Using surveillance

Information for providers of health and social care on using surveillance to monitor services

December 2014

Contents

Introduction

This information is for providers of health and adult social care services who may be considering the use of surveillance, such as CCTV cameras. It sets out some of the key points you need to consider and signposts you to guidance and sources of support.

The decision whether to use surveillance is for care providers to make in consultation with the people who use their services, and with families, carers, trade unions and staff. **This document does not give guidance on whether or not you should use surveillance systems, and CQC does not require providers to do so.**

The legal framework requires that any use of surveillance in care services must be lawful, fair and proportionate – and used for purposes that support the delivery of safe, effective, compassionate and high-quality care. Providers who already use surveillance should consider whether it was implemented, and is being used, with proper consideration of the issues raised in this document. If not, you should consider making changes to your surveillance methods.

We recognise that providers may find significant benefits in using surveillance and our inspectors will consider this in our assessment of the service. In some cases, covert surveillance (such as hidden cameras or audio recording equipment) or overt surveillance (such as visible CCTV cameras) may be the best or only way to ensure safety or quality of care.

However, there are other, less intrusive steps a provider can take to ensure that care is high quality and safe. These include:

- Always having enough capable and confident staff on duty with the right mix of skills.
- Encouraging an open culture, where both staff and people who use services are able to raise any concerns, and ensuring that those concerns are addressed.
- Ensuring supervision and appraisal are used to develop and motivate staff and, where required, review their practice or behaviour.

We would be concerned by an over-reliance on surveillance to deliver key elements of care, and it can never be a substitute for trained and well supported staff.

Providers considering the use of surveillance, particularly covert surveillance, should bear in mind the potential impact on the bond of trust with people who use their service and the possible impact on the employer/employee relationship.

CCTV and other types of cameras are the most obvious and high-profile surveillance technologies. However, it is important to recognise that there are many forms of

surveillance that do not involve cameras. Some of these, such as audio recording equipment, may be more appropriate to employ.

You will find references below that show where the regulations CQC enforces (the Health and Social Care Act 2008 (Regulated Activities) Regulations 2010) are relevant to the information. New regulations, known as the fundamental standards, will be introduced in April 2015 and this information will be updated then.

Any use of surveillance must comply with the law. **This information does not constitute legal advice and should not be relied upon as such.** The legality of using surveillance is a complex topic and we advise providers to obtain expert legal advice when considering its use, especially where it is likely to collect very sensitive information about people or intrude on their privacy. The examples in this information are general and should not be assumed to apply to any specific situations.

Key points

- Covert and overt surveillance can have legitimate uses. You should weigh their benefits against the impact on people's privacy, and other issues set out in this document, in deciding whether to use them.
- The use of surveillance in places where people are receiving health and social care services is likely to raise greater privacy concerns than many other kinds of business – especially where the care service is also a place where people live.
- Wherever possible, providers should consult with the people who use their service, families, other regular visitors, trade unions and staff when deciding about whether and how to use surveillance.
- The guidance on conducting a Privacy Impact Assessment, produced by the Information Commissioner's Office (Annex 1), is helpful for working through and recording privacy issues when considering surveillance.
- Transparency and openness are vital in order to meet legal requirements, and to maintain the trust of people who use services and of care staff. However, there may be limited circumstances where the legitimate use of covert surveillance prevents such openness for a short time.
- Providers must ensure that all staff (including contractors) involved in the use of surveillance systems are properly trained and supported to use them.
- The equipment used must be suitable, safe and properly maintained.
- Information obtained or recorded through the use of surveillance must be kept secure, and anyone with authorised access to that information must understand their legal responsibilities.
- Where people lack mental capacity to understand or consent to the use of surveillance, providers must make decisions in accordance with the statutory principles of the Mental Capacity Act 2005 (see section 8).

- Providers must ensure that they (and anyone acting on their behalf) comply with the Data Protection Act 1998, and all other relevant legislation, at all times. You should consider the guidance produced by the Information Commissioner's Office and, where relevant, the Surveillance Camera Commissioner, and seek expert legal advice where necessary. You can find a list of guidance in Annex 1.
- You should document the steps you have taken when deciding to use surveillance, as evidence of these steps may be required by a CQC inspector.

Definitions

Surveillance is the monitoring of a place, person, group, or ongoing activity in order to gather information.

Overt surveillance is where the individual being monitored would reasonably be aware of the surveillance occurring. For example, visible CCTV cameras with clear signs saying that they are in use.

Covert surveillance is where the individual being monitored would not reasonably be aware of the surveillance occurring. For example, the use of hidden audio recording devices for a time-limited and specific purpose.

Surveillance systems are the technology and equipment used to carry out surveillance, or to store and process the information gathered. Advances in technology mean that new systems or methods may become more commonplace. For simplicity in this information we will generally make reference to 'surveillance', which could encompass CCTV, Wi Fi cameras, audio recording, radio-frequency identification (RFID) tracking and many other types of system. This information sets out considerations that can be applied to these and any other existing or emerging technologies.

Privacy, in its broadest sense, is the right of an individual to be left alone. Intrusion into privacy can include the collection of information through surveillance or monitoring of how people act in public or private spaces.[1]

This document does not cover:

- Direct medical assessment or treatment that gathers information – for example equipment that monitors a person's vital signs, such as their heart rate, for medical purposes.
- The use of technology, with the knowledge and explicit consent of the patient or their appropriate representative, specifically for the purpose of keeping a record of an episode of medical treatment – for example filming a surgical procedure.

[1] *Information Commissioner's Office Privacy Impact Assessment Code of Practice* http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf

- Communications systems controlled by the person using the service – such as webcams that can be switched on and off by the user to contact the provider, or alarm buttons that can be pressed in the event of a fall. This would not be considered as surveillance, but providers should still think about issues of privacy when using these systems.

1. Why might health and social care providers want to use surveillance in their services?

The most common uses of surveillance systems, such as CCTV, are as a way to enhance the security and safety of premises and property, and to protect the safety of people. Surveillance may also be used as a tool to help protect people from the risk of abuse, or to investigate allegations or serious concerns about possible abuse or crime.

Surveillance systems may also be an effective way to promote and support the independence and autonomy of people who use care services, by monitoring their welfare with the use of 'Telecare' systems, while minimising the restriction on their movements and activities.

In some circumstances, and with the required safeguards, surveillance systems may be used as part of the appropriate deprivation of someone's liberty – for example, to monitor and identify if a person living with dementia is leaving a care home.

2. Using surveillance lawfully and appropriately in health and social care services

We consider the use of surveillance in a place where people are receiving care – and where it is likely to collect information about people who use that service – to be an aspect of that care. The regulations under the Health and Social Care Act 2008 must therefore be met when using surveillance in this way.

Providers are also required to comply with the Data Protection Act 1998 (DPA) when processing personal data. Many providers will also have legal obligations under the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA)[2]. CQC does not directly enforce compliance with this legislation, but we recommend that

[2] The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the powers of public authorities to conduct covert surveillance and some other kinds of investigations.

you take account of relevant guidance and seek legal advice on how this can affect your compliance with the regulations.

Carrying out a 'Privacy Impact Assessment' is a structured methodology that may help providers to consider and record privacy issues and ways to address those issues. The Information Commissioner's Office has produced a detailed guide[3] on how an organisation can follow this process, which will prove valuable for any provider considering the use of surveillance. This approach can be tailored to the size of the organisation and level of formality required.

3. Understanding and defining the purpose for using surveillance systems

In any situation, the *Data Protection Act 1998* (DPA) requires that surveillance must only be used in the pursuit of one or more legitimate (reasonable, lawful and appropriate) purposes[4], and must be necessary, proportionate[5] and fair[6], to meet an identified and pressing need. Providers must be able to identify the purpose(s) for their use of surveillance – what you want to achieve by using it.

If you determine that you have a valid purpose, you should make an initial consideration of whether surveillance is the best way to achieve it: could something else be done that would not involve the same intrusion into people's privacy? You may wish to consider if surveillance is the most effective way to use available resources.

You should also consider at this stage – and keep under review – whether your planned use of surveillance for the identified purpose(s) is likely to comply with the 'conditions for processing personal data' under schedule 2 of the DPA.

Surveillance that is likely to gather 'sensitive personal data[7]' will require a provider to meet additional conditions under schedule 3 of the Act. We advise you to consider guidance produced by the Information Commissioner's Office (ICO)[8], and to seek legal advice if in any doubt.

You will need to consider in more detail whether the surveillance is necessary before you make any final decision, but you should consider at an early stage – and keep under review – whether alternative measures can meet the purpose you have identified.

---

[3] http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf
[4] 2nd Data Protection Principle – http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/I
[5] 3rd Data Protection Principle
[6] 1st Data Protection Principle
[7] s 2 Data Protection Act 1998 – http://www.legislation.gov.uk/ukpga/1998/29/section/2
[8] www.ico.org.uk

You may wish to use surveillance for more than one purpose. If so, each of these purposes must be identified as necessary and proportionate in its own right.

Information gathered using surveillance for one purpose must not be used for another, incompatible purpose. For example, recordings made for the sole purpose of protecting vulnerable people from abuse should not be used as a record of staff time-keeping for disciplinary purposes.

Example

A care home provider is concerned that there have been a series of thefts from a communal, living area of the home. Alternative ways to prevent thefts or identify the thief are not suitable, as many people in the home are living with dementia or experience difficulties in communication. The provider therefore decides that the prevention and detection of crime is a legitimate purpose to consider installing a surveillance system in the room.

Record your purpose(s), and initial assessment of why surveillance is necessary to meet it. You should also document what alternatives to using surveillance you have considered and why they are not suitable, as this will be evidence to support any decision to use surveillance.

Our inspectors may wish to view records of the steps taken in identifying the purpose.

4. Needs assessment

The purpose for the proposed use of any surveillance must consider how it will support the needs and interests of people using services[9].

This is particularly relevant where an identified purpose is to protect people from risks of unsafe care or treatment. You must decide whether their needs are met by surveillance and whether the intrusion is justified.

[9] Regulation 9(1) – The registered person must take proper steps to ensure that each service user is protected against the risks of receiving care or treatment that is unsafe by means of (a) the carrying out of an assessment of the needs of the service user and (b) planning and delivery of care in such a way as to (i) meet the service user's individual needs, and (ii) ensure the welfare and safety of the service user.

5. Thinking about the information you will gather and in what circumstances

It is important to think about what information is likely to be gathered during the use of surveillance, including information gathered incidentally or inadvertently.

The more personal information that the surveillance is likely to collect – or the more sensitive that information is – the greater the impact on people's privacy will be. A key issue for providers to consider at this point is whether you plan to use covert or overt surveillance.

People may behave differently if they know they are being observed, and this could help meet a purpose, such as the prevention of crime. It also means that covert surveillance has a greater impact on people's privacy as they are not able to change their behaviour as they would if they knew they were being observed.

Providers should also consider the potential of surveillance having a negative impact on the way staff interact with those they care for (if they know they are being monitored by overt surveillance) – for example, if it means that care is delivered in a process-driven way, rather than in a warm, person-centred way.

Covert surveillance is more likely to capture sensitive, intimate or deeply personal information. This means that any decision to use **covert** surveillance techniques must satisfy a more pressing purpose and legitimate aim than the use of **overt** surveillance to remain proportionate and lawful.

To remain lawful we would expect any covert surveillance to be limited in time and purpose. It should be used to deal with an identified problem, not put into regular ongoing use.

As mentioned above, for care providers that are public bodies the use of covert surveillance will be subject to authorisation under, and compliance with, RIPA[10].

Make an initial judgment of what information the planned use of surveillance is likely to capture, and how sensitive that information is.

[10] http://www.legislation.gov.uk/ukpga/2000/23/contents

6. Consultation

The use of surveillance systems in a care setting has the potential to be intrusive to the privacy of people who use services[11], their families and friends, staff, trade unions and other people who visit.

Consultation with these people is the best way to understand their privacy concerns[12]. Providers should consult on the use of surveillance wherever it is possible to do so.

Consultation is not a 'one off' exercise, but is something to be repeated throughout the process of considering and using surveillance. For example, it would be useful to consult:

- At an early stage of consideration (to establish the appetite for, or any significant concerns about, the use of surveillance).
- When detailed proposals have been developed (when people can best understand what is being proposed).
- And from time to time throughout the use of surveillance (so that the impact of its use can be kept under review).

Providers currently using surveillance systems should consider conducting a consultation on their continued use.

The information provided to people involved in the consultation should cover:

- The type of surveillance being considered.
- Where it is being considered for use.
- The purpose of the proposed surveillance.
- What information will be collected.
- Where and how it will be stored.
- Who will have access to the information and how long it will be kept for.

The consultation methods that are appropriate will depend on the number of those affected and the size of the provider. It will help to record in detail the outcomes of your consultation and the process followed.

The privacy concerns that are identified during consultation must be given due consideration[13].

[11] Regulation 17(1) – The registered person must, so far as reasonably practicable, make suitable arrangements to ensure (a) the dignity, privacy and independence of service users.
[12] Regulation 17(2) – The registered person must (c) encourage service users to (ii) express their views as to what is important to them in relation to their care and treatment.
[13] Regulation 17(2)(d) – The registered person must, where necessary, assist service users , or those acting on their behalf, to express their views [about their care and treatment] and, so far as is appropriate and reasonably practicable, accommodate those views.

In some, limited, circumstances, consultation will not be possible. For example the use of surveillance, in a targeted and time-limited way, to investigate specific concerns of abuse may be prejudiced if possible perpetrators are 'tipped off' by a consultation process. Where a decision is made not to consult on the use of surveillance, we would expect the provider to be able to explain and justify that decision.

Our inspectors may wish to see what steps you have taken to consult on the use of surveillance.

7. Consent for surveillance

As previously explained, any use of surveillance must meet relevant conditions for processing personal data (and, in some cases, sensitive personal data) under the Data Protection Act 1998 (DPA).

Consent ('explicit' consent for sensitive personal data) is just **one** example of a DPA condition that provides a lawful basis for surveillance. However, it is not usually well suited to surveillance, since it is not normally possible to get valid consent of all visitors and people using the service.

For this reason, conditions that do not require consent of the individuals are relied on for most surveillance.

However, any surveillance that is used in a non-public place for the purpose of capturing more sensitive personal data about an individual (such as information about their health, sexual life, race or religion) is likely to require *explicit* consent of that individual to be lawful. This is also the case when gathering information that is particularly intrusive of a person's privacy (even where it is not the specific intention to do so).

For example, a camera in the private room of a person who receives care is likely to require the consent of that person, but other lawful conditions under the DPA may be available so that consent is not required from other people who may enter the room (visitors, staff etc.)

It is unlikely to be lawful to use surveillance to directly observe a person's medical treatment, intimate care, or someone practicing their religion in a private place (such as a dedicated prayer room) without the explicit consent of that person, even if the purpose of the system is to observe something else.

If you are considering surveillance of this type, and where you cannot obtain or do not intend to seek their explicit consent, we strongly advise that you first obtain specialist legal advice.

Explicit consent should be absolutely clear. The individual must be told:

- how their information will be gathered
- what type of information will be gathered (or even the specific information)
- the purposes of gathering the information
- how the information will be used and accessed
- any special aspects that may affect the individual, such as any disclosures that may be made[14].

Where consent is required, it must be freely given (it cannot be obtained by coercion or threat) and a provider cannot infer consent from a non-response to a request for consent. When using consent as a basis for surveillance, the person must have a right to withdraw that consent.

It is important that any refusal, or withdrawal, of consent – where consent has been asked for – is respected.

The initial consultation process should not to be seen as an exercise in seeking consent.

Example 1

A person who receives care in their own home feels vulnerable and concerned about having carers in her house and raised this concern with the provider of her care. A CCTV system in her home, which can be switched on during visits from carers or at other times when she feels vulnerable, is considered as an option. The consent of the person receiving care would be required to make this lawful. Care staff attending the person's home should be notified about the cameras, but their consent is unlikely to be required.

Example 2

A CCTV system in a prayer room is likely to capture sensitive personal data – images of people privately observing their religion. It is likely that explicit consent of people using the room for prayer would be required – unless the purpose of the system is in the substantial public interest for the purpose of the prevention or detection of any unlawful act **and** obtaining explicit consent would prejudice that aim.

You must establish that you have a lawful basis for your proposed use of surveillance.

If consent is used as a basis for surveillance, you must keep appropriate records. Consent must be fairly and lawfully obtained, and refusal of consent must be respected.

Our inspectors may wish to see these records.

[14] http://ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing

8. Capacity to consent and to contribute to a consultation

Providers of care will be familiar with the statutory principles of the Mental Capacity Act 2005 (MCA). This Act provides the legal requirements to support and enable individuals who lack capacity.

Someone's lack of mental capacity is likely to mean that it is not possible to rely on their consent. You will not be able to seek that consent from others, such as their family, unless the person has given relevant powers under a health and welfare lasting power of attorney.

Where explicit consent is likely to be required to use surveillance lawfully, for example in the room of an individual, and it is established that an individual lacks mental capacity, it would not be appropriate for a provider to make a decision or attempt to provide explicit consent on behalf of the individual, in the absence of a relevant power of attorney, even when acting in accordance with the MCA. A 'best interests' decision made in accordance with the Act does not have the same legal basis as consent.

This means that there may be circumstances where surveillance that is particularly intrusive to the privacy of an individual who lacks mental capacity may require permission from the Court of Protection, who can fairly decide if this is appropriate.

If you have concerns that a person who lacks capacity to consent, or any other vulnerable person, may be being abused, you should report this through local safeguarding processes.

Whenever you are consulting on, or considering, the use of surveillance, you must also be careful to consider the best interests of individuals lacking in mental capacity. You should consider whether and how you can support people to enable them to express their views about privacy, and you should consult with their families, friends and representatives as appropriate.

A lack of mental capacity must not be used as an excuse to ignore or dismiss the right of privacy of any person.

You should take special care to record how you have handled the best interests of people who lack mental capacity when consulting on the use of surveillance and, in particular, any consent-based, or more privacy intrusive use.

You should consider consulting on the use of surveillance with family, friends and representatives when making decisions about the best interests of an individual who lacks capacity. This may be used to identify the individual's likely privacy

concerns. However, a best interest decision does not have the same legal basis as consent.

You will need to regularly check whether people deemed to be without mental capacity at one time still lack capacity. Therefore, those previously deemed without mental capacity when decisions were made about the use of surveillance should be informed, consulted with and consent obtained as appropriate when they are deemed to have capacity.

9. Protecting privacy and treating people with dignity and respect

Providers should take steps to address any concerns about surveillance that have been identified from people who use services or their families, with the aim of minimising the potential impact on privacy[15].

It is not the responsibility of individuals to identify all the relevant concerns but for the care provider to be aware of the need to treat people with dignity and respect.

Some privacy protections will be relevant to all surveillance, such as ensuring that only authorised people can access the information collected. Others may depend on the particular situation and the privacy risks that have been identified.

This could include taking steps such as:

- Repositioning cameras or audio recording equipment, or limiting the times at which they are in use, to capture less sensitive information, information about fewer individuals, or to avoid capturing behaviours that may be more intrusive on people's privacy (such as intimate care).
- Seeking to gather information that is less identifiable, for example statistical information from sensors instead of video.
- Allowing staff, or people using the service, to turn off a surveillance system at certain times.
- Following the ICO's CCTV Code of Practice, and the Surveillance Camera Code of Practice, on the positioning and use of CCTV cameras.

Recording sensitive information, such as intimate care or people privately observing their religious beliefs, should always be avoided wherever possible. More privacy

[15] Regulation 17(1)(a) The registered person must, so far as reasonably practicable, make suitable arrangements to protect the dignity, privacy and independence of service users.

intrusive surveillance, such as indiscriminate recording of audio in semi-public or private places should be minimised.

Cameras worn on people providing intimate care may be particularly intrusive. If these cameras are used, they should be switched off while intimate care is being delivered.

As detailed above, more privacy intrusive types of surveillance will require a greater justification and need to meet higher requirements to remain lawful[16].

Documenting how you have addressed privacy concerns, or where you are unable to and why, will be invaluable in making your final decision. Our inspectors may wish to view the steps you have taken.

Providers must balance their legitimate and necessary aim against the privacy concerns and intrusion of those affected to decide if the surveillance is fair and proportionate[17]. These decisions should be made by an appropriate and senior person or group within the provider organisation, and clear records of their consideration, decision and reasons for their decision must be retained.

If an organisation is a public body, subject to the requirements of the Regulation of Investigatory Powers Act 2000, the decision to use covert surveillance may only be made by an Authorising Officer who is empowered to do so under the Act.

Any use of covert surveillance under RIPA must be undertaken in line with your established policies. An inspector may wish to see evidence of policies and whether they have been followed.

10. Additional consideration in relation to deprivation of liberty and restraint

In some circumstances, surveillance systems could be used for purposes that fall within the definition of 'deprivation of liberty' – for example, the use of CCTV or RFID tracking devices to monitor the location of an individual for the purpose of preventing them from leaving the premises[18].

[16] As there will be a greater infringement of Article 8 ECHR rights. A lawful basis under Schedule 3 DPA for processing sensitive personal data is likely to be required.
[17] Regulation 17(1)(a) The registered person must, so far as reasonably practicable, make suitable arrangements to protect the dignity, privacy and independence of service users / Regulation17(2)(a) – The registered person must treat individuals with consideration and respect.
[18] Regulation11(2) where any form of control or restraint is used, the registered person must have suitable arrangements in place to protect the service users against the risk of such control or restraint being (a) unlawful, or (b) otherwise excessive.

If the identified purpose or use of surveillance has the potential to act as a restriction on, or deprivation of liberty, special care must be taken to consult with individuals and to consider the relevant guidance. This is in addition to the usual considerations that must be made on the use of surveillance.

Providers should be aware that restraint, as defined in the Mental Capacity Act, includes the restriction of movement of a person lacking mental capacity, whether the individual is resisting or not.

Restraint is only lawful if, in addition to the requirements for all best interests decision making, the person carrying out the restraint reasonably believes that this restraint is necessary to prevent harm, and is proportionate to the risk and seriousness of that harm[19].

Deprivation of liberty occurs when a person lacking mental capacity is not free to leave the place where they are receiving care and treatment, and are under continuous supervision and control[20].

If a person might be deprived of their liberty, the provider must be sure that it is in the person's best interests, and proportionate as above. Every effort should be made to provide the necessary care or treatment in a way less restrictive of the person's rights and freedom.

If this is impossible, the provider must request authorisation of the deprivation of liberty, either from a local authority (where the deprivation of liberty safeguards would be used) or from the Court of Protection[21].

CQC must be notified of all applications for a deprivation of liberty authorisation, and the outcomes.

11. Safety, suitability and maintenance of equipment

Any surveillance system must be suitable for its intended purpose. For example, a CCTV system that needs to be able to identify an individual person will not meet its purpose if the resolution of the images is not high enough or the lighting is not sufficient.

[19] Mental Capacity Act 2005 S 5 and 6
[20] [2014] UKSC 19 https://www.supremecourt.uk/decided-cases/docs/UKSC_2012_0068_Judgment.pdf
[21] http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_085476

'Meta-data', such as the date, time and location of a recording, should be collected and retained as appropriate to support the purpose.

The equipment should be maintained regularly to ensure it is working correctly and remains suitable for its purpose.

In particular, providers must assess whether any surveillance equipment may represent a risk to health and safety, and take appropriate steps to mitigate it.

12.Staff training and record keeping

Controls must exist to ensure that only appropriate and authorised people are given access to any information recorded; for example by placing monitors for viewing CCTV images in a lockable office, where only an appropriate manager can access them.

Only people with a legitimate and lawful need to access private information obtained by surveillance should have access to that information. The provider must ensure that adequate security is in place to prevent unauthorised access – the more sensitive and private the information, the greater the required level of security.

Information being stored or transmitted electronically must be kept safe through the use of strong passwords and appropriately secure software.

If information is being stored on your behalf by a third party (for example, on a web-based server) you are still responsible for ensuring that it is kept secure.

Staff who are authorised to have access to information gathered by surveillance should have appropriate training on its use. You should keep a record of when and why recorded information has been accessed.

When recording information via surveillance systems, there will be statutory obligations on care providers under the DPA and – for public authorities – the *Freedom of Information Act 2000*[22], which may create a right of access to the information[23].

There should be clear policies and procedures in place for handling requests for access to recorded information, on sharing and disclosing information, and on handling complaints about the use of surveillance (for example, where someone considers that the use of surveillance is causing harm or distress).

There should also be clear policy on the secure[24] retention and destruction of information. Retention of data should be in line with the requirements of the original

[22] http://www.justice.gov.uk/information-access-rights/foi-guidance-for-practitioners/code-of-practice
[23] Individuals are likely to have a right to be provided copies of surveillance information about them under section 7 of the DPA.

purpose(s)[25] for its collection, not based on the technical limitation of the system. For example, footage from a camera used to prevent or detect crime should not be retained beyond the agreed policy timeframe for this purpose.

13. Informing people

Wherever possible, you should ensure that staff, people using the service and all visitors are informed about the use of surveillance. Consider whether they can be notified in general terms about the use of covert surveillance, if this does not prejudice the purpose.

Part of this may be via an appropriate Privacy Notice[26] and physical signage, but this alone is unlikely to be sufficient. You should consider the mental capacity[27] of those affected and decide the most appropriate way to communicate, within the principles of the Mental Capacity Act as appropriate. You should also consider people's differing physical needs as this may affect how you inform and communicate with them.

Providers that use surveillance are required to register as a 'data controller' with the Information Commissioner's Office. Most providers will already be required to be registered anyway, but you should ensure that your registration is adequate to cover the use of surveillance.[28]

14. Operation of the system

You should have a clear record of who is responsible for the operation of any surveillance system, and for the protection, management and control of the information obtained using surveillance.

---

[24] Regulation 20(1)(b) - The registered person must maintain such records as are appropriate in relation to the management of the regulated activity, these records must be: 20(2)(a) kept securely and located promptly when required.
[25] Regulation 20(2)(b) – [these records must be] retained for an appropriate period of time, and 20(2)(c) securely destroyed when it is appropriate to do so.3.
[26] Information Commissioner's Office Privacy notice topic guide http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices
[27] Regulation 17(2)(b) – The registered person must provide service users with appropriate information about their care.
[28] Required under section 17 of the *Data Protection Act 1998*

15. Surveillance equipment installed by people who use the service, or their relatives

From time to time, people naturally worry about whether a loved one is being properly cared for. Whether they are being looked after in a health or social care setting, there will be times when relatives and friends may be concerned because they cannot see directly what is going on. They may think about using a hidden camera or audio recording device to reassure themselves about the care their loved one is receiving. We will shortly publish information for the public to help them with these considerations.

If a provider discovers that covert or overt surveillance is being used in their service, the welfare and care of the person using the service must remain their primary consideration. Even if the use of the camera breaches a contract of service, the continuity and safety of the person's care must be ensured.

The decision to use surveillance may well arise from a significant fear or concern about the quality of care or about the welfare of a vulnerable person. It may indicate a problem which you were not aware of, and it is very important that this is investigated and understood. In some cases, this may even lead you to think about undertaking your own surveillance, with consideration of the information in this document.

The person using the service or their friend or relative should not suffer any detriment of care or consideration if you discover that they have used surveillance without your knowledge. As with any other circumstance where concerns are raised, we would expect the provider to follow appropriate procedures to investigate and respond.

If you are concerned that the surveillance may be unreasonably intruding on the privacy or rights of a person using the service or others, then you will want to ensure this is properly assessed and make a decision about the continued use of the surveillance equipment, including the position relating to consent and safeguarding circumstances.

Deliberately damaging a surveillance device, deleting recordings or removing the device with the intention of **not** returning it to its legal owner is likely to be a criminal offence. However, switching a camera off, or removing it for safekeeping and return to its owner would not be.

16. The Care Quality Commission and the use of information recorded using surveillance

CQC's powers[29] allow us to have access to information that has been recorded using covert or overt surveillance (or to have access to surveillance systems) where we consider it necessary and proportionate to do so to exercise our functions as a regulator.

However, we would not *routinely* access this information. We would ask to access these recordings where we believe that they may assist us in understanding the quality and safety of the care provided, or in assessing your compliance with the standards of care set out in regulations.

Where we receive or access a recording that shows abuse, or poor or unsafe care, we will, of course, act on that information.

Alongside this document, we have published guidance for our staff on how we will handle and use recordings made using hidden cameras and other covert equipment.

[29] Principally under sections 62 to 64 of the Health and Social Care Act 2008

Annex 1 – Relevant guidance

Guidance on meeting the CQC inspection standards[30] **–** How providers should meet CQC standards.

Surveillance Camera Commissioner code of practice[31] – Principles for the use of CCTV

Information Commissioner's Office Privacy notice topic guide[32] – How to notify individuals of an impact on their privacy

The Information Commissioner's Office Code of Practice on CCTV[33] – Complying with the DPA in relation to CCTV

The Information Commissioner's Office employment practices code[34] and **supplemental**[35] – Complying with the DPA in an employer / employee relationship.

The Information Commissioner's Office guide to data protection[36] – A general guide to complying with the DPA, as any surveillance which records personal information must do.

The Mental Capacity Act 2005 Guidance for providers[37] **–** A CQC guide to issues of capacity.

The Mental Capacity Act Code of Practice[38] – A guide from the department of constitutional affairs on complying with the Mental Capacity Act, useful for guidance on acting in the best interests of an individual.

ICO Privacy impact assessment code of practice[39] – Detailed guidance applicable to all forms of surveillance on completing an assessment of the privacy impact.

The ICO Guide to Data Protection[40] **–** A general guide on complying with Data Protection Act 1998.

---

[30] http://www.cqc.org.uk/content/guidance-meeting-standards

[31] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

[32] http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices

[33] http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/cctv-code-of-practice.pdf

[34] http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/the_employment_practices_code.pdf

[35] http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/employment_practice_code_supplementary_guidance.pdf

[36] https://ico.org.uk/Global/~/media/documents/library/Data_Protection/Practical_application/THE_GUIDE_TO_DATA_PROTECTION.ashx

[37] http://www.cqc.org.uk/sites/default/files/documents/rp_poc1b2b_100563_20111223_v4_00_guidance_for_providers_mca_for_external_publication.pdf

[38] https://www.justice.gov.uk/protecting-the-vulnerable/mental-capacity-act

[39] http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf

[40] http://ico.org.uk/for_organisations/data_protection/the_guide

Published December 2014

How to contact us

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