CCTV Policy & Documentation

Policy information

Policy number: 323
Classification: Corporate
Supersedes: V2
Local Safety Standard for Invasive Policys (LOCSSIP) reference: Not applicable
National Safety Standards for Invasive Policys (NatSSIPs) standards: Not applicable
Version number: V3
Date of Equality Impact Assessment: 12/12/2024

Approval information

Approved by: Health and Safety Sub-Committee
Date of approval: 06/02/2025
Date made active: 19.02.2025
Review date: 06.02.2028

Summary of document:
A Health Board wide approach to the use of CCTV systems, defining roles and responsibilities. Describing practices that are compliant with all relevant legislation including the viewing and disclosure of recorded data.

Scope:
This policy covers everyone that is employed by Hywel Dda University Health Board whilst in the course of their duties including temporary staff and any visitors to Hywel Dda Health Board sites

To be read in conjunction with:
UK General Data Protection Regulation (UK GDPR)
201 – All Wales Disciplinary Policy and Procedure – Opens in a new tab
836 – All Wales Information Governance Policy – Opens in a new tab
837 – All Wales Information Security Policy – Opens in a new tab
Home Office, Surveillance Camera Code of Practice – Opens in a new tab

Patient information: Not applicable

Owning group:
Security Management Group (via Key Stakeholders) 11/12/2024

Executive Director job title: Director of Allied Health Professions and Health Science

Reviews and updates:
V3 – 06/02/2025 Full Review
V2 – 10/01/2022 Full Review
V1 – 23/04/2013 New Policy

Keywords
CCTV, recording, police, evidence, data, data protection, disclosure, playback, DVR, access, disc, copy, security, footage, prosecution, violence, aggression, criminal, proceedings, UK GDPR.

Glossary of terms
CCTV – Closed Circuit Television
BWV – Body Worn Video
UK GDPR – UK General Data Protection Regulation
CFSMS – Counter Fraud and Security Management Service

Key points:
This procedure outlines the processes for the use of CCTV and the accessing/disclosing of images.

Contents

Introduction

This document sets out the appropriate actions and procedures, which must be followed to comply with the Data Protection Act 2018, UK GDPR (General Data Protection Regulation) and codes of practice in respect of the use of CCTV (Closed Circuit Television) and BWV (body worn video) recording or surveillance systems managed by Hywel Dda University Health Board (HDdUHB) and will include buildings subject to shared working arrangements.

Policy Statement

HDdUHB is committed to providing a safe and secure environment for all staff, users and visitors to its premises, this includes the protection of medical equipment and assets that all contribute to health care delivery. CCTV/BWV will be used to record events, where recording is lawful and available, thereby protecting HDdUHB assets, preventing and deterring crime, securing the successful prosecution of offenders, reducing the fear of crime whilst enhancing patient, staff and visitor safety. At all times HDdUHB staff will ensure compliance to relevant legislation and this policy.

In drawing up this policy, due account has been taken of the following:

- Home Office, Surveillance Camera Code of Practice
- UK General Data Protection Regulation
- CCTV guidance produced by the Information Commissioner
- The Human Rights Act 1998
- The Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Caldicott Report 1997

GDPR was adopted in the United Kingdom on 14th April 2016 and became enforceable on 25th May 2018. The regulation contain 7 key principles for the management of personal data held by businesses and organisations and covers the processing of images of individuals caught by CCTV/BWV cameras. The changes and principles of the UK General Data Protection Regulation are as follows:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Data Security
- Accountability

It is paramount to consider that recorded images of individuals is classed as personal data and should be managed to the highest standards giving regard to the UK GDPR principles at all times as material breaches expose individuals and the Health Board to potentially criminal offences and sanction including sizable financial penalties.

An important feature of the legislation regarding the use of surveillance camera systems is the CCTV Code of Practice that sets out the measures that must be adopted to comply with the latest version of the Data Protection Act and should be considered in conjunction with the UK General Data Protection Regulation. This goes on to set out guidance for the following of good data protection practice. The code of Practice has the dual purpose of assisting owners and operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place. Organisations should also look to gain compliance as good practice and minimum standards to the Information Commissioners CCTV checklist report from 11th March 2020.

Where CCTV Systems are the responsibility of HDdUHB all staff must abide by this policy and comply with procedures detailed within it.

Scope

This policy covers everyone that is employed by HDdUHB whilst in the course of their duties including temporary staff and any visitors to HDdUHB sites.

Aim

The aim of this policy is to formulate legislation compliant, consistent working practices in relation to the use of CCTV/BWV on HDdUHB premises. These practices will protect Data held by the HDdUHB whilst allowing the appropriate level of access to material when requested by individuals or other agencies.

The effectiveness of CCTV/BWV will also be improved utilising its ability to prevent and detect crime, reduce the fear of crime and thereby enhance staff, patient and visitor safety. Retention of copied images is also covered in the Policy together with monthly/annual reviews to consider and lawfully justify the installation and continued use of cameras or devices.

Objectives

The main objective of this policy is to allow, where practicable, data to be recorded, stored securely, reviewed, copied and disclosed with compliance to all legislation. The accurate recording of all relevant information will also improve the integrity of the CCTV/BWV systems. This will allow robust lawful compliant procedures should future reviews or audits be carried out.

Definitions and Explanation of Terms

Prior to considering compliance with the principles of the Data Protection Act 2018 and UK General Data Protection Regulation, a user of CCTV or similar surveillance equipment, will need to determine two issues.

The type of personal data being processed, i.e. is there any personal data, or data that falls within the definition of sensitive personal data as defined by Article 9 (1) GDPR; Sensitive personal data' includes:

- personal data revealing **racial or ethnic, origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes) data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation.**

The **purpose(s)** for which both personal and sensitive personal data is being processed.

The Information Commissioner will take into account the extent to which users of CCTV/BWV and similar surveillance equipment have complied with UK GDPR and CCTV/BWV Code of Practice when determining whether they have met their legal obligations when exercising their powers of enforcement.

Policy Application

Initial Assessment of Procedures

The Chief Executive has the legal responsibility for the HDdUHB CCTV/BWV systems. Any authorised user of the systems will have responsibility for the day-to-day compliance with the requirements of the UK GDPR and latest CCTV Codes of Practice and this policy.

For the purpose of this policy HDdUHB CCTV/BWV, schemes are installed/used for the:

a) Prevention or detection of crime or disorder;
b) Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings)
c) Interest of public and employee Health and Safety
d) Protection of public health
e) Protection of HDdUHB property and assets
f) To promote safe sites and effective traffic management and parking control

Any breach of the Codes of Practice will be detected via controlled access to the system and auditing. Employees found to have inappropriately accessed the CCTV/BWV systems will be reported under the HDdUHB Disciplinary policy and potentially face both criminal and disciplinary process.

Positioning / Review of the Cameras

It is essential that the purpose and location of the equipment be carefully considered, so as not to unnecessarily invade the privacy/activity of persons inside/outside the perimeter of HDdUHB premises because the way in which images are captured will need to comply with the UK UK General Data Protection Regulation 2016, Data Protection Act 2018, Human Rights Legislation and CCTV/BWV codes of Practice.

All cameras are to be located in prominent positions within public and staff view and do not infringe on clinical / treatment areas unless authorised by Welsh government. All CCTV surveillance with the exception of some legacy systems is automatically recorded. BWV will be utilised in order to secure evidence of disorder or criminal activity and shall be of a design to make this obvious when it is in operation and recording together with a verbal disclosure by the user where practicable, using the phrase **"Everything you say and do is being recorded on video".** Although minor deviations are acceptable, the overriding burden is to ensure that persons know they are being recorded. In some instances of serious or spontaneous violence then to give a verbal warning would increase risks to the user or is not practicable, devices may be activated and the reasons and footage recorded on Form C (See Appendix C).

Signs are to be erected on all entrance points to HDdUHB premises and throughout the site to ensure staff and visitors are aware they are entering an area that is covered by CCTV surveillance equipment. Where BWV (body worn video) is present this will be displayed in a clear and transparent manner with notices informing all persons on the premises that such a system exists and the purpose for which it is used for.

Signage reinforces the deterrent and protective properties that CCTV/BWV has to offer but also satisfies the criteria for being for a defined purpose, lawful fair and transparent.

Use of Covert CCTV (Directed) surveillance if required must be requested through the Police. If the request through the police is refused then authority can only be given by the Chief Executive NHS Wales or the Director of Resources, Department for Health and Social Services, regarding a requirement for directed surveillance activities within healthcare premises for security related matters. This is covered by WHC (2006) 060 following amendments to the Regulation of Investigatory Powers Act 2000 (RIPA), which removed NHS establishments from the schedules of the Act.

Counter Fraud and Security Management Service (CFSMS) previously known as the NHS Counter Fraud Service should undertake surveillance (involving fraud and corruption) on behalf of the NHS bodies in England and Wales.

Prior to any camera installation the Estates Manager/Department Manager in conjunction with the Head of Information Governance and security provider will ensure that the installation complies

with UK GDPR, CCTV Code of Practice and Surveillance Camera Code of Practice.

Installations need to consider the purpose for which they are installed giving consideration to privacy impact assessments using a PLAN model. In that, the installation of cameras has a clear need satisfying the following:

P - Proportionate
L - Lawful
A - Appropriate
N - Necessary

Where less intrusive methods of resolving an issue are practicable such as increased lighting for car park areas, then these should be considered and implemented in preference to CCTV.

All cameras should be checked at least monthly together with recording devices BWV units, NVRs or DVRs to ensure their correct operation and functionality and a yearly review should consider the purpose use and necessity of cameras on every HDdUHB site using the PLAN standard.

Quality of Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme be clearly identified. For example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

Approved security companies should undertake all camera installations and service contracts. Upon installation, all equipment is tested to ensure that only the designated areas are monitored and high-quality pictures are available in live and play back mode. All CCTV/BWV equipment should be serviced and maintained on a regular basis. Existing CCTV systems can be updated through the purchase and installation of improved cameras, providing its does not impact on the areas of coverage. This process should be continuous as legislation and technology changes.

Processing of Images

Images, which are not required for the purpose(s) for which the equipment is being used, should not be retained for longer than is necessary, with regards CCTV systems, Digital and Network video recorders currently overwrite to ensure this process, while BWV images would need to be downloaded and stored securely with stored images on the devices being erased once images had been downloaded. While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the Data Protection Act 2018 and UK GDPR. No images should be retained longer than is needed, with steps made to ensure the data

is recorded of being disposed and ensuring that no breaches or use of the images can occur from this point.

Where images are required for evidential purposes in legal or NHS disciplinary proceedings and a Data recording is made, encryption techniques should be considered and deployed. The Data can then be placed in a sealed envelope signed and dated and retained securely by the relevant department or head of investigation until all processes are completed. As stipulated, this data at the conclusion of proceedings should be retained in accordance with Data and evidential guidelines and destroyed in compliance with those guidelines.

Viewing of images is controlled by the Data Protection Lead or a person nominated to act on their behalf (e.g. Investigating Officer, Human Resources, Department managers, hotel services staff, Estates staff, Buildings managers). Only persons trained in the use of the equipment and authorised by the relevant IT Department can access data.

All images viewed in playback mode shall be recorded on the appropriate record sheet and a further record made if data is copied.(See Appendices A & B). On no account is there to be unrecorded viewing of recorded Data unless in the event of an emergency to prevent loss or life, serious harm or loss.

Access to and Disclosure of Images to Third Parties

It is important that access to, and disclosure of, the images recorded by CCTV/BWV and similar surveillance equipment is restricted and carefully controlled. This will ensure compliance with UK GDPR the CCTV/BWV codes of practice and that the rights of individuals are preserved, but also ensure that the continuity of evidence remains intact should the images be required for evidential purposes e.g. a Police enquiry or an investigation being undertaken as part of the NHS disciplinary procedure.

Access and disclosure to images is permitted only if it supports the purpose of the investigation. Under these conditions, the CCTV/BWV images view / release form (See Appendix A) must be completed. Each request must be received in writing signed and assessed prior to any images being reviewed copied or released.

Data will only be reviewed or disclosed upon receipt of a correctly completed authority. For police purposes, this will be an officer not below the rank of Inspector for normal investigations and Superintendent where grounds are not disclosed to the HDdUHB. On no account are Hywel Dda University Health Board staff to access or request data unless compliant with the above process.

Access to Images by Individuals

Article 15 of the UK General Data Protection Regulation gives any individual the right to request access to CCTV/BWV images. These are known as **subject access requests.**

Individuals who request access to images must submit a request to the Information Goverance Team. Upon receipt the Information Governance Team and Data Protection Officer will determine whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties. If the duty of care cannot be discharged then the request can be refused.

A written response will be made to the individual, giving the decision (and if the request has been refused, giving reasons) within 30 days of receipt of the enquiry.

Enforcement

The Information Commissioner has the power to issue Enforcement Notices and proceedings against individuals or HDdUHB where they consider that there has been a breach of one or more of the UK General Data Protection Regulation principles or CCTV/BWV codes of Practice. An Enforcement Notice would set out the remedial action that the Commissioner requires of any health board to ensure future compliance with the requirements of the Act together with consideration of prosecution and financial penalties.

Roles and Responsibilities

The **Chief Executive** shall:

- Have overall responsibility for the implementation of this policy.
- Be overall accountability for the management of health & safety and will delegate responsibility to ensure that adequate and appropriate resources are made available to ensure that the HDdUHB meets its legislative statutory and operational obligations.

The **Director of Estates** shall:

- Be responsible for the overall management of the HDdUHB CCTV/BWV systems in regard to signage, positioning and coverage of cameras including maintenance and repair and ensuring this policy and that UK GDPR and the CCTV/BWV Code of Practice issued by the Information Commissioner Office (ICO) is complied with wherever practicable in relation to those matters.
- Ensure that where users identify defects to any registered CCTV/BWV systems, there are processes for prompt assessment and repair wherever practicable within acceptable timelines.

The **Assistant Director of Informatics** shall:

- Be responsible for the overall management of the HDdUHB CCTV/BWV systems regarding Data recording devices, network access and security measures including maintenance and repair of information technology hardware and systems. Ensuring this policy and the Code of Practice issued by the Information Commissioner is complied with wherever practicable in relation to those matters.
- Ensure that where users identify equipment or systems failures, there are processes for prompt assessment and repair wherever practicable within acceptable timelines.

The **Security Advisor** shall:

- Be responsible for ensuring that the sites within HDdUHB that have CCTV/BWV are aware of this policy and implement its requirements. Providing practical and lawful procedures/advice for its use.
- Advise on operational and strategic issues that involve the use of CCTV/BWV for investigative and preventative purposes.
- Assist the Information Governance Lead in investigations in relation to the use of CCTV/BWV.

The **Information Governance Lead (Data Protection Officer)** shall:

- Be responsible for ensuring that systems and procedures are in place on all sites for which they have responsibility to ensure compliance with this policy and the ICO's Code of Practice and the Data Protection Act 2018 and UK GDPR.
- Ensure that the use of CCTV/BWV equipment on HDdUHB premises has been registered with the Information Commissioner and the notification for the purpose is maintained.
- Be responsible for identifying breaches of policy or legislation and taking remedial or investigative actions.
- Be responsible for investigating any violations that are identified by the ICO.

County Heads / Site Managers / Building Managers shall:

- Ensure that all CCTV/BWV systems can be accessed appropriately at all times by identifying and training authorised members of staff.
- Ensure that monthly checks and yearly reviews of CCTV/BWV are conducted.

All **Operators and Users of HDdUHB CCTV/BWV Systems** shall:

- Be responsible for upholding and adhering to the arrangements in this policy as well as compliance with UK GDPR and the Information Commissioners CCTV/BWV codes of Practice.
- Ensure that all data/images are handled securely and responsibly within the aims of the policy. (Breaches and violations may result in internal or criminal investigations).

- Report any breaches of this policy to the HDdUHB Data Protection Lead.
- Attend training/refresher sessions as may be required in order to maintain compliance with legislation.

Training / Support

All staff will receive awareness of this policy through their induction and mandatory training updates.

This policy will be available to view on the HDdUHB intranet.

Should anyone require support, advice or guidance on any element outlines in this policy they should speak to their line manager, Estates and Facilities Manager, Trade Union Representative, Data Protection Lead or Security Adviser.

Implementation

This policy will be implemented throughout HDdUHB at all sites holding any CCTV systems and will apply to all staff.

Review Arrangements

This policy will be reviewed by the policy owner within 3 years of approval. However, a review earlier than this may be prompted by factors including:

- Legislative or regulatory changes;
- Structural or role changes;
- Operational or technological changes in the evidence-base;
- Organisational learning;
- Audits and reviews of the effectiveness of the policy.

References and Further Information

The listed references below can be used to gain further information:

- Information Commissioners Office, Video Surveillance (including guidance for organisations using CCTV): Video surveillance (including guidance for organisations using CCTV) | ICO – Opens in a new tab.
- Information Commissioners Office, UK GDPR Guidance and Resources: UK GDPR guidance and resources | ICO – Opens in a new tab.
- Home Office, Surveillance Camera Code of Practice: Surveillance Camera Code of Practice – Opens in a new tab.
- Home Office, Cod Ymarfer ar Gyfer Camerâu Gwyliadwrieth (Surveillance Camera Code of Practice - Welsh Version):

Surveillance Camera Code of Practice – Opens in a new tab.
- Caldicott Report 1997

Relevant Law:

- Health and Safety at Work Act 1974
- Human Rights Act 1998
- Management of Health and Safety at Work Regulations 1999
- Freedom of Information Act 2000
- Regulations of Investigatory Powers Act 2000
- Data Protection Act 2018
- UK General Data Protection Regulation 2016

Appendix A – Personal Data Request Form

Personal Data Request Form

Part A	Application

To: (name and position if known) _____

Organisation: Hywel Dda University Health Board (HDdHUB)

In line with the protocol agreed between Dyfed Powys Police and the HDdUHB I herewith make formal application for access to view / listen to and (if necessary) copy CCTV recorded data of an occurrence / incident within the site which occurred:

at approx.: (time) _____ On: (date) _____

Specific details of the data referred to is attached. (See Part B)

I require access to this personal data for one or more of the following purposes:
(tick appropriate reasons)

Purpose:	Legal Basis	√
For the prevention, investigation and detection of crime	1 & 2	
For the apprehension and prosecution of offenders	1 & 2	
To confirm or corroborate information for intelligence purposes	1 & 2	
To put before a court to obtain a search warrant.	1 & 2	
To prepare a file for the Coroner's Court	3	
To further a money laundering or confiscation investigation.	4	
To risk assess and address Health and Safety issues.	1, 2 & 5	
To identify, assess or confirm any Child Protection issues.	6	
To progress enquiries into a Road Traffic incident	1 & 2	
To protect life or property	1 & 2	

Key to legal basis:				
	1	Police Act 1996	2	Common Law
	3	Coroner's instructions	4	Proceeds of Crime Act 2002
	5	Health and Safety Law	6	Children's' Act 2004

I can confirm that:

(a) The information / data will only be used in connection with the enquiry, held, and used only as long a required for policing purposes including any subsequent criminal justice or Coroner's proceedings.

(b) if this personal data is not disclosed it will prejudice the purpose(s) indicated above

Requesting Police Officers Details:

Print Name: _____ Rank: _____ Date: _____

Signature: _____

Authorising Police Officers Details:

Print Name: _____ Rank: _____ Date: _____

Signature: _____

Personal Data Request Form

Part B	Details of the Data to be Viewed / Copied

The personal data which I am seeking authority to view and / or copy is:

Describe the information sought and the subject of the enquiries as far as is possible without prejudicing them. Also – please specify which specific area(s) of the department did the incident / occurrence(s) take place.

Requesting Police Officers Details:

Print Name: _____ Rank: _____ Date: _____

Signature: _____

Authorising Police Officers Details:

Print Name: _____ Rank: _____ Date: _____

Signature: _____

Request for Access to Personal Data Hospital Response Form

NB: Please respond to all requests in order to help prevent duplication.

To: (name and applicant) _____

Organisation: **Dyfed Powys Police**

Please strike through whichever Part is inappropriate.

Part A	**Application Approved**

I refer to the Access to Personal Data Request Form submitted by you on: _____

and I can confirm that:

(a) I am authorised by the Hywel Dda Health Board to consider such applications; and

(b) having considered your application, I hereby authorise you:

(i) access to view the data ☐

Tick which boxes are appropriate

(ii) to receive a copy of the data ☐

Part B	**Application Refused**

I refer to the Access to Personal Data Request Form submitted by you on: _____

I can confirm that:

(a) I am authorised to undertake this duty by the Hywel Dda Health Board and

(b) having considered your application - authority is denied for the following reason(s):

(please state reason for refusal here so that applicant can ascertain whether you need additional information before perhaps reconsidering the application or in order that the applicant can consider whether a Court Disclosure Order is appropriate/necessary)

Signed: _____ Position: _____ Date: _____

_____
Print Name

NB The subject of the request should not be given any indication that this request has been made prior to consultation with the requesting officer.
If your organisation subsequently receives a request for a copy of this document (e.g. under the Data Protection Act or Freedom of Information Act), please contact the Dyfed Powys Police Data Protection or Freedom of Information Officer.

Appendix B – Access to View / Copy Images (Internal)

Bwrdd Iechyd Hywel Dda Health Board

REQUEST TO VIEW OR COPY IMAGES (INTERNAL)

Name of the person making the Request:	
Department: Position:	
Address:	
Telephone Number:	

DETAILS OF IMAGES TO BE VIEWED

Date:			
Reason:			
Signed:		**Dated:**	
Request Granted:		**Request Denied: (Reason)**	

TO BE COMPLETED IF IMAGES ARE REMOVED

Ref No:			
Issued to:			
Authorised by:			
Date Issued:			
Issued by:			
Return Date:			
I acknowledge receipt of the above CD / Data Medium:			
Signed		**Date:**	

Appendix C – Activation of Body Worn Video (Internal)

GIG CYMRU NHS WALES
Bwrdd Iechyd Hywel Dda Health Board

Recording made with Body Worn Video – Internal

Name of the person completing form:	
Department: Position:	
Address:	
Telephone Number:	

Details of Images to be Viewed

Date:	Time recording started Time recording ended		
Reason:	Give details including Datix Reference		
Signed	Recording person	**Dated:**	
Images required for Police		**Request Approved / Denied: (Reason)**	

To Be Completed if Images are Copied

Ref No:			
Issued to:			
Authorised by:			
Date Issued:			
Issued by:			
Return Date:			
I acknowledge receipt of the above CD / Data Medium:			
Signed		**Date:**	

Please send copy of this form to charles.scarf@wales.nhs.uk upon completion.