Use of surveillance in health and care settings: Guidance for UNISON representatives

Introduction

Recent incidents of abusive or neglectful care in care homes and hospitals (Winterbourne View, Orchid View and mid-Staffordshire NHS Trust) have prompted a debate about the use of surveillance cameras to deter and detect poor care.

- HC One, which took over many former Southern Cross homes, including scandal-hit Orchid View in West Sussex, has recently consulted residents on installing visible CCTV cameras in all its care homes.

- Care sector regulator for England, the Care Quality Commission (CQC), has issued guidance for health and care providers, and for the public, on the use of surveillance to monitor care standards.

- Meanwhile, worried relatives sometimes resort to installing hidden cameras to check up on their loved ones' care when they feel their concerns are not being addressed. Some recordings have ended up being aired in TV exposés.

This is a sensitive debate with implications for the rights of patients and service users, and for the workforce.

UNISON's over-riding concern is to raise standards of care and to campaign for greater regulation and protection from abuse. We believe that the use of surveillance can only ever address the symptoms of poor care provision and not the causes. UNISON wants all health and care settings to be safe, welcoming places where people can be confident they will receive decent care, and where staff can be proud to work.

In the meanwhile, UNISON members may be facing the installation of surveillance cameras where they work. The advice in the next sections covers the legal, bargaining and policy issues that UNISON representatives will need to protect members' rights and promote the rights and dignity of service users.

ADVICE FOR UNISON REPRESENTATIVES

Employer proposals for *visible* surveillance

A health or care provider may decide to install visible surveillance cameras to provide reassurance to relatives, or to deter and detect abusers. The cameras may be in communal areas or on wards. They could also be installed in care home bedrooms, or service users' own homes. This would require the individual consent of the patient, resident or service user. Some residents may come under pressure from worried relatives to consent even though the cameras could be recording intimate personal care tasks. These are very sensitive issues and care providers will need to tread very carefully around issues of consent, including mental capacity.

Any attempts by employers to use CCTV cameras as a pre-text for reducing staffing – for example on night shifts – should be resisted robustly.

KEY LEGAL REQUIREMENTS FOR PROVIDERS

1. 1998 Data Protection Act

The 1998 Data Protection Act (DPA) protects people's personal information in relation to the use of surveillance. You can read a legal guide to the Data Protection Act at www.thompsons.law.co.uk/ltext/l1000001.htm .

The Information Commissioner's Office (ICO) publishes a *Data protection code of practice for surveillance cameras and personal information.* This applies across the UK and to all types of organisation, not just the public sector: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

For health and care settings, the key provisions of the Code advise that:

a) Providers must have a legitimate, necessary, proportionate and fair purpose for installing surveillance, in order to meet a pressing need.

b) Providers must consider alternative means of dealing with the problem before they proceed with surveillance.

c) Providers should consult with patients and residents, their families and staff about installing surveillance. Where someone doesn't have capacity they should consult with an authorised person ie someone who has 'health and welfare' power of attorney.

d) Providers should consider conducting a 'privacy impact assessment' to ensure they have looked at all privacy issues and the means of addressing them. This should include thinking about what sensitive information is likely to

be captured by the surveillance, who it could adversely affect, and what alternatives could be used. The ICO has a code that tells organisations how to do privacy impact assessments at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf . This looks at assessing wider human rights obligations as well as data protection.

e) Use of surveillance in the workplace should interfere as little as possible with workers' legitimate expectations of privacy.

f) Providers must have clear procedures for how they handle information gained from surveillance including disclosure, storage, and disposal.

g) Providers must notify the Information Commissioner on an annual basis about their surveillance set-up. They must also identify a named data controller for their organisation.

h) In the run-up to the annual notification date, providers should take the opportunity to review whether surveillance use continues to be justified.

i) Providers must display prominent notices warning visitors to health and care facilities of the type of surveillance that is in operation there, and who can be contacted about the scheme.

j) It should be made prominent and clear to staff when, how and why surveillance is taking place, and who they can contact about it.

2. 1998 Human Rights Act

People whose care is publicly funded or commissioned for them by a public body, are also protected by the 1998 Human Rights Act. You can read a legal guide to the Human Rights Act at www.thompsons.law.co.uk/ltext/l0730001.htm.

Among other things, the Act protects an individual's right to a private and family life. The effect of the Act is consistent with the Data Protection Act, in that use of surveillance cameras has to be justifiable. For example, the provider must show that their use was necessary to address a pressing need, such as a risk to public safety or the need to prevent a crime. It also has to be proportionate and done only after consideration of other means of dealing with identified problems.

3. Care standards: regulatory guidance

The Care Quality Commission (CQC) regulates health and social care services in England and has produced guidance for health and care providers, and for the public, on the use of surveillance in settings such as care homes, hospitals and people's own homes.

CQC Guide for providers:
http://www.cqc.org.uk/sites/default/files/20141215_provider_surveillance_information.pdf

CQC Advice for the public:
http://www.cqc.org.uk/sites/default/files/20150212_public_surveillance_leaflet_final.pdf

CQC says that it is for providers to decide, operating within the law, whether they use surveillance, but: *"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."*

The guidance also says that where surveillance is used by providers, CQC inspectors will expect to see an evidence trail, in line with with legal requirements, justifying the decision to use it – including what alternatives they considered, and what consultation they carried out.

CQC has powers to access surveillance footage recorded by providers or families if they consider it necessary and proportionate as part of their regulatory functions. And they encourage members of the public to share any recordings which give cause for concern so that CQC can take appropriate action.

BARGAINING ADVICE

Health and care providers should enter into a process of consultation with staff and their UNISON reps as soon as they are considering installing surveillance devices. Staff should have a genuine opportunity to air their views and concerns. A full consultation with residents/service users/patients will also be required.

The guidance for providers issued by CQC says they *"should consult with people who use their service, families, other regular visitors, trade unions and staff when deciding about whether and how to use surveillance."*

Questions for reps to ask – cameras under consideration

1. What evidence of problems does the provider have and why do they think surveillance will effectively address them?

2. What other measures have they considered? For example, if it is about providing reassurance to absent relatives – could Skype and webcam facilities be made available so they can communicate visually with their loved one? If it is about deterring abusers, should the provider focus on improving its training, vetting and

supervision procedures? Are more staff needed? Are there trusted ways for staff to raise concerns about standards of care?

> **The guidance for providers issued by CQC** says they should first consider whether they have enough skilled competent staff on duty at all times; an open culture where the raising of concerns is welcomed; good supervision and appraisal of staff.

UNISON representatives should be consulted about whether they believe all possible alternatives have been explored.

3. How much will the surveillance system cost to install and maintain? Could this money be put to more effective use – eg staff training, improving wages, extra staff on night-shifts and at mealtimes?

4. Has the provider assessed whether their plans are compliant with the Data Protection Act, the Information Commissioner's Office Code of Practice for surveillance cameras and personal information, and the Human Rights Act?

Questions for reps to ask – cameras in operation

5. Does the provider intend to use cameras permanently or on a temporary basis? If temporary, for how long?

6. Will the cameras record constantly or just at certain times of day?

7. Will the system record audio, video or both? If audio recording is used the ICO Code says that additional evidence and justification is required, as this is likely to be a greater intrusion of privacy than video alone.

8. What are the specifications of the system in terms of picture quality, accurate date and time marking, and system maintenance.

9. Who will be the named individual responsible for operation of the surveillance system?

10. Who will be able to watch footage? How often will it be monitored? Will it only be viewed if a concern or allegation is raised?

11. How long will the footage be stored and where (retention period)? What records will be kept of who footage is disclosed to and why?

12. Will the provider operate the surveillance system directly – if not who will it be contracted out to and what are the terms of the contract governing security, disclosure, storage of footage etc?

Policies and procedures to negotiate if surveillance is used

13. There should be an overarching policy for staff which fully informs them of the location, purpose and specification of all surveillance devices. This information needs to be clearly referenced in staff handbooks and properly covered in induction of new staff.

14. The policy should set out the terms of use together with things like who will have access to the footage, how long it will be kept, security of storage and disposal

15. Anyone who is the subject of recordings or images has the right under the Data Protection Act to request a copy of them (a fee of up to £10 fee may be charged). So, for example, a patient or service user can request to see any images or recordings featuring themselves that the health or care provider holds. Or a family member may do this on their behalf. There should be a clear procedure for informing staff if they feature in surveillance footage or recordings disclosed to relatives, the regulator or other parties – unless this would prejudice a criminal investigation.

16. Staff also have a right to request to a copy of images or recordings of themselves that their employer holds. They may want this to defend themselves where an allegation has been made, or they may want access to evidence that they have suffered an assault or attack at work. There should be agreed procedures for staff to request such access (subject access). The employer must respond within a maximum of 40 calendar days. You should seek agreement that the employer will not charge staff the £10 fee. (nB there are some circumstances where the employer is able to refuse to release footage or recordings – for example if it would prejudice an ongoing investigation).

Use of *covert* surveillance

Under the Data Protection Act, covert surveillance will only be justified in very exceptional circumstances. This could happen as part of an investigation of suspected criminal abuse, neglect or serious malpractice affecting safety, where open use of surveillance might prejudice detection. It should be time-limited and not in regular and ongoing use. If the provider is a local authority, use of covert surveillance has to be specially authorised under the *2000 Regulation of Investigatory Powers Act* or *Regulation of Investigatory Powers (Scotland) Act*.

Covert surveillance can only be used where the provider has genuine suspicions of criminal activity. It must be strictly targeted at gathering evidence linked to this activity. It cannot go wider than what is necessary for the investigation – **fishing expeditions are not permitted**. If in the course of a surveillance exercise, the cameras capture images of wrongdoing unrelated to the original purpose they can only be used if the actions are sufficiently serious to make this reasonable and necessary eg an act of gross as opposed to minor misconduct. For example, if the

cameras were installed to detect suspected abuse of care home residents, incidental footage can't be used as the basis for disciplining someone for being late, or taking a smoking break at the wrong time. Footage of workers who are not the target of the investigation should be obscured or deleted as soon as possible.

Surveillance measures installed by families

There may be circumstances when families install covert cameras in health or care settings where UNISON members are working. If they do this without the knowledge of the provider, members are likely to find it harder to enforce their rights. The law here is complex – cameras installed by individuals (as opposed to organisations) for "domestic purposes" ie for an individual's own "personal, family or household affairs" are exempt from the Data Protection Act. Furthermore, Human Rights Act obligations don't apply to private individuals, only to public bodies.

Where surveillance has been installed by a private individual, but on a health or care provider's premises, the situation is unclear. The CQC guidance states that there has never been a legal challenge so far to a family's use of recording equipment, so the position is untested. But they advise that to reduce legal risks, family members should ensure devices only record in their relative's private room, are used only for a time-limited period, and that recordings are kept securely.

The CQC guidance says that if providers discover that relatives have installed hidden cameras they need to take steps to investigate and understand the concerns that have prompted this. They should also make an assessment of the privacy impact of the cameras before discussing their continued use.

However, if a relative approaches a care provider for permission to install a camera, the care provider would need to satisfy itself that this is justified. The ICO makes it clear that using surveillance just because a client or customer has asked for it will not meet the DPA requirements.

You may find yourself representing members on disciplinaries where surveillance material is introduced. You will need to be prepared to ask questions about why, when, how and where the footage was obtained in order to assess whether the employer can legitimately use it. If in doubt, seek further advice from your Regional Organiser.

APPENDIX 1

UNISON policy: Raising standards and deterring abuse

UNISON believes that problems affecting standards within health and social care are complex and require systematic and comprehensive reforms. For example, much of the care sector is characterised by high staff turnover, poverty pay, poor training and qualifications, staff shortages, volatile market conditions and inadequate regulation. Recruiting and retaining a skilled workforce is a constant struggle when care work continues to be under-valued and over-looked by every part of the system.
The use of surveillance cameras may provide short-term reassurance to worried families, but it is clear that a much more systematic response is needed. Unless there is a long-term government-led plan for ensuring consistent quality standards, people will continue to be failed. Nobody wants elderly and disabled people to have to rely on hidden cameras to feel less threatened in their daily lives.

UNISON believes this require a series of reforms:

1. Investment in high quality training and minimum qualification requirements for care staff
2. Mandatory training on dementia, learning disability and other conditions as appropriate
3. Annual personal development reviews for all staff
4. Statutory requirements for safe staffing ratios throughout the day and night
5. Access to regular and supportive supervision by trained senior staff
6. Statutory professional registration for healthcare assistants
7. Minimum pay levels, regardless of sector, starting with the Living Wage and building in progression to help retain good staff
8. Regular engagement by care homes and hospitals with their wider communities through open days, links with schools and other activities
9. Safe and supportive channels for staff and relatives to raise concerns without fear of reprisals

Local authority and health commissioners need to ensure that when they are procuring health and care services they require contractors to meet minimum standards of training and staffing levels.

Regulatory safeguards

UNISON does not want to see providers introducing surveillance in order to paper over underlying problems and poor practices. We believe that as well as notifying the Information Commissioners Office, providers should be required to notify the health and/or care regulator in advance of installing surveillance so that checks can be

carried out and recommendations made for alternative or additional measures. The perceived need for cameras may be an indicator that things are going seriously wrong in a service.

APPENDIX 2

Additional information on regulation of surveillance

- **Additional ICO information on surveillance in the workplace**

The ICO also publishes additional information about use of video and audio monitoring in the workplace. This is contained in employment-specific guidance from the ICO and stresses the need to consult with trade union representatives.

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

and

https://ico.org.uk/media/for-organisations/documents/1066/employment_practice_code_supplementary_guidance.pdf

- **2012 Protection of Freedoms Act (POFA) – Surveillance Camera Code of Practice (England and Wales)**

The POFA places additional requirements on local authorities and the police. They must have regard to the *Surveillance Camera Code of Practice* issued by the Secretary of State, covering England and Wales. Other operators of surveillance cameras are encouraged to adopt the Code voluntarily, and the government has said that it will consider extending the requirement to other organisations in the future.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

- **CCTV Strategy for Scotland**

The Scottish Government has issued a strategy document with a common set of principles predominantly aimed at local authorities and police partners and operation of surveillance cameras in public spaces.

http://www.gov.scot/Resource/Doc/346155/0115210.pdf