Claypath and University Medical Group

CCTV Policy

DOCUMENT CONTROL

A. Confidentiality Notice

This document and the information contained therein is the property of the Claypath and University Medical Group.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from the Claypath and University Medical Group.

B. Document Details

Classification:	
Author and Role:	Sarah Lambert
Organisation:	Claypath and University Medical Group
Document Reference:	CCTV Policy.doc
Current Version Number:	1
Current Document Approved By:	
Date Approved:	

C. Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1	10.05.2021	Sarah Lambert		

Claypath and University Medical Group

CCTV Policy

1. Introduction

The Practice complies with the legal obligations of the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR'). The Practice gathers and uses data about workers, employees and consultants, both to manage our relationships with these individuals and in the course of conducting our business.

This Data Protection Policy applies to current and former employees, workers, volunteers, consultants, apprentices, patients and members of the public ('data subjects').

The Practice is a 'data controller' for the purposes of these individuals' personal data, and is responsible for determining the purpose and means of the processing of that data.

The CCTV footage generated from cameras located both at reception and within the practice car park will be retained for no longer than 45 days. The purpose of the CCTV cameras is to protect staff and property should an incident occur that causes harm to either.

This policy has been created to be fully compliant with GDPR and the 2018 Act. Where any conflict arises between those laws and this policy, the Practice will comply with the 2018 Act and the GDPR.

This policy is separate from data subjects' contracts of employment (or contract for services) and can be amended by the Practice at any time.

2. The Six Data Protection Principles

The Practice processes personal data in accordance with the six Data Protection Principles for GDPR identified by the ICO, which means it will:

- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be processed fairly, lawfully and transparently;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- be collected and processed only for specified, explicit and legitimate purposes;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

3. Personal Data

'Personal data' is defined as information relating to a living person ('data subject') that can be used to identify them on its own, **OR** in combination with other information likely to be collected by the Practice. This applies whether the information is stored physically, electronically, or in any other format.

For the purpose of this policy the personal data in question is CCTV footage recorded on practice premises from the car park and main reception desk.

A limited number of people have access to the CCTV footage – the General Manager and Assistant General Manager.

4. CCTV Code of Practice

The Surveillance Camera Commissioner has published 12 principles for organisations using CCTV. Details of how we comply with these principles can be found at Appendix 1.

5. Data Protection Impact Assessment

A data protection impact assessment has been completed for the use of CCTV at the practice and can be found at Appendix 2.

In summary the benefits to the practice for installing CCTV are:

- deterrent for building damage, damage to vehicles or aggressive behaviour
- it provides a record of evidence should an incident occur to support the practice in taking action and/or alerting authorities

The risk assessments undertaken within that impact assessment concerning recording footage highlighted a *possible* likelihood of harm, *minimal* severity of harm with a *low* overall risk.

A risk was identified in recording personal activities but this can be minimised by not routinely reviewing the camera footage and only referring to it if an incident occurs and to check that the equipment is functioning as it should. This eliminated the risk leaving a low residual risk.

The angle of the camera is set to record the minimum possible information required to capture areas under surveillance and to retain the privacy of as many individuals as practically possible.

6. When the Practice Might Process CCTV Footage

The Practice is required to process individuals' personal data in various situations during their recruitment, employment (or engagement) and even following termination of their employment (or engagement) for reasons including but not limited to:

- Assisting the authorities in their enquiries
- Assisting the Practice Manager when investigating an incident

9. Handling Data Breaches

The Practice has robust measures in place to minimise and prevent data breaches from occurring. Should a breach of personal data occur, the Practice will make note of the relevant details and circumstances, and keep evidence related to that breach. All data breaches will be reported to the practice Data Protection Officer. If the breach is likely to result in a risk to the rights and freedoms of individuals then the Practice will notify the Information Commissioner's Office within 72 hours. All affected patients will also be informed.

If you are aware of a data breach you must contact Gillian Bevan, General Manager, or Tracy Watson, Deputy General Manager, immediately and retain any related evidence to the breach that you may have.

10. Subject Access Requests

Data subjects can make a Subject Access Request ('SAR') to access the information the Practice holds about them. This request must be made in writing. If you receive a SAR you should forward it immediately to Cynthia Dunn, Medicals Administrator, who will prepare a response.

For the purposes of CCTV footage, it may take longer than usual to process the request because CCTV footage would need to be reviewed, redacted and assessed in case it breached the confidentiality of another party by sharing it. Should this be the case then you would be notified accordingly.

The ICO advises:

"When disclosing surveillance images of individuals, particularly when responding to subject access requests, you need to consider whether the identifying features of any of the other individuals in the image need to be obscured."

GMC guidance on confidentiality also needs to be considered and this outlines that to disclose personal information, one of 4 situations must apply:

- The patient has provided consent
- The disclosure is of overall benefit to a patient lacking capacity
- The disclosure is required by law
- The disclosure can be justified in the public interest

If you wish to make a SAR in relation to your own personal data this should be made in writing to Gillian Bevan, General Manager. The Practice will respond within one month unless the request is complex or numerous – if this is the case, then the Practice will need more time to complete the request, and can extend the response period by a further two months.

A Subject Access Request does not incur a fee, however, if the request is deemed to be manifestly unfounded or excessive then the Practice is entitled to charge a reasonable administrative fee, or refuse to respond to the request.

11. Data Subjects' Rights

In most situations the Practice will not rely on your consent as a lawful ground to process your data. If the Practice does request your consent to the processing of your personal data for a specific purpose, you have the right to decline or withdraw your consent at a later time. To withdraw consent, you should contact Gillian Bevan, General Manager.

Data subjects have the right to information about what personal data the Practice processes, how it is processed and on what basis. They have the right to:

- access their personal data via a Subject Access Request.
- correct any inaccuracies in their personal data. To do so please contact Gillian Bevan, General Manager.
- request that we erase their personal data in the case that the Practice was not entitled under the law to process it, or the data is no longer needed for the purpose it was collected. In this case please contact Gillian Bevan, General Manager.
- object to data processing where the Practice is relying on a legitimate interest to do so and the data subject contends that their rights and interests outweigh those of the Practice and wish us to stop.
- object if the Practice processes their personal data for the purposes of direct marketing.
- receive a copy of their personal data and transfer their personal data to another data controller. The Practice will not charge for this and will in most cases aim to do this within one month.
- with some exceptions, they have the right not to be exposed or subjected to automated decision-making.
- be notified of a data security breach (within the appropriate timescales) concerning their personal data.

If you have a complaint about how your data is processed that cannot be resolved with the

Practice, you have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office at www.ico.org.uk.

Where your personal data is being corrected or erased, or the Practice is contesting the lawfulness of the processing, you can apply for its use to be restricted while the application is made. In this case please contact Gillian Bevan, General Manager.

Resources

Information Commissioner's Office website
www.ico.org.uk

NHS Employers guidance on criminal checks
www.nhsemployers.org/your-workforce/recruit/employment-checks/criminal-record-check

Records Retention Policy

CCTV guidance from Information Commissioners Office
https://ico.org.uk/for-organisations/guide-to-data-protection-1998/encryption/scenarios/cctv/

Appendix 1

CCTV Code of Practice and how we comply:

The surveillance camera commissioner has published 12 principles for organisations using CCTV and in doing so requires organisations to be able to answer the following questions. This give assurance that we are actively following the 12 principles in the way we operate our CCTV system.

• *What's your system for?*

Security of the car park and security for staff on the front facing patient desk after a series of safety incidents concerning aggressive members of the public. The CCTV system has been deemed necessary to safeguard staff and other members of the public when using our premises.

• *Do you review its use?*

Use of the CCTV usage will be reviewed annually in line with CCTV policy reviews or before if an incident arises that suggests we may need to review how we use it earlier

• *Have you carried out a privacy impact assessment?*

Yes and this is appended to our CCTV Policy

• *Do you publish your privacy impact assessment?*

Yes this is available to view on the practice website (check)

• *Do you have signage in place to say surveillance is taking place?*

Yes we have a notice up at reception explaining that CCTV is in operation at reception and in the patient car park for security purposes (DO)

• *Is there a published point of contact for people to raise queries or complaints with?*

Yes the contact at the practice is Tracy Watson, Assistant General Manager

• *Who's responsible for your system?*

The practice are responsible for the maintenance and upkeep of the CCTV system.

• Are your staff aware of their responsibilities?

The CCTV Policy has been shared with staff.

• *Do you have clear policies and procedures in place?*

Yes

• *Do your staff know what your policies and procedures are?*

Yes, the CCTV Policy and attachments have been circulated to all staff

• *How long do you keep images/information?*

We use the Amazon NEST camera system in conjunction with wi fi connections from the 3 network. Images are held for 45 days in total which is a reasonable amount of time to be able to investigate incidents should this be necessary.

• *How do you make sure images/information is deleted once they're no longer needed?*

The system does not hold information after 45 days and the information is then auto deleted from the NEST software.

• *Do you have a policy on who has access to the stored information?*

Yes this information is stated in the CCTV Policy and access is limited to senior members of staff

• *Do you have a policy on disclosure of information?*

Our Subject Access Request Policy sets out how information may be disclosed to members of the public on request however; we are required by law to assist the authorities by disclosing information from CCTV to assist in crime prevention or other investigations as needed.

• *Do you follow any recognised operational or technical standards?*

Yes and these are outlined in our policy. We have undertaken an impact assessment and ensured that we are compliant with the advice given by the Information Commissioner on the ICO website.

• *Do you make sure that the images captured by your system are caught securely?*

Yes they are caught and stored via a private 3 wi-fi network which is held separate to the practice. The software is stored on specified practice mobile phones via the NEST app.

• *Are only authorised people given access to the images?*

Yes. Only some senior members of staff are able to access the images.

• *Do you evaluate your system regularly to make sure it's still required?*

Yes as part of our annual review or before if needed.

• *Could there be an alternative solution to a surveillance camera system?*
No

• *Can the criminal justice system use the images and information produced by your surveillance camera system?*

Yes we would work with the authorities if needed to satisfy their work.

• *Do you have a policy on data storage, security and deletion?*

Yes

• Do you use any specialist technology such as ANPR, facial recognition, Body Worn Video (BWV) or remotely operated vehicles (Drones)?

No.

• *Do you have a policy in place to ensure that the information contained on your database is accurate and up to date.*

See CCTV policy

Claypath DPIA for CCTV

Appendix 2

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
CCTV installation has been agreed as a result of prior damage to cars in car parks and aggression experienced by staff from patients and members of the public. A camera will be installed to the reception area at the front desk and to the side of the building for monitoring the car park. NEST cameras will be used, and CCTV footage will be stored for 45 days and a standalone wi fi connector via 3 will be used.

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?
Data will be collected from the camera and stored on NEST software for 45 days and will then be deleted. Data will be used/reviewed for security monitoring purposes only in the areas of reception and the external car park.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
The cameras will cover the reception area and practice car park only. The camera will record continuously in the car park and reception areas and will record general information inly, holding it for 45 days before deletion. All practice patients and staff may be affected and while it is not intended to store information in relation to criminal offenses, it may if an incident occurs. The cameras aim to provide a deterrent.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
We have based our policy and supporting documentation on best practice – referring to guidance from the Information Commissioners Office (ICO) and the 12 principles set out in the Surveillance Camera Commissioners guidance. Recording may include children or vulnerable persons; however, the system is not novel, and it is not intended to review images routinely. Images will only be reviewed where an incident of concern has been reported to the practice and that may need subsequent support from the relevant authorities. *The CCTV Policy once completed will be shared with the patient participation group of the practice for further comment.*

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?
The only benefits to the practice for installing CCTV are: • Deterrent for building damage, car damage, aggressive behaviour • A record of evidence should an incident occur to support the practice in acting and/or alerting authorities

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
We have researched best practice within the ICO website and tailored our documentation accordingly. We will discuss the installation of CCTV with our Patient Participation Group to obtain their views and feedback.

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Risk of recording personal and/or private activity of citizens unintentionally	Remote, Possible, or probable	Minimal, significant, or severe	Low, medium or high

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA