PSI
CUMANN CÓGAISEOIRÍ NA hÉIREANN
The Pharmaceutical Society of Ireland

AN RIALTÓIR CÓGAISÍOCHTA
THE PHARMACY REGULATOR

Closed Circuit Television Policy

Version 1 July 2016

Table of Contents

1. Introduction

The purpose of this policy is to regulate the use of Closed Circuit Television (CCTV) and its associated technology when monitoring both the internal and external environs of the Pharmaceutical Society of Ireland (PSI) premises under the remit of Bilfinger HSG. A copy of this CCTV Policy will be made available on the PSI website, provided to all PSI staff, Council and Committee Members and a copy will be provided to visitors on request.

2. Scope

This policy applies to all personnel in and visitors to PSI House, Fenian Street, Dublin 2. Moreover, it relates directly to the location and use of CCTV, and the monitoring, recording and subsequent use of such recorded material. The CCTV Policy is in place to enable Bilfinger HSG to operate the CCTV system within the PSI.

This policy prohibits CCTV monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc. Furthermore, CCTV monitoring is limited to uses that do not violate the reasonable expectation to privacy as defined by law. The CCTV cameras will be used to:

- protect the PSI buildings and assets, both during and outside of operational hours (the system will be in operation 24 hours a day, every day);
- promote the health and safety of personnel and visitors;
- support the Gardaí in a bid to deter and detect crime; and
- assist identifying, apprehending and prosecuting offenders.

The personal data recorded and stored by the CCTV system will be used only for the purposes outlined in this policy document. Collection, storage and use of CCTV footage shall be in compliance with Data Protection legislation.

3. Data Controller

The data controller in respect of images recorded and stored by the CCTV system at the PSI premises is the PSI. The data processor is Bilfinger HSG. The PSI Registrar is responsible for monitoring the implementation and compliance of the CCTV policy within the PSI.

4. Fair Obtaining

The fair obtaining principles inherent in the Data Protection Acts 1988 and 2003 require that those people whose images may be captured on camera are so informed. Accordingly, the PSI Data Protection Officer will provide a copy of this CCTV Policy to staff, Council and Committee members, and on request to visitors to the PSI. Adequate signage will be placed at each location in which CCTV

cameras are situated to indicate that CCTV is in operation (locations listed in following section). Signage shall include the name and contact details of the data controller as well as the specific purpose for which the CCTV camera is in place in each location.

5. Location of Cameras

The CCTV network for the PSI is located in the following areas:

- Front External (Main entrance and ramp)
- Rear of building (Car park)
- Lift lobbies on each floor
- Reception area

There are 21 cameras in total. Cameras will be positioned so that they cannot capture non-relevant images in their vicinity (for example neighbouring private property, or passers-by).

6. Operation of the System

The recording system is a Milestone XProtect Smart Client Network Video Recorder (NVR) solution which records video data over TCP/IP networks. The system can only be accessed by authorised personnel from Bilfinger HSG and Rockbrook Engineering (Installers of system), and PSI's ICT Unit. A Service Level Agreement has been put in place between the PSI and Bilfinger which details the terms of the contract including confidentiality agreements, data security and disclosure. The system is housed in the Communications room on the ground floor which reception and the facilities administrator have access, in addition to Bilfinger HSG and Rockbrook Engineering.

The system can be accessed remotely using a unique password only available to Bilfinger HSG and Rockbrook Engineering. Access by Rockbrook Engineering is only by request of Bilfinger HSG and must be logged. Should the system be accessed or works conducted on it by unauthorised personnel or without Bilfinger HSG Management instruction, this will be viewed as extremely serious and will be grounds for automatic termination of the contract.

7. Data Protection, Storage and Retention

The data captured from the CCTV cameras is securely stored as electronic data in the Communications Room on the ground floor. Typically, this data is recorded on a loop and will be retained for maximum of 30 days. It will be over written after that period. However, data may be retained for longer periods where in the opinion of the PSI the events captured may give rise to court proceedings.

The Communications Room is a restricted area. Unauthorised access to that area will not be permitted at any time. Access to the data is restricted to authorised personnel (see Section 6 for list). The area is swipe card secured with only the individuals identified in section 6 having access.

The storage devices are password protected. Supervising the access and maintenance of the CCTV system is the responsibility of Bilfinger HSG. Unauthorised access will be viewed as a data breach. In such an event, the PSI Data Breach Management Policy and Procedure must be followed.

8. Access Requests

Access to the CCTV system and stored images will be restricted to authorised personnel only (as indicated in Section 6). In relevant circumstances, CCTV footage may be accessed:

- By An Garda Síochána where the PSI are required by law to make a report regarding suspected crime;
- Following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on the PSI premises;
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to the PSI;
- To individuals (or their legal representatives) subject to a court order;
- To the PSI's insurance company where the insurance company requires the same in order to pursue a claim for damage done to the insured property.

Any person whose image has been recorded, has a right to be given a copy of the information recorded, providing that such an image/recording exists (i.e. that it has not been deleted), and provided that an exemption/prohibition does not apply to the release. To exercise that right, a person must make an application in writing to the PSI using the Data Access Form found on the website, providing sufficient information to identify themselves, giving a reasonable indication of the time period sought, and identifying the location of the camera. If the person is under eighteen years, the parent or guardian may make an application**.** The cost for making this application is €6.35 and will be borne by the applicant. Requests must be responded to by the PSI within 40 days.

Access requests can be made to:

Dr. Cheryl Stokes
Data Protection Officer
PSI -The Pharmacy Regulator
PSI House
15 - 19 Fenian St
Dublin 2

When a data access request is received, the relevant footage is copied and a specific retention time is assigned to this copy. In giving a person a copy of his/her data, the data controller may provide a still/series of still pictures, a tape or a disk with relevant images. However, other people's images should be obscured before the data is released. Data will be delivered to the requester ensuring that security measures have been considered and implemented. A log of access to images will be maintained. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data.

9. Providing CCTV Images to An Garda Síochána

With regard to requests from An Garda Síochána to download footage, the Data Protection Commissioner recommends that requests for copies of CCTV footage should only be granted when a formal written (or fax) request is provided to the PSI stating that An Garda Síochána is investigating a criminal matter.

For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request must be followed up with a formal written request.

It is up to the PSI to be satisfied that there is a genuine investigation underway. For practical purposes, a phone call to the requesting Garda's station may be sufficient, provided that you speak to a member in the District Office, the station sergeant or a higher ranking officer, as all may be assumed to be acting with the authority of a District/Divisional officer in confirming that an investigation is authorised.

A log of all An Garda Síochána requests will be maintained by the PSI and data processors. Any such requests should be on An Garda Síochána headed paper, quote the details of the CCTV footage required and should also cite the legal basis for the request (i.e. Section 8(b) of the Acts). Prior to the PSI issuing any CCTV images to An Garda Síochána, it will be discussed and agreed with the responsible PSI staff member.

There is a distinction between a request by An Garda Síochána to view CCTV footage and to download copies of CCTV footage. In general, An Garda Síochána making a request to simply view footage on the premises of a data controller or processor would not raise any specific concerns from a data protection perspective.

10. Review and Approval of the CCTV Policy

This policy will be reviewed and updated regularly to take into account changing Data Protection legislation or guidelines from the Data Protection Commissioner, An Garda Síochána, and relevant bodies.

Revision	Date	Description	Approved by
1	July 2016	Policy developed and issued to all staff, Council and Committee Members, placed on the PSI website and a copy made available at reception for visitors.	SMT

Appendix: Glossary of Terms

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

The Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.