CCTV (closed circuit television) Policy

Date drafted: 4 May 2022
Date review due: 3 May 2025 at the latest

CCTV is installed within the reception area inside the building at Alexandra Surgery.
The images recorded includes people and are considered personal data.
This data is controlled according to the relevant provisions in the Data Protection Act.

INTRODUCTION

This policy and the accompanying procedures explain the purpose, use, and management of the Closed Circuit Television (CCTV) installation at the premises used by Alexandra Surgery. The Practice prioritises the safety and security of all patients, staff and visitors and aims to provide environments that are safe and secure.

POLICY STATEMENT

The purpose of the CCTV installation is for:

- The protection of staff, patients, visitors, and the assets of Alexandra Surgery.
- The prevention, investigation and detection of crime.
- The apprehension and prosecution of offenders (including the use of images/data as evidence in criminal / civil proceedings).
- The monitoring of the security of premises.
- Investigation into a missing or vulnerable person.

The principles of the policy are that:

- Individuals' rights are respected and protected.
- The installations are operated fairly and within the law.
- The CCTV system is operated for the purposes for which it was set up.
- The recorded material/data stored is fairly and lawfully processed.
- The recorded material/data is adequate, relevant and not excessive for the purposes.
- That recorded material/data is accurate, securely stored, and not kept for longer than is necessary.

The aim of this policy is to ensure (so far as is reasonably practicable) that any system installed and operated on its premises complies with regulatory requirements, national standards and codes of practice. The Organisation's Digital Recording systems form part of the overall security management measures aimed at achieving compliance and delivering best practice in the interests of delivering safe services and providing a safe and secure environment.

Alexandra Surgery's Health and Safety policy sets out the roles and responsibilities of all staff. Additional responsibilities to enable the effective management and use of the Organisation Digital Recording systems are detailed in this policy. To assist in the provision of safe and secure environments at Alexandra Surgery the use of CCTV is used across its services. This policy applies to all members of staff employed by Alexandra Surgery, locum/bank staff and agency staff, volunteers as well as contractors and any others working on behalf of Alexandra Surgery.

DEFINITIONS

CCTV

Closed-circuit television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. They are primarily for surveillance and security purposes.

GDPR

General Data Protection Regulations 2016 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.

Senior Information Risk Owner (SIRO)

The SIRO is the Chief Executive and they are familiar with information risk and the organisations response to risk. The SIRO takes ownership of the organisation's information governance policy including all information risk and acts as an advocate on the Board.

Purposes of the CCTV system

In accordance with the legislative requirements the registered purpose of CCTV is for the prevention and detection of crime, the safety and security of public, patients, visitors and staff. The use of a CCTV system must take into account its effects on individuals and their privacy, with regular reviews to ensure its use remains justified. The CCTV system is not installed for the purposes of recording conversations. Alexandra Surgery will ensure that CCTV is sited in areas where it is only monitoring for the purposes outlined above and not positioned in areas where it would be considered private e.g. changing rooms and toilets.

The system will be operated in accordance with the requirements and articles of the Human Rights Act 1998 and the GDPR 2016. The system will be operated fairly, within the law, and only for the purposes for which it has been established and are identified within this policy. The operation of the system will also recognise the need for formal authorisation of surveillance as required by the Regulation of Investigatory Powers Act 2000, in particular part 2 of this Act.

The information commissioner's office (ICO) must be notified of the purpose(s) of the scheme operating. Registration with the ICO is carried out by the Practice Manager. The system will be maintained on behalf of Alexandra Surgery by Alexandra Surgery's Information Governance lead Abhi Sivananthan and IT lead Dr Chenthuran Umapathee to ensure compliance with the General Data Protection Regulations 2016. The CCTV surveillance system is owned by Alexandra Surgery.

The CCTV system includes cameras inside the practice. The system may be operated up to 24 hours per day, 365 days of the year. The CCTV installation comprises of fixed cameras, signs, recording and playing equipment and data. Recorded material/data means any material recorded by the installation. It should be noted that all recorded material/data are the property of Alexandra Surgery. Staff, patients and any visitors to Alexandra Surgery practice premises are informed about the use of CCTV.

All release of information will be in accordance with the ICO registration and legislative requirements.
A data protection exemption relates to the disclosure of information for the purposes of:

- The prevention, investigation, detection or prosecution of criminal offences.
- The execution of criminal penalties, including the safeguarding against and the prevention of threats to public security
- A serious or significant nature such as safeguarding or a missing vulnerable persons.

CCTV footage retention and viewing

Footage that is not required for the purpose for which the equipment is being use must not be retained in an identifiable form for longer than necessary, in compliance with GDPR principles 5 (Article 5 e). In order to ensure compliance with data protection principles the data controller Alexandra Surgery and system operators will ensure that footage is not retained for longer than 30 days, unless it is required for evidential purposes in legal or other investigation proceedings. Footage retained for evidential purposes will be removed from the system and retained in a secure place to which access is controlled. It is important to ensure that access to and security of the images is controlled in accordance with the requirements of the GDPR and for law enforcement purposes (Data Protection Act 2018 – and Law Enforcement Directive 2017). It should be noted that a full risk assessment will be carried out if footage is retained outside of the 30 day retention period.

Alexandra Surgery's standard retention period is 30 days unless the footage is justifiably marked and retained as 'EVIDENCE.' The Practice Manager must ensure that each site has a stock of blank memory sticks and the facility for playback if required. The ability to review recorded and live images is limited to authorised staff personnel only, namely: Abhirami Sivananthan Practice Manager and CCTV maintenance engineers. Once the image retention period has expired, the footage itself is removed or erased automatically from the system.

Disclosure of images to third parties

It is important to ensure that access and disclosure of CCTV footage is restricted or carefully controlled not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should they be required for evidential purposes. If disclosure is requested for any of the registered purposes in 4.8, Alexandra Surgery as the data controller must satisfy themselves that:

- The reason(s) or purposes(s) for the disclosure are compatible with the reason(s) or purpose(s) for which the footage was originally obtained.
- Access is restricted to authorised persons who need to have access in order to achieve the purpose(s) of using the equipment.
- All access to images must be documented.
- Access to images must only be allowed for a lawful purpose and prescribed circumstances and must be authorised by the Practice Manager, with notification sent to the SIRO.

Disclosure as per 4.16 will be considered if the third party is either:

- A law enforcement agency, such as the police, where the images recorded would assist in a specific criminal enquiry, or where the images are to be used to assist law enforcement agencies in the return of patients who take unauthorised leave of absence under the Mental Health Act 1983, or relevant criminal justice legislation.
- Prosecution agencies.
- Relevant legal representatives.

Under chapter 3, Article 23, GDPR 2018 the Data Controller may grant relevant authorities as indicated in 4.17 access to personal CCTV data without the consent of the data subject. This is not an automatic right of access to information. The data controller can assess the merits of requests and decide whether or not to apply chapter 3 requests. If footage meets the criteria for release, then the Practice Manager will ensure that it is burned onto a memory stick. Two copies will be made (one for the third party and one for THE PRACTICE) and then sent to the Information Governance Lead Abhi Sivananthan (also Surgery Security lead) or Dr Athee Sivananthan who will release it to the requestor.

All requests for disclosure to a third party must be made by official letter. Please note that this letter must be signed off by someone of inspector rank or above if it is being submitted by the Police.

Access to images as part of a Subject Access Request (SAR)

Access to personal data as part of a SAR will be handled by Alexandra Surgery Governance Team and all such requests must be submitted to Practice Manager Abhi Sivananthan.

Due to the cost implication of editing footage (to ensure redaction of third party data) Alexandra Surgery will be unable to release CCTV footage as part of a SAR. The requestor will be informed of this in writing within the 30 day time limit by the Alexandra Surgery Governance Team. A viewing of CCTV footage will be offered instead if within the time limit in an area made private for the purposes of viewing footage only as recommended by the ICO. If the requestor refuses the offer of viewing the footage then Alexandra Surgery may produce a report or transcript of the recording. However this should not be offered instead of viewing.

Alexandra Surgery Governance Team will ensure a log is kept of all requests and the resulting decision. All requests for access to images as part of a SAR must be made by official letter. Your request will be assessed to ensure that your request falls within the scope of Chapter 3 of the regulations and is proportionate to the reason the information is being requested. There is no statutory time limit for responses to requests made under Chapter 3.

All authorised releases of footage will be retained on a log kept by the Practice Manager. This must include the following information:

- Date and time access was requested.
- Date of disclosure.
- Identification of third party.
- Reason for allowing or declining disclosure.
- Extent of information disclosed.

A formal record for all SAR and third party requests and will detail whether it has been granted or denied.

In addition to the right of access, an individual also has the right to ask Alexandra Surgery to stop processing personal data where this is likely to cause substantial and unwarranted damage to him or her. Any such requests should be submitted in writing to Alexandra Surgery SIRO. Upon receipt of such a request Alexandra Surgery has 21 days in which to respond with its decision. All decisions should be documented and a record should be kept of all requests and the response to those requests.

REPORTING

All requests to access CCTV will be monitored and reported by the Practice Manager. Spot check audits may be carried out to ensure that erasure of images are being carried out in accordance with this policy.

ROLES AND RESPONSIBILITIES

Practice Partners

Alexandra Surgery partners have overall accountability for the organisation's ability to meet the policy requirements. Alexandra Surgery is the identified Data Controller for all systems operating on its premises and Alexandra Surgery act on behalf to process any requests made under this policy. Alexandra Surgery is responsible for all cameras, monitors and data collection and retention processes. Roundwood Surgery uses external companies (Data Processors) to control and maintain its system. All contracts with such companies will include adherence to this policy.

Practice Manager

The Practice Manager is the responsible person for the management and operation of the system, with nominated individuals given authority to operate the system in strict compliance with this policy. The Practice Manager will ensure that the CCTV equipment performs properly, that images are as clear as possible and that time and date stamps are accurate and checked regularly.

Line Managers

Line Managers are responsible for ensuring that their staff are aware of and adhere to this policy.

All Staff

All staff are responsible for ensuring that they are aware of the requirements of this policy and for ensuring that they comply with these on a day to day basis. All staff are accountable under the Office of the Information Commissioner's Code of Conduct.

TRAINING REQUIREMENTS

The Practice Manager will receive training on how to utilise the CCTV system and cascade it to other senior members of staff on a need to know basis.

Alexandra Surgery will provide appropriate training for all staff to cover awareness of data protection and information security matters, the CCTV policy and any associated operational procedures.

MONITORING

This policy and its operations will be subject to regular reviews and audits, no less than every three years.

REFERENCES

- General Data Protection Regulations 2016
- The Freedom of Information Act 2000
- Data Protection Act 2018
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000