4) of the Health and Social Care Act 2008.

r. For example, there are some restrictions on disclosure of 'protected information' under the Gender Recognition Act 2004.

When making decisions to disclose confidential personal information, we will always consider the sensitivity of that information and the duty that we have to maintain confidentiality and protect people's privacy. For example, we would only disclose confidential personal information from someone's medical records to the police if we were satisfied that this was necessary to enable them to investigate or prosecute offenders of the most serious crimes.

Where a person has expressed a wish that their information should not be shared, or should not be used for purposes other than their direct care, we will respect those wishes unless there are exceptional circumstances.

In most cases, the information that we publish, share or disclose will not be confidential personal information. Usually, we share information about our actions and judgements and the quality of services, rather than private information about individual people. We provide guidance for our staff about anonymising information to make it easier and safer to use and share.

How CQC publishes information

We are required by law to publish some information, for example reports about inspections that we have carried out, and information about some decisions that we have made.

We also choose to publish information as a way of helping us to perform our regulatory functions. For example, we may publish information to explain a regulatory decision that we have taken, or to help people to make informed choices about the care services that they use.

We will always be careful to avoid publishing confidential personal information – particularly when the information relates to people who use services – and we follow guidance on how to anonymise information, but it will sometimes be necessary to do so in order to perform our regulatory functions. If this is the case, we will take all practicable steps to minimise the impact on privacy. This will include taking reasonable steps to ensure that people are aware of any likely disclosure of their confidential personal information and taking steps to address their concerns as part of the necessity test.

Example

We inspect a service that provides periods of respite care. Only two people use the service and have done so for short periods over several years. We judge that the service is not meeting its duty to provide person-centred care because it does not meet the complex nutritional needs of people using the service, and we are required to publish this in our report. Although they would not be named or directly identified in the report, someone who knows the people who use that service would be able to infer that at least one of them has complex nutritional needs.

How CQC shares information

CQC has a responsibility to protect and promote the rights of people who use health and social care. This will often mean cooperative or joint working with other public bodies, both in and outside of the health and social care sector.

Failing to share information between regulators and other partner organisations creates significant risks and inefficiencies. Reviews of previous failures in systems, including the Mid Staffordshire NHS Foundation Trust Public Inquiry, have highlighted these issues and resulted in recommendations to improve the sharing of information between CQC and others.

We use the necessity test (see page 9) to ensure that we share information appropriately, where this is in the public interest. We will only make a disclosure where we consider that the balance of public interest favours disclosing the information, having taken account of the likely impact on privacy.

When sharing confidential personal information, we will notify the people that it relates to if it is possible and practicable to do so, and if doing so will not prejudice the purpose of sharing that information. For example, we may decide to share confidential personal information with the police without notifying the person that it relates to, if informing them would interfere with the police's ability to investigate alleged criminal activity of a very serious nature.

We may also share confidential personal information with private or voluntary organisations that we have contracted 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 information will be kept secure and will not be misused. We will only share the minimum amount of confidential personal data that is needed for the purpose.

We will not pass confidential personal information to private organisations for direct marketing or other commercial uses that are not directly related to the delivery of care, or in circumstances where it could be used in that way.

We provide guidance and training for our staff on making decisions to share confidential personal information, and on how to effectively anonymise information.

See the appendix (page 30) for links to CQC's guidance on how we disclose confidential personal information.

PRACTICE 4: Securely handling confidential personal information

How CQC keeps confidential personal information secure

CQC recognises that it is vital to ensure that confidential personal information is appropriately and safely handled. We achieve this in the following ways:

- We ensure that CQC holds all confidential personal information securely. We publish a policy setting out the security standards that we apply and how we meet those standards.
- We have a Senior Information Risk Owner (SIRO) and Caldicott Guardian, both of whom are members of our Board. The SIRO provides assurance to the Board that risks to information are properly understood and managed. The Caldicott Guardian provides 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.
- We also have a Data Protection Officer (DPO) whose role is to monitor and advise on our compliance with data protection laws. The DPO and their team are involved in all data protection matters within CQC and they are able to report directly to the Board and our senior leaders. Contact details for the DPO are published on our website and they can also be contacted through the Information Access Team (see page 28 for contact details).
- We establish standards for all the information that we hold, with an understanding of the sensitivity and value of each 'information asset', and with clearly assigned responsibilities for managing and assuring those assets. Where we obtain and handle information that is subject to external standards (for example, data that we receive from the Health and Social Care Information Centre), we ensure that this data is handled in accordance with those standards.
- We have appropriate systems and processes in place to manage and process this information, and to ensure that access to the information is controlled and monitored. We assess these systems and processes against the Information Governance Toolkit and other external standards, and test them regularly.
- Confidential personal information is only handled by trained staff who need access as part of their roles.
- We analyse the information that we hold to ensure that we can understand and use it as effectively as possible. Wherever it is practicable to do so, we extract anonymised statistical information, which can be used and shared more freely than confidential personal information.

- We have processes in place to identify, manage and report any incident involving confidential personal information – including incidents involving the loss of, or unauthorised access to this information or 'near misses'. Under these processes, we will notify people if there has been such an incident involving their information.[s]
- We dispose of confidential personal information securely once it is no longer needed. We publish a 'retention schedule', which shows how long we keep different kinds of information.
- When we no longer need to keep information, including confidential personal information, in electronic files, we dispose of it by deleting it from our system. When equipment, disks and other storage media that has held this information is no longer in use, we ensure that these media are destroyed or that the data is securely over-written so that it is not possible for it to be retrieved.
- We only hold confidential personal information on 'portable media' (such as laptop computers or USB memory sticks) that are securely encrypted.
- Where we ask others to handle information on our behalf, we ensure that they meet these same standards.

See the appendix (page 30) for links to our guidance.

s. Other than in exceptional circumstances, such as where we have reason to believe that notifying the person may cause them serious harm.

Healthwatch England

CQC hosts Healthwatch England, which is a committee of CQC.[t] Healthwatch England acts independently, working with a network of local Healthwatch organisations to make sure that the overall views and experiences of people who use health and social care services are heard and taken seriously at a local and national level.

Although the practices set out in this Code apply to Healthwatch England, our responsibilities in relation to Healthwatch England are not 'regulatory functions', so we don't have powers to enter or inspect, or to obtain information for the work of Healthwatch.

Local Healthwatch organisations do have some powers of their own, but are not part of CQC. Local Healthwatch organisations have their own responsibility to obtain, use, hold and share personal data lawfully and appropriately.

Healthwatch England will usually rely on getting consent to obtain, handle, use or disclose the confidential personal information of people who use health and social care services. But in exceptional circumstances, where there is another lawful basis to do so – for example, disclosing information to protect a person from very serious harm if their circumstances make them vulnerable – they do not need consent.

Freedom to Speak Up – National Guardian

CQC also hosts the National 'Freedom to Speak Up' Guardian.

The National Guardian has been created as a result of recommendations from Sir Robert Francis's Freedom to Speak Up review, which looked at how systems and culture could be changed to better support staff who raise concerns about the services where they work ('whistleblowers').

The independent role will provide high profile national leadership to a network of Freedom to Speak Up Guardians across NHS trusts. These guardians are another important way of creating a culture of openness across the NHS but they will not be part of CQC.

The role of the National Guardian is not a 'regulatory function' of CQC, so the National Guardian will not be able to use CQC's powers to access and obtain confidential personal information. The Office of the National Guardian will be subject to the same legal requirements in relation to confidential personal information as CQC.

t. Under section 181 of the Health and Social Care Act 2012.

How to access information about you that CQC holds

If you want to request information about yourself that you think CQC might hold, you can send an email to information.access@cqc.org.uk or write to us:

Information Access Team
Care Quality Commission
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4PA

We will respond to your request under data protection laws. If an organisation such as CQC holds information about you, data protection laws give you a right to have copies of that information.

To protect your privacy, we need to have proof of your identity before we will disclose your personal data to you. When making a request, please send us **copies** of at least one item of identification that includes a photograph or signature (for example, your passport or driving licence), and another other item that includes your name and current address (for example, a utility bill, council tax bill, or a letter from your council or another government agency).

Please do not send original documents. We will either securely destroy any copies of identification that you send, or will return them to you if you ask us to do so.

Once we have received the request and proof of identification, we are usually required to respond within one month. We will let you know if a response will take longer than this.

We welcome comments from all interested parties about the way we obtain, handle, use, or disclose confidential personal information. Please send your comments to the Information Rights Manager at the postal or email address above.

How to object to CQC accessing or using your information

If you use a service that CQC registers and inspects, and if you do not want CQC (or others) to access information about you, you should discuss this with your care provider. They can put a note on your records so that we will know about your wishes.

As explained in this Code, other than in very rare and exceptional circumstances, we will respect your wishes where we know about them.

If you want to complain about how CQC has obtained, used, handled or shared your own confidential personal information, you can find details of how to do so on our website at www.cqc.org.uk.

Appendix: Further guidance on confidential personal information

Guidance from CQC

CQC guidance on obtaining confidential personal information:

Guidance on accessing medical and care records using powers under the Health and Social Care Act 2008

Confidentiality: Key Messages for Inspection

How we inspect and regulate

Protecting your privacy when using your information

CQC guidance on using confidential personal information:

How we use information

Privacy Impact Assessment process

CQC guidance on sharing, disclosing and publishing confidential personal information:

Guidance on sharing information

Anonymisation Guidance

Memoranda of Understanding and Joint Working Agreements with other organisations

CQC guidance on secure handling of confidential personal information:

Information Security and Governance Policies

Information classification and protective marking scheme

Retention and disposal schedule

Information security: Quick guide

External guidance on confidential personal information

Department of Health

Confidentiality: NHS Code of Practice

To share or not to share: The Information Governance Review

National Data Guardian

Review of Data Security, Consent and Opt-outs

NHS Digital (formerly the Health and Social Care Information Centre)

Code of Practice on Confidential Information

A Guide to Confidentiality in Health and Social Care

The Information Governance Toolkit

The Caldicott Guardian Manual

Information Commissioner's Office (ICO)

Guide to Data Protection

General Medical Council

Confidentiality

Ministry of Justice

A Guide to the Human Rights Act 1998

Other relevant guidance

Mental Capacity Act Code of Practice

For general enquiries:

Call us on: **03000 616161**

Email us at: **enquiries@cqc.org.uk**

Look at our website: **www.cqc.org.uk**

Write to us at: **Care Quality Commission**
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4PA

Follow us on Twitter: @CareQualityComm