ic2 DESIGN INSTALL PROTECT

CCTV, compliance and the NHS: A guide to wellbeing for hospital security managers

CCTV compliance in NHS trusts and adult social care settings

www.ic2cctv.com

INTRODUCTION

The NHS is one of the most admired institutions in the world. A model for socialised health systems, it is the envy of any nation that aspires to fairness and equality for its citizens. However, few would argue that it's perfect, and the NHS faces some tough challenges as it tries to adapt to a rapidly changing world.

One of the biggest challenges has been in the continuing hardening of the regulatory framework for ensuring high standards of care. This is written into law, distilled into practical policy and enforced by the government's all-powerful watchdog, the Care Quality Commission.

Technology is perhaps the single most important agent of change and it is a double-edged sword. It provides immense life-saving and life-changing benefits in medicine. But it is also a source of risk. The data generated by computerised systems in healthcare settings is especially sensitive.

And it's not just medicalised systems. CCTV video and data collected by other security systems are also examples. In hospitals this is not governed by the CQC. This falls under the regulatory control of the Information Commissioners' Office (ICO) and is governed by the Data Protection Act (DPA).

If the NHS is a model for socialised healthcare systems, then each hospital trust needs to exhibit exemplary behaviour in addressing its CCTV compliance obligations. In this guide we discuss the considerations that shape the use of CCTV in NHS hospitals and the wider health and social care system in the UK.

CCTV compliance framework: Fitting the pieces together

The use of CCTV is governed by a number of different codes, guidance and legislative instruments. Most directly, these are the:

- Surveillance Camera Code of Practice (Home Office, 2013)
- In the picture: A data protection code of practice for surveillance cameras and personal information – 'CCTV Code of Practice' (ICO, 2014)
- Data Protection Act, 1998 (DPA)

As CCTV systems in NHS trust facilities are operated on or behalf of a public authority, additional legislative instruments and guidance weave together to create quite a complex framework and widen the considerations for healthcare environments. These include:

- Freedom of Information Act, 2000 (FOI)
- Human Rights Act, 1998 (HRA)
- Protection of Freedoms Act, 2102 (POFA)

What the DPA says about CCTV

CCTV systems consist of devices which view and record images of individuals. They also enable the capture of other information that relates to individuals, such as vehicle registration marks. Consequently, the use of CCTV systems is brought into scope of the DPA by guidance and codes of practice issued by the Home Office and the ICO.

The DPA creates obligations for organisations and gives individuals the right to gain access to the information held about them and to claim compensation should they suffer damage as a result of DPA non-compliance.

The legal requirement is to comply with the DPA and the eight Data Protection Principles enshrined within the Act to ensure:

- Persons tasked with capturing images of individuals are in compliance with the DPA
- Captured images are of usable quality
- Reassurance is available to those whose images are being captured

Hierarchy of responsibility

Security in general and CCTV in particular sits very high up on the Governance agenda. Consequently, ultimate responsibility rests with the trust Chief Executive and the executive with Security Management responsibility. Reporting to this top level is likely to be the senior manager of the site, typically the Director of Estates and Facilities, who in turn is likely to delegate day-to-day oversight to a Security Manager.

Enforcement action

Under the compliance rules, a data controller is responsible for viewing, sharing and securing access to CCTV footage. The ICO has a number of tools at its disposal for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information, or to punish breaches of the regulations such as misuse of data.

These include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller.

The tools are used in combination where justified by the circumstances.

The main options are:

- Serve information notices requiring healthcare organisations to report specified information within a certain time period to the Information Commissioner's Office
- Issue undertakings for organisations to commit to a particular course of action to improve compliance and avoid further ICO action
- Enforcement notices requiring organisations in breach of legislation to take specific steps in order to comply with the law
- Liaise to conduct consensual audits to check healthcare organisations are in compliance
- Serve assessment notices of compulsory audits to assess whether a healthcare organisation is following good practice in processing personal data
- Issue financial penalty notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010
- Prosecutions and custodial sentences for those who deliberately commit criminal offences under the Act
- Report to Parliament on issues of concern

New EU General Data Protection Regulations (GDPR) proposes fines of up to 5% of global turnover. Recent figures show between January 2013 and October 2014 there were 66 enforcement notices issued by the ICO for DPA infringements and financial penalties totalling £2.17M were issued.

Application of CCTV to hospitals

For the purposes of deploying CCTV in the UK's public healthcare facilities, hospital sites are broken down to designate each area as Public, Communal or Private.

Public areas

Public areas are areas of the hospital to which the public have unrestricted access. These areas may be internal or external. Typical Public areas include the hospital grounds, access roads, car parks, entrances and exits, reception and waiting areas

There are no special considerations for hospital deployment of CCTV in areas designated as Public except those that are required by the Information Commissioner for CCTV cameras in any general public setting, such as signage and notification.

Communal areas

Communal areas are parts of a ward or other closed healthcare facility shared by all patients. Typical Communal areas include ward areas, day rooms, dining areas, garden areas and corridors.

CCTV is sometimes used in communal areas where it justifiably supports the safety of service users, staff or the public. It is central to any decision that, in line with the requirements of the Information Commissioner, a clear reason for installation is determined.

Private areas

Private areas are those where any individual might reasonably expect privacy.
These include bathrooms, bedrooms, toilets, and consulting, interview and seclusion rooms.

The legal basis for deploying CCTV in areas designated as Private arises from a patient's capacitated consent or because monitoring is a proportionate measure for any individuals detained under the Mental Health Act 1983 for compulsory treatment.

Naturally the use of CCTV and audio surveillance in Private areas is a matter of the highest sensitivity and the following considerations should be noted:

- There is considerable burden on the trust or care provider to prove that any intrusion is proportionate
- This burden may be higher if the cameras are linked to a recording device. If recording rather than real-time unrecorded monitoring is required, then the General Medical Council (GMC) guidance on making and using visual and audio recordings of patients, Making and Using Visual and Audio Recordings of Patients (May 2002) should be consulted
- Care needs to be taken in the siting of the monitors to ensure that inappropriate accidental or deliberate viewing of images by patients, staff or visitors cannot take place
- Gender issues and the potential for increasing patient vulnerability, inappropriate behaviour, sexual harassment or abusive relationships are also very important
- Any decisions on CCTV in private areas must be made in consultation with clinicians using a robust and documented authorisation process
- Questions of legality should be addressed by consulting the Information Commissioner, the GMC and other appropriate legal resources
- Issue undertakings for organisations to commit to a particular course of action to improve compliance and avoid further ICO action
- Enforcement notices requiring organisations in breach of legislation to take specific steps in order to comply with the law

Legitimate and fit for purpose

Essentially, in any setting it is necessary to define a legitimate reason for CCTV and obtain a solution fit for purpose. To do this we must consider what we want to achieve with the system.

Legitimate reasons for deploying CCTV are to act as a deterrent and as a tool for detection and identification during and after an incident. Examples include:

- Theft and criminal damage
- Staff, patient and public safety
- Violence and aggression
- Antisocial behaviour and vandalism
- Movement on, off and within the site through access points including gates and barriers

Typical use cases include:

- Monitoring large areas
- Detecting individuals approaching a building
- Observing the actions of a group of people
- Verification of individuals at access points

To ensure a system in a hospital setting is fit for the purposes intended, a system should be specified only after a thorough analysis of the site is undertaken, including a Risk Assessment to identify vulnerabilities.

Security risk assessment

A security Risk Assessment enables hospital estates, buildings and facilities managers to develop a thorough understanding of the requirements and the best way to use CCTV to support security across a hospital site. It enables the overall level of security to be assessed and an understanding of where there are gaps between the level of security needed and the existing security measures in place. Some of the things likely to be covered by the assessment include:

- The presence and condition of boundary and perimeter security such as fences
- Physical security of buildings and the ability to resist forced entry
- Areas where service users, staff and the public may be vulnerable to attack

CCTV and security system integration

Designing a system to address all the elements identified by a Risk Assessment often requires integration of additional security systems. Integration offers the ability to interlink the outputs and control systems at a central monitoring station. This may be at an internal hospital security station or at an external monitoring station compliant with the requirements of the emergency services. CCTV delivers much better value when deployed as part of an integrated security system.

CCTV supports the following systems by enabling visual verification of alarm activation, access activity or any other alerted event:

- **Access control**
    - Audio entry systems
    - Number keypad entry systems
    - Biometric fingerprint readers entry systems
    - Swipe cards/fobs ('token') entry systems
        - Includes 'binary' systems where two complementary fobs need to be presented, such as mother & baby tags for maternity units
- **Alarm systems**
    - Intruder alarms
    - Fire alarms
- **Sound monitoring**
- **PA systems to warn trespassers off before committing intrusion offences**
- **Gates and barriers**
- **ANPR (Automatic Number Plate Recognition) vehicle identification**

One key advantage is verification of fire and intruder alarm activation. Sensors on alarm systems may go off in response to things other than fire or intrusion; animals and bad weather are just two common causes of false activation.

Verification of alarm activation with visual information from CCTV systems eliminates false activations and helps emergency service response to be correctly prioritised. Wireless, IP-based CCTV systems provide greater safety for security personnel. Real-time camera images may be viewed on mobile devices equipping first responders with live, real-time video and are able to understand exactly what to expect when investigating a dynamic situation.

SUMMARY

Why trust iC2 on CCTV compliance in your hospital?

iC2 is a leading mid-market security systems provider and was established in 2001. The business is owned and managed by a team with a collective experience of over 100 years in the electronic security business. iC2 holds CCTV and security accreditations with the National Security Inspectorate (NSI) and the British Standards Institute (BSI).

Whether the requirement is solely for CCTV, or for fully integrated systems, iC2 provides the consultancy led services to specify, supply, install and support a full range of integrated electronic security solutions. This includes HD CCTV, Wireless CCTV, ANPR (Automatic Number Plate Recognition), Remote Monitoring, Access Control, Gates & Barriers, PA Systems, Fire Alarms and Intruder Alarms.

The advent of greater regulatory control makes it an imperative for hospital trusts and the wider adult social care system to take control of CCTV and integrated security system compliance obligations.

iC2 offers a complete compliance service tailored to the needs of each hospital site:

- iC2 works with internal hospital security, buildings and facilities management and operational teams to consult or provide selected elements of CCTV and security services
- iC2 provides a complete range of outsourced services to NHS trusts to specify, supply, install, operate, monitor and fully support high quality CCTV and integrated security solutions

A prestigious client list including luxury international boutique brands, top flight sporting venues, retail developments and educational and social environments demonstrates how solutions are deployed to meet a variety of requirements.

From deterring theft of high value luxury goods, to sports fan and public safety and child protection, solutions are deployed to meet a range legitimate purposes for which they are appropriate and fit for purpose.

REFERENCES AND FURTHER READING

Surveillance Camera Code of Practice
Home Office; 2013

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

In the picture: A data protection code of practice for surveillance cameras and personal information
ICO; CCTV Code of Practice; 2014

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Appropriate response: A guide to security system integration, monitoring and verification
iC2 CCTV and Security Specialists (UK) Ltd

www.ic2cctv.com/pdfs/iC2-integration-verification-guide.pdf

5 ways to get locked up with electric gates
iC2 CCTV and Security Specialists (UK) Ltd

www.ic2cctv.com/wp-content/uploads/2015/05/iC2-5-ways-locked-guide.pdf

iC2 DESIGN INSTALL PROTECT

T: 020 3747 1800

E: info@ic2cctv.com

W: www.ic2cctv.com

About Us

Keeping you safe and secure at all times

iC2 provide you with innovative solutions tailored to you and your sector. We are London-based with a national team of surveyors and engineers that work closely with our clients throughout the UK and internationally.

Our unique consultative approach allows us to tailor bespoke systems to your individual requirements, ensuring that your operational requirements are met.

We appreciate the need to demonstrate the best value to you every time and as a technology-led company, you can expect our cutting-edge and ground-breaking approach to serve your needs for many years to come.

Please feel free to contact us to discuss any requirements you may have. We are happy to give you impartial advice, should you have any queries.