

DPIAs

Record ID
Date created
Logged by
Assessment Owner
Directorate
Service
Other staff involved in the assessment

8
09/11/2020
[REDACTED]
[REDACTED]
Patient & Family Services
Estates and Facilities
Verkada surveillance system installation at Myland Hall site
CCTV DPIA
St Helena Hospice, Myland Hall, Barncroft Close, Colchester Essex, CO4 9JU

DPIA Title
DPIA Type

Address of CCTV installation

This DPIA will help you to identify whether the use of CCTV cameras is appropriate for the problem you wish to address, assess the risks and form a record of your decision making.

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.

Identify the need for a DPIA

St Helena operates Closed-Circuit Television (CCTV) surveillance at the Hospice at Myland to improve security, patient safety and deter anti-social or criminal behaviour. In particular, the CCTV allows reception and nursing staff to monitor anyone trying to enter or leave our buildings through the main entrance. This is particularly valuable at night when there is reduced staff.

This requires a DPIA because the system captures biometric information (physical images used for identification purposes) and has facial recognition functions.

Does the system's technology enable recording?
State where recording is undertaken and if audio recording is enabled?

Yes

The CCTV cameras record of images of persons around the Myland Hall site. The cameras have no capacity to record sound.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Additional cameras in place from July 2021:

If data is being disclosed, how will this be done?

Please specify

Explain the information flow from initial capture to eventual destruction

Copies of footage released (e.g. encrypted digital media, via courier, etc) (please specify)

Surveillance footage can be delivered to individuals or organisations using e-mails

Live monitoring.

- It is capable, but not required, to use watchlists or any integrated surveillance technologies, such as facial recognition.
- Auto deletion after the retention period, set up for 30 days.

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?

Describe the nature of the processing

- Our use of CCTV is governed by our CCTV Policy (616), which provides further detail of the following.
- We capture CCTV footage using nine cameras. The footage captured only covers private land owned by St Helena.
- There is no recording of public streets or other properties.
- There are four scenarios under which St Helena may disclose CCTV footage; internally to staff (i.e. through live monitors or patient safety investigations), to external individuals via a Subject Access Request (SAR), to law enforcement officials or regulatory agencies, or to external individuals via a Freedom of Information request.
- Data will only be transferred to other media by authorised staff, if necessary to provide it to someone with a legitimate interest in it.
- A live feed of the footage will be displayed on three monitors, [REDACTED]. These monitors are shielded and visible only to staff.

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?

Describe the scope of the processing

The data will contain identifiable information on individuals as they enter and egress the Farmhouse, Learning and Development Centre, and the Terrace.

The cameras record continuously and cannot be automatically turned off.

We will store data for a rolling period of 30 days, at which time the data will be deleted automatically. Footage will not be viewed retrospectively by any employees unless necessary to investigate an incident that has occurred on site and has been deemed as justifiable by the Head of Estates and in consultation with the DPO. Justifiable reasons must be stated within this DPIA and these cannot be adjusted without formal consultation process.

All request for non-live footage are to have a clear record of:

- Date
- Reason for access
- Specific data accessed
- Identity and role of person accessing the footage and staff facilitating the process.

These records will then be regularly audited by the DPO.

This use of CCTV potentially affects all staff and patients are our Myland Hall site and any visitors to it.

The geographical area covered is restricted to the Myland Hall site and no adjacent properties are surveilled.

The geographical area where the cameras are located is shown in the site plan in the associated documentation file area. The cameras are all located on private land owned wholly by St Helena.

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)?

Describe the context of the processing

The individuals who will be recorded consist of either persons who have a relationship with St Helena, or general members of the public within the following groups:

- Patients
- Family and friends of patients
- Staff
- Volunteers
- Fundraisers
- Trustees
- Contractors
- Suppliers

Families and friends can often include children.

St Helena has a relationship and trust with both staff and patients as well as a duty of care. In particular, patients at end of life are often frail and vulnerable and we are required to protect them from needless stress and disruption. We believe that our staff, patients, and visitors will have a reasonable expectation that we would use a limited deployment of CCTV and they would be familiar with this from visits to other healthcare settings.

The technology that we use is that commonly provided by security contractors and the use to which we put it is entirely standard.

The external cameras that captures the front of the (dining room) Rm 5 and 6's bay windows and the Terrace camera both have views of patient rooms, this privacy issue will be mitigated with the use of mirror film for the windows, enabling the patients to look out normally but the camera footage not see in.

■ external camera have views of private houses on the boarders of St Helena property. The views of these properties have been manually blanked out c/o IT team.

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 main purpose of the CCTV is primarily to act as a deterrent for any anti-social behaviour.

The CCTV will also be used by the nursing team to identify visitors prior to granting access to the reception and main IPU area and monitor the safety of patient accessing the smoking shelter and movement around the site.

Also to ensure the safe egress and ingress of staff to the Learning and development centre including rapid response teams during unsociable hours.

Describe the purposes of the processing

Monitored in real time to detect and respond to unlawful activities, Monitored in real time to track suspicious persons/activity, Linked to sensor technology, Used to search for vulnerable persons, Recorded data disclosed to authorised agencies to support post incident investigation , Recorded data disclosed to authorised agencies to provide intelligence

How is the information used?

Data automatically deleted after retention period stated in the Estates Data Retention policy.

How long is data stored? (please state and explain the retention period)

Under certain circumstances authorised persons may override the retention period, e.g. retained for law enforcement agencies

Article 6 lawful bases for processing

6(1)(f) Legitimate interests

ICO lawful basis interactive guide. You can use the online tool [here](#) to help you decide on your lawful basis (Ctrl+ left click to open in a new browser tab).

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Article 6 details

Our lawful basis for operating CCTV at our Myland Hall site is GDPR Article 6(1)(f), where processing is in our legitimate interest. In this case, we believe we have a legitimate interest to use CCTV to protect our staff, patients, visitors, and property. Other methods of deterring antisocial behaviour, such as increased illumination at night, would not allow staff to monitor the main entrance.

Our use of CCTV is controlled by our CCTV policy (616), which specifies that no further installations or re-siting of existing installations may be carried out without an additional assessment. This policy also restricts the purposes to which the data may be kept.

We will ensure data minimisation via the rolling 30-day deletion, mentioned above. The quality of the footage is assured by our IT department and the technical functioning of the system is subject to periodic review.

We will support third parties access to the footage via our Data Subject Access Requests Policy (901).

Does the system have the ability to use facial recognition?

Where facial recognition is used, an Article 9 Lawful Basis must also be completed as this will include processing special categories of information.

Will this require processing special category data?

Yes

Types of special category data

Type of data

Biometric ID information (including facial recognition)

Confirm that this type of data is necessary to the processing

Yes

Reasoning

To ensure the safety of patients (and any site visitors, staff and volunteers) and the premises. Also to supply law enforcement agencies with high quality evidence if any incidents occur across the site. The intelligent surveillance technology is available to us and offers immediate access to tracing where an individual is or has been on site from facial recognition.

Article 9 lawful bases

9(2)(h) Preventative or occupational medicine

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

(e) processing relates to personal data which are manifestly made public by the data subject

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Article 9 details

We are a public authority and are required under the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 Regulation 12(2)(d) to ensure the safety of premises.

What other less intrusive solutions have been considered?

Security lighting is in place but not a sufficiently effective deterrent and doesn't offer a patient safety aspect.

The camera operation needs to be continuous to provide effective surveillance.

How will you ensure the processing is restricted to its lawful purpose and minimum data?

IT are creating a Power app through the Helpdesk to request any CCTV footage viewing. These will be sent through to the Estates Manager [REDACTED] to accept or decline, this feedback will automatically go back to the requester and once the footage is acquired [REDACTED] will send a link containing the footage within the Helpdesk ticket so the process is fully captured in one place. This process will be audited by the DPO ([REDACTED]), on a quarterly basis.

Audits are to be introduced to ensure compliance with the CCTV policy [616].

Verkada automatically logs all user access and sessions. For any activity — including adjustments to settings, accessing and sharing footage — Verkada keeps detailed logs including time, date, and the user who took any action within the platform.

The Verkada system retains audit logs for 1 year and they cannot be tampered with or altered.

What measures do you take to ensure processors comply with the lawful basis for processing? What information will you give individuals? How will you help to support their rights? How do you safeguard any international transfers?

How will you ensure the security and integrity of the data?

By following the procedures outlined in the CCTV policy. Only justified information will be share with the pre-approved parties.

To ensure greater access security, Verkada includes options for integration with single-sign-on (SSO) and two-factor authentication (2FA) providers.

End-to-End Encryption

All connections to Verkada devices are securely encrypted, and cameras only make outbound connections to our cloud services. By default, all Verkada systems encrypt data in transit using TLS, and all communication is over Port [REDACTED].

Automatic Firmware Upgrades

Verkada’s cloud-based management interface runs exclusively on Amazon Web Services (AWS), which meets the highest industry-standards for ensuring the security and protection of its customers’ data. Verkada also provides integration with Single Sign-On providers for secure authentication and role-based access control for fine-grained permissions management and has implemented full audit logs of video access and configuration changes.

Secure Backend Infrastructure

We provide automatic updates to the firmware running on the cameras which include security patches, as well as new features and enhancements for device performance. These updates are delivered securely from our cloud service to the cameras and require no additional external downloads or configurations.

State what privacy notice will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in the context.

How will you inform people that they are under surveillance and ensure that they are provided with relevant information?

Signage details how the CCTV in is place for the purpose of prevention of crime and public safety, the scheme is controlled by Verkada and the Estates Manager's contact details for further information.

1. Main IPU entrance door
2. On the fence to the Terrace
3. On the wall at the Barncroft Close entrance
4. On the front facade of the Joan Tomkin Centre
5. On the external bin store fencing,
6. Learning and Development centre, front entrance.

Is there a written policy specifying the following?

Further policy details

Are these procedures made public?

Are there auditing mechanisms?

The agencies that are granted access , How information is disclosed, How information is handled

CCTV policy [616]

No

Yes

Consider how to consult with relevant stakeholders

The views of our patients were not sought in the original installation, as it is felt that it was not appropriate to do so given the general vulnerability and deteriorating poor health of the patient profile entering the Hospice.

Stakeholder consultation

Record the stakeholders you have consulted about the data processing and the outcomes of your engagement.

Stakeholder name

Consultation method

Risk and Incident Group

Meeting / Group discussion

Views raised

After a clinical incident on Myland Hall site, (Incident Number 2511 - Action ID 2217) - IPU Matron [REDACTED] raised the issue of blind spots in the present coverage of CCTV.

Measures taken

Resulting in the agreement of [REDACTED] additional external cameras.

Stakeholder consultation

Record the stakeholders you have consulted about the data processing and the outcomes of your engagement.

Stakeholder name

IPU

Consultation method

Trial cameras

Views raised

Ease of access to view footage.

Measures taken

Additional monitor provided to [REDACTED] to allow surveillance.

Stakeholder consultation

Record the stakeholders you have consulted about the data processing and the outcomes of your engagement.

Stakeholder name

SMT

Consultation method

Project application

Views raised

Agreement from SMT on need to provide more comprehensive CCTV surveillance at Myland hall, that is compliant with current GDPR requirements.

Measures taken

See Associated documentation around the e-mail exchanges.

Business case approved.

Stakeholder consultation

Record the stakeholders you have consulted about the data processing and the outcomes of your engagement.

Stakeholder name

Verkada

Consultation method

Remote consultation

Views raised

Placement suggestions.
Installation logistics discussed.
Camera capabilities discussed.

Measures taken

Verkada appointed as CCTV provider, following business case to SMT.
Order placed for [REDACTED] cameras.

Identifying and addressing risks

Describe source of risk and nature of potential impact on individuals (include associated compliance and corporate risks as necessary).

Risk of CCTV footage being distributed to the public domain.

Likelihood of harm

Remote

Severity of harm

Minimal

Overall risk

Low

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk

Options to reduce or eliminate risk	Only selected IT and Estates staff have access to the system.
Effect on risk	Reduced
Residual risk	Low
Measure approved?	Yes

Identifying and addressing risks

Describe source of risk and nature of potential impact on individuals (include associated compliance and corporate risks as necessary).	Risk of GDPR regulations being breached.
Likelihood of harm	Remote
Severity of harm	Minimal
Overall risk	Low
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk	
Options to reduce or eliminate risk	Quarterly Audits to be undertaken to ensure proper use of the system is taking place.
Effect on risk	Reduced
Residual risk	Low
Measure approved?	Yes

Associated documentation

Associated documentation ID	17
Document Name	Phase 2 new cameras field of vision images
Document description	View of each camera's vision and shows image blocking of private properties.
Document date	12/07/2021
Attach File	CCTV signage pictures (Email from [redacted]).msg FW Vsaas Business Case Oct 2020 SMT e-mail conversation.msg Myland Hall Cameras.docx Phase 2 new cameras 12.07.21.docx SMT email approval.msg Verkada User accounts 11.05.21.docx

Associated documentation

Associated documentation ID	9
Document Name	Vsaas Business Case
Document description	Business case from Head of IT and Head of Estates
Document date	14/10/2020
Attach File	CCTV signage pictures (Email from [redacted]).msg FW Vsaas Business Case Oct 2020 SMT e-mail conversation.msg Myland Hall Cameras.docx Phase 2 new cameras 12.07.21.docx SMT email approval.msg Verkada User accounts 11.05.21.docx

Associated documentation

Associated documentation ID	10
Document Name	SMT Q&A's for system
Document description	E-mail trail for conversation between SMT and IT / Estates.
Document date	16/10/2020
Attach File	CCTV signage pictures (Email from [redacted]).msg FW Vsaas Business Case Oct 2020 SMT e-mail

conversation.msg
Myland Hall Cameras.docx
Phase 2 new cameras 12.07.21.docx
SMT email approval.msg
Verkada User accounts 11.05.21.docx

Associated documentation

Associated documentation ID

11

Document Name

SMT approval confirmation

Document description

E-mail from [REDACTED] confirming approval

Document date

27/10/2020

Attach File

CCTV signage pictures (Email from [REDACTED]).msg
FW Vsaas Business Case Oct 2020 SMT e-mail conversation.msg
Myland Hall Cameras.docx
Phase 2 new cameras 12.07.21.docx
SMT email approval.msg
Verkada User accounts 11.05.21.docx

Associated documentation

Associated documentation ID

7

Document Name

Verkada CCTV Compliance

Document description

Verkada support document about staying GDPR compliant.

Document date

21/12/2020

Attach File

CCTV signage pictures (Email from [REDACTED]).msg
FW Vsaas Business Case Oct 2020 SMT e-mail conversation.msg
Myland Hall Cameras.docx
Phase 2 new cameras 12.07.21.docx
SMT email approval.msg
Verkada User accounts 11.05.21.docx

Associated documentation

Associated documentation ID

5

Document Name

Account Holders

Document description

Management of Verkada account holders and access to mobile application.

Document date

11/05/2021

Attach File

CCTV signage pictures (Email from [REDACTED]).msg
FW Vsaas Business Case Oct 2020 SMT e-mail conversation.msg
Myland Hall Cameras.docx
Phase 2 new cameras 12.07.21.docx
SMT email approval.msg
Verkada User accounts 11.05.21.docx

Associated documentation

Associated documentation ID

2

Document Name

Signage placement

Document description

Pictures of the recently installed signage across the site.

Document date

04/01/2021

Attach File

CCTV signage pictures (Email from [REDACTED]).msg
FW Vsaas Business Case Oct 2020 SMT e-mail conversation.msg
Myland Hall Cameras.docx
Phase 2 new cameras 12.07.21.docx

SMT email approval.msg
Verkada User accounts 11.05.21.docx

Associated documentation

Associated documentation ID	3
Document Name	Field of vision images
Document description	View of each camera vision and overview of individual camera locations.
Document date	21/12/2020
Attach File	CCTV signage pictures (Email from [REDACTED]).msg FW Vsaas Business Case Oct 2020 SMT e-mail conversation.msg Myland Hall Cameras.docx Phase 2 new cameras 12.07.21.docx SMT email approval.msg Verkada User accounts 11.05.21.docx

Associated documentation

Associated documentation ID	1
Document Name	Site Plan of Myland Hall
Document description	Plan of the geographical area where the cameras are located. The cameras are all located on private land owned wholly by St Helena.
Document date	09/11/2020
Attach File	CCTV signage pictures (Email from [REDACTED]).msg FW Vsaas Business Case Oct 2020 SMT e-mail conversation.msg Myland Hall Cameras.docx Phase 2 new cameras 12.07.21.docx SMT email approval.msg Verkada User accounts 11.05.21.docx

Activity Log

Date of activity	12/07/2021
Entry by	[REDACTED] - Facilities and Health & Safety Manager
Activity or note	<p>After a clinical incident on Myland Hall site, (Incident Number 2511) - IPU Matron ([REDACTED]) raised the issue of blind spots in the present coverage of CCTV and lack of on site security out of office hours.</p> <p>Phase 2 of the site CCTV installation includes 4 new cameras:</p> <ol style="list-style-type: none">1. [REDACTED] - to cover a blind spot of potential entrance to the ward, (this area would benefit from additional signage).2. [REDACTED] - to protect oxygen which has been targeted in other NHS localities and the maintenance shed contents of high value.3. [REDACTED] - covers access to the building that currently has an unmanned reception area and will provide visibility for staff lone working.4. [REDACTED] - captures the entrance to reception and access to the staff-only staircase.

File attachments

Associated documentation sub-form shows field of vision images for these cameras (ID# 17).

Internal Audits

Internal Audits ID	8
Date of Audit	12/01/2023
Audit conducted by	██████████ - Compliance Officer
Audit tool used	CCTV audit tool
Audit tool version	Version 1
Upload completed audit	CCTV Audit - Myland - Jan 23.xlsx
Date of report	12/01/2023
Audit report completed by	██████████ - Compliance Officer
Upload completed report	CCTV Report Myland Site - Jan 23.docx
Date of next internal audit	12/07/2023

If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation.

Measures approved by	██████████ - Head of Estates and Facilities
Date measures approved	07/07/2021
Residual risks approved by	██████████ - Head of Estates and Facilities
Date risks approved	07/07/2021
Is this DPIA ready for the DPO review?	Yes
Set Initial Review Date	01/09/2022
Date of next review	08/09/2023

Reviews

Review date	07/09/2022
Reviewer	██████████ - Head of Estates and Facilities
DPO Review?	
Summary of review	The CCTV system has had no further changes, or additional cameras or monitors. Will review in 12 months time.
Next review date	08/09/2023
Review documentation	CCTV - labels and field of view.PNG

Reviews

Review date	01/04/2022
Reviewer	██████████ - Head of Estates and Facilities
DPO Review?	
Summary of review	<p>■ additional CCTV camera devices installed since last record. The ■ additional locations are:</p> <p>██████████ ██ ██████████ ██</p> <p>See screen shot attached illustrating the fields of vision for each device.</p> <p>The monitor for live surveillance was never installed and deemed unnecessary following the movement of the service back to the SinglePoint Office.</p>

In addition, the following updates:

- 1 A camera towards the pond was adjusted to capture the smoking shelter to help ensure patients remain safe.
- 2 No PowerApp was ever implemented
- 3 Additional external signage was erected for the L & D Centre
- 4 Still outstanding query around obtaining audit data that is fit for purpose and user friendly to permit an audit to be conducted.
- 5 The iPad for surveillance was removed and replaced with a kiosk desktop with surveillance 24/7 on display
- 6 A monitor with live surveillance has been installed in the Farmhouse reception

Next review date

01/09/2022

Review documentation

CCTV - labels and field of view.PNG

DPIA status

Active

Links to the Information Asset Register

Record ID	15
Information Asset Name	Verkada - Video Surveillance as a Service
Information Asset Owner's Directorate	Patient & Family Services
Information Asset Owner's Service	Estates and Facilities
Location	St Helena site
Specific location of the data server used	UK
Process ID	77
Directorate	Patient & Family Services
Service	Estates and Facilities
Short description of processing activity	Myland Verkada CCTV

Links to ROPA

Record ID	15
Information Asset Name	Verkada - Video Surveillance as a Service
Information Asset Owner's Directorate	Patient & Family Services
Information Asset Owner's Service	Estates and Facilities
Location	St Helena site
Specific location of the data server used	UK
Process ID	77
Directorate	Patient & Family Services
Service	Estates and Facilities
Short description of processing activity	Myland Verkada CCTV

Links to contracts

Record ID	15
Information Asset Name	Verkada - Video Surveillance as a Service
Information Asset Owner's Directorate	Patient & Family Services
Information Asset Owner's Service	Estates and Facilities

Location	St Helena site
Specific location of the data server used	UK
Process ID	77
Directorate	Patient & Family Services
Service	Estates and Facilities
Short description of processing activity	Myland Verkada CCTV