Barnsley Hospital NHS
NHS Foundation Trust

‘Hospital Eyes’
CCTV Code of Practice for Operational Procedures

Revised February 2023

Contents

- Introduction
- Purpose of the Scheme
- Ownership
- Partners
- Changes of The Code
- Objectives of The Code
- Responsibility of the Scheme
- Getting in touch
- Governing Legislations
- Installation of Cameras
- Equipment Specification
- Maintenance
- Time and Date
- Staff
- Contractors
- Visitors
- Recording Images and Data Retention
- Disclosure to Subject Access and Third Parties
- Disclosure to South Yorkshire Police
- Disclosure to Non-Internal Partners
- Audit and Review

Introduction

The Hospital Eyes CCTV service provides site wide CCTV cameras and Body Worn Video and central monitoring station security services 24 hours per day, 365 days per year. The aim of the service is to prevent, detect and reduce crime and Anti-Social Behaviour (ASB), improve public safety and provide reassurance. The Trust Surveillance Camera Policy fully explains our approach to public surveillance.

CCTV and body worn video (BWV) used by security and clinical staff is considered to be tools which the public support, although they expect it to be used responsibly with effective safeguards in place. Maintaining public trust and confidence in the Hospital Eyes CCTV system is essential if its benefits are to be realised and the Trust aims of building safer, stronger cohesive communities is to be achieved.

Purpose of the scheme

Similar to the Policing by Consent of the Public; we must also strive to achieve Surveillance by Consent of the Public. They expect the CCTV and both Body Worn Video systems (Security & Clinical) to be used in keeping with the reasons initially established. Those are: To prevent, detect and deter crime and disorder and Anti-Social Behaviour (ASB); to improve public and staff safety and provide public reassurance alongside policy issues.

Ownership

The CCTV and Body Worn Video systems are owned by Barnsley Hospital NHS Foundation Trust. Operated in partnership with G4S Security Solutions.

Barnsley Hospital is the Data Controller.

Partners and users of the scheme

Through its partnership arrangements, Service Level Agreements and Data Sharing Codes of Practice Hospital Eyes allow selected services to have restricted access to some of its CCTV systems. These partners are:

South Yorkshire Police

Yorkshire Ambulance Service

South Yorkshire Fire and Rescue

Barnsley Metropolitan Borough Council

All partners that have access to the Hospital Eyes system are required to comply with this Code of Practice.

This Code of Practice (The Code) replaces all existing codes of practice in relation to the Hospital Eyes CCTV service. This revised code, builds on previous guidance issued by the Information, and Biometric and Surveillance Camera Commissioners and reflects changes in

the use of CCTV and Body Worn Video; it is to be read in conjunction with current Trust policies.

Changes to the Code

The details of The Code will be reviewed annually and any major changes will only be made after appropriate consultation within the management team and subsequent approval by the Head of Business Security.

This code of practice details the guiding principles of the CCTV and Body Worn Video systems for monitoring staff and partners benefiting from the use of the Hospital Eyes CCTV and Body Worn Video, and also covers the governance requirements and the management of the information derived from camera equipment.

Objective of the Code

The objective of the code of practice is to ensure good practice standards are adopted by the Hospital Eyes surveillance camera service and partners who benefit from the use of the Hospital Eyes CCTV systems and equipment.

Responsibility for the scheme

Overall responsibility of the Hospital Eyes System sits with the Head of Business Security who is the Trust's Strategic Lead for Surveillance Camera Systems and allied Information.

Data Controller responsibilities for the Hospital Eyes system sits with the Trust Business Security Specialist.

Day to day responsibility for surveillance camera issues sits with the G4S site manager.

All administrative issues relating to CCTV or (Clinical/Security) Body Worn Video sits with the Business Security Support Officer.

Getting in touch

All comments, complaints or enquiries relating to CCTV, BWV and Control Room Systems should be directed through process found at the hospitals service user feedback.

Day to day queries should be directed to the G4S Security Site Manager through Hospital.Eyes@nhs.net or by telephoning 01226 431889.

Further information and surveillance camera Subject Access Request data request forms can also be found at www.barnsleyhospital.nhs.uk

Governing Legislation

In operating the systems the Trust and its partners must pay due regard to the following legislation and Codes of Practices:

The Data Protection Act 2018

General Data Protection Regulations 2018

The Human Rights Act 1998

The Regulation of Investigatory Powers Act 2000

The Protection of Freedoms Act 2012

The Information Commissioner's Codes of Practice

The Surveillance Camera Commissioner's Codes of Practice

Barnsley Hospital NHS Foundation Trust Data and Information Sharing Protocols

All managers, users and operators of the system will be responsible for complying with the Code. They also have a responsibility to pay due regard to the governing legislation and Codes of Practice above.

Surveillance camera data (or captures) may be released to third parties, members of the public and other public bodies who can demonstrate a legitimate reason for access as in accordance with the General Data Protection Regulations and Data Protection Act. More information on the process and release of data can be found at www.barnsleyhospital.nhs.uk

Installation of additional cameras

The installation of additional permanent or moveable CCTV cameras operated through the Business Security CCTV Service will be approved by the Trust Head of Business Security.

All requests will be subject to a robust assessment process and will need to satisfy the following points:

That there is a pressing need for a camera at the location;

That other solutions have already been attempted or considered to resolve the pressing need;

That a Privacy Impact Assessment has been completed;

That the proposed site will address the pressing need;

That all technical standards are satisfied;

That consultation has been undertaken;

That there is appropriate signage in place;

That the camera and the pressing need will be reviewed annually;

That there is appropriate funding in place for the installation of the camera;

That there is appropriate funding in place for the on-going annual support, maintenance and monitoring of the camera.

All requests for additional cameras should be made in writing to the Trust Healthcare Security Managers, who will then support the requestor in processing through the process and reviewing the options available to them.

Equipment Specification & Location

The Hospital Eyes CCTV system is intended as a Public Space monitoring tool for the purposes stated in The Code.

All Hospital Eyes CCTV cameras will be identified by appropriate signage, detailing the owner of the camera, the purpose of the system and a contact telephone number.

CCTV equipment needs to be of a recognised standard in keeping with the existing equipment and systems linked to Hospital Eyes as well as of an appropriate standard to meet law enforcement and evidence requirements.

Only authorised equipment can be connected to the Hospital Eyes system on approval.

The deployment of CCTV equipment must protect the rights of the individual as outlined within the Human Rights Act.

The Hospital Eyes system includes technical equipment to enable privacy zones to be established where a camera captures images from a private property. Only in emergency circumstances without the required written authority would the G4S site manager be authorised to remove the privacy zones.

The Hospital Eyes CCTV system uses both permanent and moveable CCTV cameras. The quality standard of the images obtained from the cameras ensures high quality clear pictures.

Maintenance

The maintenance and installation of all the equipment connected to Hospital Eyes system is covered by a single maintenance contract and all logs of maintenance will be maintained in accordance with the General Data Protection Regulations and Data Protection Act.

Only authorised contractors provided and approved through the corporate contract are permitted to work on or have access to the equipment and network connected to the Hospital Eyes system.

All cameras will be checked for faults on a twice daily basis, all faults will be reported through the maintenance and support provider, who will log and respond as per the current contract for maintenance.

Time and Date

The Hospital Eyes system is automatically attuned for time and date through a time syncing transmission which is managed through a recognised international time server.

Accuracy checks of time and day displays are carried out at the commencement of each security team shift. All discrepancies are recorded in accordance with the principles of the General Data Protection regulations and the Data Protection Act.

Staff

Only authorised personnel who have undergone appropriate training are approved to use the Hospital Eyes CCTV equipment. All personnel will hold a current SIA licence for CCTV; this includes the members of the Trust Business Security Unit.

Only authorised personnel may operate equipment within the Security Control office or connected to the Hospital Eyes CCTV system, which has PIN coded electronic access control and there is no public access allowed.

All users of the system have a responsibility to comply with The Code and procedures manuals. They have a responsibility to respect the privacy of the individual and understand and comply with the objectives of the scheme.

Only authorised users may monitor or review images at Hospital Eyes CCTV Control Room or at an authorised connected and restricted access terminal.

All users, contractors and visitors will be required to sign a formal confidentiality declaration that they will treat all data as strictly confidential and that they undertake not to divulge it to any unauthorised person.

Contractors

Hospital Eyes maintains its systems through the annual BFS maintenance contract. Only authorised contractors are given administration level access to the Hospital Eyes system or any equipment connected to it.

All contractors are vetted to an appropriate level and hold professional membership of a nationally recognised professional body.

Visitors

The Hospital Eyes service is a secure and restricted service. The location of the service and all of it equipment is restricted for security and safety purposes.

All visits to the Hospital Eyes system are by appointment only and all visitors must be signed in as accompanied whilst on site.

The Hospital Eyes system is monitored by CCTV at all times and data recorded and retained in accordance with the Code.

Recorded Images and data retention

The CCTV system records data from its cameras 24 hours each day and then stores this data automatically for 31 days.

The Body Worn Video and audio (Reveal & Calla) cameras record when activated by an officer and stores the data via DEMS software for a period of 30 days.

Footage is only kept after this if it has been saved by an operator, who may place it in the secure drive and server area. This may be done if an operator observes an incident whilst monitoring the cameras, if they are advised of an incident by one of the partners such as South Yorkshire Police or if they are made aware of an incident in any other way such as through a telephone call made to the Trust Contact Centre by a member of the public.

Once footage is saved onto the Hospital Eyes server that footage will be reviewed for evidence purposes by the data controller and then either deleted as not of evidence value or saved for a period 7 years to align with NPCC guidance and the NHS retention schedule.

All requests for data will be made through the appropriate procedures as detailed in the Service Level Agreement and ICO's Code of Practice and in accordance with the Data Protection Act. Only requests that are accompanied with the completed documentation will be considered.

Downloading data onto media such as a DVD or data-stick or other data medium from the Hospital Eyes CCTV system shall only be allowed through the Trust Security Office Review Room and through a restricted access designated terminal within Business Security.

The Copyright in all recording will remain the property of BHNFT.

Disclosed data will be provided on an data-stick, DVD, other data medium or cloud based systems, or in certain law enforcement cases password protected hard drive storage and properly documented in accordance with the Data Protection Act. In the interests of security of data and accountability the preferred method of transfer will be via a password protected hyperlink from the cloud server. The password and link will be forwarded under separate and secure email cover.

There is no facility for members of the public or non-partner agencies to attend Hospital Eyes to review data.

All data recorded for evidential purposes will be retained and processed in accordance with the General Data Protection Regulations and the Data Protection Act.

Disclosure Subject Access and Third Party

Disclosure of images from the CCTV and Body Worn Video systems must be controlled and consistent with both the purpose for which the systems were established and General Data Protection Regulations and the Data Protection Act.

All Subject Access and Third Party Requests will be processed through either the G4S Site Manager or if unavailable the Surveillance Camera Duty and Trust Information Governance Manager. Members of staff will not be allowed to view video data directly.

Images must not be released to the media for identification purposes this could only be done by an appropriate enforcement agency in accordance with Police and Criminal Evidence Act 1984.

All requests for data should be submitted in writing on the approval form. This form is available at www.barnsleyhospital.nhs.net. This form explains the process through the Data

Protection Act, including an explanation of the rights of the individual as well as contact address and details of the Information Commissioners Office and all of the required information and identification to process the request.

A Subject Access Request must be responded to within one calendar month..

An individual can make a request just by writing in, in accordance to the Data Protection Act, however their request cannot be properly processed without supporting identification documents.

On receipt of a request, the Security Management Team will use the system to search for all relevant footage relating to information provided in request. The search should make use of all available cameras in the locality provided to ensure that footage is not missed. Any footage that can be seen as relating to the request should be saved into the CCTV folder. The system will provide it with a Unique Reference Number. A copy of the footage should be made. In the case of DVD or data-stick transfer this should be sealed with an evidence sticker and all of the details relating to the request should be recorded on the form supplied and also recorded on the CCTV shared drive.

Once copied the data should be provided to the G4S Site Manager who will access the CTV system and remotely review the recorded data to consider if it is appropriate to release the footage in accordance with the General Data Protection Regulations and the Data Protection Act. Consideration must be given to the privacy of other individuals in any footage. Prior to releasing the data it will be necessary to redact any other personally identifiable information such as faces and/or vehicle details.

The G4S Site Manager and the BSU have the discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or personal information access rights as set out in General Data Protection Regulations and the Data Protection Act.

All released footage is to be accompanied with a cover letter explaining the responsibility of the receiver in relation to the Data Protection Act.

Disclosure to South Yorkshire Police

All South Yorkshire Police (SYP) requests will be processed via a form CID/49 and duty signed or authorised. Attendance at the Security Control Room will be by pre-arranged appointment only.

Image data including still images must not be released to the media for identification purposes; this should only be done through the press office and in accordance with Police and Criminal Evidence Act 1984. In ALL cases permission is to be sought from a Trust ASMS before release.

All requests for data should be submitted in writing on the request form. A version of this form is available from the Security Control Room.

The Trust does not charge the relevant agencies at this time.

If the total footage required exceeds 15 hours the Police must provide 2 password protected hard drives e.g. disclosure to obtain the data. Both hard drives MUST be new, boxed and unopened to prevent the introduction of viruses to the Hospital Eyes system. Requests will not be actioned unless the supporting paperwork is fully completed.

Any footage that can be seen as relating to the request should be saved onto the server unless the request exceeds 2 hours in total. The system will provide it with a Unique Reference Number. A copy of the footage should be made. This should be sealed with an evidence sticker and all of the details relating to the request should be recorded on the form supplied.

In cases where more than 2 hours of footage but less than 15 hours is required you should consult with the BSU for a decision on how to store and process the request.

For requests where the footage is to be provided on a hard drive, the required clips of footage should be prepared and then transferred onto the first hard drive. The Trust will provide a Unique Reference Number. A second copy of the incident should be made on the second hard drive.

These should be sealed with evidence stickers and all of the details relating to the request should be recorded on the form supplied.

Once the copies have been made a working copy should be provided to the requesting officer and recorded. The second copy should be provided to the G4S Site Manager who will make arrangements for the master copy to be securely held by the Trust Business Security Unit.

The G4S Site Manager or Supervisor has the discretion to refuse any requests for information unless there is an overriding legal obligation such as a court order or personal information access rights as set out in General Data Protection Regulations and the Data Protection Act..

All released footage is to be accompanied with a cover letter explaining the responsibility of the receiver in relation to the General Data Protection Regulations and the Data Protection Act.

Disclosure to Non-Internal Partners

For all other non-internal partner requests for footage, the requestor must complete the appropriate request form.

On receipt of a request, the CCTV operator will use the system to search for all relevant footage relating to information provided in the request. The search should make use of all available cameras in the locality provided to ensure that footage is not missed. Any footage that can be seen as relating to the request should be saved into the evidence locker. The Trust will provide it with a Unique Reference Number. A copy of the footage should be made. This should be sealed with an evidence sticker and all of the details relating to the request should be recorded on the form supplied.

Once copied the data should be provided to the G4S Site Manager who will access the CCTV system and remotely review the recorded data to consider if it is appropriate to release the footage in accordance with the General Data Protection Regulations and the Data Protection Act.

All released footage is to be accompanied with a cover letter explaining the responsibility of the receiver in relation to the General Data Protection Regulations and the Data Protection Act.

Audit and Review

The Head of Business Security will be responsible for undertaking regular audits of compliance to the Service Level Agreements, Protocols, and Procedures which cover this code.

All Partners will ensure that appropriate access is provided for the G4S Site Manager or BSU to undertake the required audit.

The G4S Site Manager will report on audits through an annual review to the Trust Head of Business Security.