## Select Healthcare Group Ltd

## Data Protection Impact Assessment (CCTV)

**Select Healthcare Group** operates CCTV systems. As such, **Select Healthcare Group** has considered the privacy implications of such systems. There are a number of other issues **Select Healthcare Group** has also considered. The completion of this Data Protection Impact Assessment highlights some of the key implications.

A Data Protection Impact Assessment is also recommended by the Surveillance Camera Code of Practice which sets out the guiding principles that should be applied when CCTV systems are in place to ensure that privacy risks are minimized whilst ensuring the aims of the CCTV system are met.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for the CCTV system and the impact it may have on individual privacy.

The Data Protection Impact Assessment helps determine whether the proposed system can be justified as proportionate to the needs of the organisation. In undertaking this Data Protection Impact Assessment **Select Healthcare Group** has considered its obligations under Data Protection Law. (DPA 18 and UK GDPR)

**Select Healthcare Group** recognizes that changes do occur, and on this basis good practice recommends that the organisation reviews its Data Protection Impact Assessment. The organisation recognizes that it is good practice to undertake a Data Protection Impact Assessment before a system is put in place and follows the surveillance commissioner’s passport to compliance. The organisation also has a CCTV Policy. A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce and eliminate the risks.
5. Sign off the outcomes of the DPIA.

# Step 1: Identify the need for a DPIA

|  |
| --- |
| Explain broadly what 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. |
| **What is the aim of the project?** – CCTV consistently delivers benefits in terms of improved health and safety and security within organisations. It complements other security measures which are in place within the organisation.  CCTV aims to achieve the following:   * Improve the health and safety and security of clients, staff, and visitors * Protect the organisation buildings and internal infrastructure * Improve client behavior * Reduce vandalism * Provide assistance in the detection and prevention of crime   **Select Healthcare Group** has updated its Privacy Notice for its CCTV system. The Privacy Notice highlights what personal information is used and the lawful basis for using this personal information. It also highlights who the organisation will share the personal information with and how long the information will be kept. The Privacy Notice (Client) and Privacy Notice (Workforce) documents what rights an individual has regarding their personal information.  Reference should be made to the CCTV system in the organisation’s Information Asset Register. |

# Step 2: Describe the processing

|  |
| --- |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
| **How will you collect, use, store and delete data?** – The CCTV system will provide the organisation with pictures from fixed based cameras located in the Organisation building and grounds the organisation and the images will be transmitted/captured on a digital video recorder (DVR). The CCTV system is operational 24 hours a day, 7 days a week.  The transmitted images can be viewed live and also be viewed securely on the Organisation Business Manager’s workstations. This is documented in the organisation’s CCTV Policy. This helps to maintain site security, access control, Client and staff safety.  **What is the source of the data?** – The CCTV system provides still/video pictures, which are transmitted from cameras positioned in various locations throughout the organisation. All of the CCTV cameras are fixed on a particular scene. The location of the CCTV cameras are as follows:  See schedule A    **Will you be sharing data with anyone?** – The information is used to ensure the health and safety and security of clients, staff and visitors. They can be used to detect unauthorized visitors, clients with poor behavior/internal truancy, and protection of damage to organisation assets. The information may be shared with Senior Leadership Team and the Police for investigation and enforcement purposes.  Disclosure of data is covered by the organisation’s internal processes which are fully compliant with relevant legislation and Codes of Practice (please see the organisation’s CCTV Policy).  **What types of processing identified as likely high risk are involved?** – Recording of images. Storage of images securely. Appropriate data retention applied to the images.  The digital video recorder is located in the Server Room within a locked cabinet. Access to the images is password protected.  Data Management controls include passwords to the CCTV system. (See comment above)  Individuals can request copies of CCTV data which contains their personal information by submitting a subject access request. |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| **What is the nature of the data?** – The CCTV data captured are still and video recordings.  **Special Category data?** – By default, the CCTV may be picking up special category data including race/ethnic origin and the health of an individual  **How much data is collected and used and how often?** – The CCTV system is operational 24 hours a day, 7 days a week.  **How long will you keep the data for?** – Images will be retained for 30 days unless requested as part of an incident and then stored on archive for the period of the investigation process or for 12 months whichever is the lesser. The Data Management System automatically deletes the information after 30 days. This is included in **Select Healthcare Group** Data Retention Policy.  **Scope of data obtained?** – The CCTV images are obtained within the confines of the organisation grounds. |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| **What is the nature of your relationship with the individuals?** – The organisation provides care to its clients. The organisation may receive a number of visitors on a daily basis including contractors, inspectors, support and agency staff, etc.  **How much control will they have?** – The organisation does inform clients, staff and visitors that CCTV is in use by installing signs detailing their presence. Recommendation states that signs contain details of who the data controller is (i.e., **Select Healthcare Group** and the organisation’s contact telephone number. The CCTV signage needs to be located on entry to the organisation site (car park and pedestrian access). It also needs to be located to the rear of the site.  The CCTV system is capable of identifying individuals from the system and the images can be used in both criminal and civil court cases.  If a Subject Access Request is made data may be downloaded or copied for release to the data subject or a third party (in the case of a Data Protection request). Each request for data must be requested via a signed data release form. In the case of the Police this can be authorized by a person at the rank of Sergeant or above using a WA170 form.  **Do they include vulnerable groups?** – Cameras are located in areas where clients and staff have access. Cameras are not located in areas where privacy is expected. There are no cameras in toilet areas, changing rooms, and there are no cameras aimed at private areas such as residents’ rooms etc.  **Are there prior concerns over this type of processing or security flaws?** – The organisation has a CCTV Policy. The system is operated in line with relevant legislation and the Surveillance Camera Code of Practice (consideration respecting data retention). |
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? |
| The CCTV system is proportionate and justified. It also achieves for the organisation the following benefits:   1. demonstrates a duty of care to its clients, staff, and visitors 2. protects the fabric of the organisation both externally and internally 3. as a consequence of this budgets can be reduced/deferred to other organisation projects 4. encourages improvement client behavior 5. provides assistance in the detection and prevention of crime 6. to assist in managing the organisation   CCTV system is be referenced in the organisation’s Privacy Notice (Client)(Workforce and Volunteers). |

# Step 3: Consultation process

|  |
| --- |
| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
| The decision to install and expand the CCTV system was agreed by **Select Healthcare Group** Board.  This has been communicated to clients via the organisation’s CCTV Privacy Notice. This will be published on the organisation website. |

# Step 4: Assess necessity and proportionality

|  |
| --- |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
| **What is the lawful basis for processing?** – The lawful basis for processing is contained in the organisation’s Privacy Notice (Client). The lawful basis includes the following:   * Article 6 and Article 9 (Special Category Data) under Data Protection Law * The Common Law Duty of Care * Health and Safety at Work Act * Safeguarding Vulnerable Groups Act * Working together to Safeguard Children Guidelines (DfE)   **Does the processing achieve your purpose?** – Cameras are located in areas where clients and staff have access. Cameras are not located in areas where privacy is expected.  **Is there another way to achieve the same outcome?** – To support organisation security a locked in organisation policy has been adopted along with improved lighting and other improvements have been put in place.  **How will you prevent function creep?** – The lawful basis for processing will be contained in the organisation’s Privacy Notice (CCTV). Where there have been material changes to the way CCTV is used, the organisation will undertake a review of its CCTV system to ensure compliance and mitigate against ‘function creep.’  **How will you ensure data quality and data minimisation?** – Consider the source of the data. The organisation will consider developing a separate data retention policy which identifies data retention periods for CCTV. However, the organisation will note data retention periods against CCTV as documented in the Information Asset Register. The organisation will continue to be compliant with its CCTV Policy.  **What information will you give the individuals?** – The organisation will inform clients, staff and visitors that CCTV is in use by installing signs detailing the scheme and its purpose, along with a contact telephone number. The organisation does have a Privacy Notice for its CCTV.  **How will you help them support their rights?** – The organisation has a Subject Access Request procedure in place to ensure compliance with Data Protection Law. CCTV signage states a contact telephone number. The organisation will continue to be compliant with its Data Protection Policy. |

# Step 5: Identify and assess risks

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| Positioning of CCTV cameras at entrance points to the organisation and the issue of privacy  Housing of CCTV cameras outside and ingress of water  Ongoing maintenance of CCTV equipment preventing breakdowns, etc.  CCTV policies and procedures not in place leading to inconsistencies, etc.  Appropriate CCTV signage in place which conforms to industry standards  Training not undertaken by those using CCTV  Privacy Notice (Clients); (Workforce)  Noncompliance when upgrading the organisation’s CCTV system | Remote, possible or probable  Remote  Possible  Possible  Probable  Possible  Possible  Possible | Minimal, significant or severe  Minimal  Significant  Significant  Significant  Minimal  Significant  Significant | Low, medium or high  Low  Medium  Medium  Medium  Low  Medium  Medium |

# Step 6: Identify measures to reduce risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| CCTV & ingress of water  CCTV Maintenance  CCTV Policies & Procedures  Training  Privacy Notices  CCTV Passport to Compliance | Use of waterproof enclosures  Maintenance contract in place with Security Services  Policies and Procedures insitu  Undertaken in GDPR and Information Security  Update the Privacy Notices to include reference to CCTV  Upgrade CCTV using guidance from CCTV Passport to Compliance | Eliminated reduced accepted  Reduced  Reduced  Reduced  Reduced  Reduced  Reduced | Low medium high  Low  Low  Medium  Low  Low  Low | Yes/no  Yes  Yes  Yes  Yes  Yes  Yes |

# Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/date** | **Notes** |
| Measures approved by Caldicott Guardian: | Director | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by SIRO: | Director | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | DPO | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice:  Recommend that signage is put in place which meets industry standards (name of Select Healthcare Group, contact telephone number)  Include in **Select Healthcare Group’s** Information Asset Register  Working towards CCTV Passport to Compliance when updating CCTV | | |
| DPO advice accepted or overruled by: | Yes | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: | Retrospective | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: | PCU | The DPO should also review ongoing compliance with DPIA |