Dr. Neil Potter
Dr. Julie Morgan
Dr. Richard Estall

Church Green
Marden
Tonbridge
Kent TN12 9HP
Tel:01622 831257

CCTV POLICY AND CODE OF PRACTICE

Introduction

Closed circuit television (CCTV) is installed at the practice premises for the purpose of staff, patient and premises security. Cameras are located at various places on the premises, and images from the cameras are recorded.

The use of CCTV falls within the scope of the Data Protection Act 2018. In areas of surveillance, signs will be displayed prominently to inform individuals that CCTV is in use.

In order to comply with the requirements of the 2018 Act, data must be:

- Fairly, lawfully and transparently processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in accordance with individuals' rights
- Secure
- Accountable

Data Protection Statement

1. Marden Medical Centre are the Data Controllers in accordance with Data Protection Legislation.
2. CCTV is installed for the purpose of staff, patient and premises security.
3. Access to stored images will be controlled on a restricted basis within the practice.
4. Use of images, including the provision of images to a third party, will be in accordance with the practice's Data Protection registration.
5. CCTV may be used to monitor the movements and activities of staff and visitors whilst on the premises.
6. CCTV images may be used where appropriate as part of staff counselling or disciplinary procedures.
7. External and internal signage are displayed on the premises and in the practice leaflet stating of the presence of CCTV, and indicating the names of the Data Controllers and a contact number during office hours for enquiries.

Retention of Images

Images from cameras are recorded on the hard drive on the computer system. Where recordings are retained for the purposes of security of staff, patient and premises, these will be held in secure storage, and access controlled. Recordings which are not required for the purposes of security of staff, patient and premises, will not be retained for no longer than 3 weeks at a time.

The system has not an automatic power backup facility which may operate in the event of a main supply power failure.

Access to Images

It is important that access to, and disclosure of, images recorded by CCTV and similar surveillance equipment is restricted and 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 the images be required for evidential purposes.

Access to Images by Practice Staff

Access to recorded images is restricted to *the Data Controllers*, who will decide whether to allow requests for access by data subjects and/or third parties (see below).

Viewing of images must be documented as follows:

- The name of the person removing from secure storage, or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The name(s) of the person(s) viewing the images (including the names and organisations of any third parties)
- The reason for the viewing
- The outcome, if any, of the viewing
- The date and time of replacement of the recordings

Removal of Images for Use in Legal Proceedings

In cases where recordings are removed from secure storage for use in legal proceedings, the following must be documented:

- The name of the person removing from secure storage, or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The reason for removal
- Specific authorisation of removal and provision to a third party
- Any crime incident number to which the images may be relevant
- The place to which the recordings will be taken
- The signature of the collecting police officer, where appropriate
- The date and time of replacement into secure storage of the recordings

Access to Images by Third Parties

Requests for access to images will be made using the 'Application to access to CCTV images' form (which is at **Appendix 1**).

The Data Controller will assess applications and decide whether the requested access will be permitted. Release will be specifically authorised. Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances. For example, in cases of the prevention and detection of crime, disclosure to third parties will be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- Prosecution agencies
- Relevant legal representatives
- The press/media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented as above.

Disclosure of Images to the Media

If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of other individuals must be disguised or blurred so that they are not readily identifiable.

If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the data controllers
- The written contract makes the security guarantees provided by the editing company explicit

Access by Data Subjects

This is a right of access is provided by the Data Protection Act 2018. Requests for access to images will be made using the 'Application to access to CCTV images' form (which is at **Appendix 1**). The requestor needs to provide enough

information so that they can be identified in the footage, such as a specific date and time, proof of their identity and a description of themselves. Any footage provided may be edited to protect the identities of any other people.

The Practice may charge a reasonable fee to provide the footage if the request to see a copy of the personal information is deemed unfounded or excessive.

Procedures for Dealing with an Access Request

All requests for access by Data Subjects will be dealt with by the Practice Manager. The data controller will locate the images requested. The data controller will determine whether disclosure to the data subject would entail disclosing images of third parties.

The data controller will need to determine whether the images of third parties are held under a duty of confidence. In all circumstances the practice's indemnity insurers will be asked to advise on the desirability of releasing any information.

If third party images are not to be disclosed, the data controllers will arrange for the third party images to be disguised or blurred. If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the data controllers
- The written contract makes the security guarantees provided by the editing company explicit

The practice manager will provide a written response to the data subject within **30** days of receiving the request setting out the data controllers' decision on the request.

A copy of the request and response should be retained.

Complaints

Complaints must be in writing, and addressed to the practice manager. Where the complainant is a third party, and the complaint or enquiry relates to someone else, the written consent of the patient or data subject is required. All complaints will be acknowledged within 3 days, and a written response issued within 10 days.

Date of review February 2020 MJBournes

shared drive: practice policies&forms

>>> Continues Below >>>

Appendix 1
Data Protection Act - Application for CCTV Data Access

ALL Sections must be fully completed. Attach a separate sheet if needed.

Name and address of Applicant	
Name and address of "Data Subject" – i.e. the person whose image is recorded	
If the data subject is not the person making the application, please obtain a signed consent from the data subject opposite	Data Subject signature……
If it is not possible to obtain the signature of the data subject, please state your reasons	
Please state your reasons for requesting the image	
Date on which the requested image was taken	
Time at which the requested image was taken	
Location of the data subject at time image was taken (i.e. which camera or cameras)	
Full description of the individual, or alternatively, attach to this application a range of photographs to enable the data subject to be identified by the operator	
Please indicate whether you (the applicant) will be satisfied by viewing the image only	

A response will be provided as soon as possible and in any event within **30** days.

The Practice may charge a reasonable fee to provide the footage if the request to see a copy of your personal information is deemed unfounded or excessive.

PRACTICE USE ONLY	PRACTICE USE ONLY
Access granted (tick)	
Access **not** granted (tick)	Reason for not granting access:
Data Controller's name: Signature: Date:	