

DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the [Criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	Dr Atheetha Sivananthan
Subject/title of DPO	Information governance lead/ Practice security lead/ Practice manager
Name of controller contact /DPO (delete as appropriate)	Ms Abhirami Sivananthan

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.

We are considering installation of CCTV on our surgery premises.

The aims are to provide a safer environment for staff, patients and carers by:

- deterring aggressive or abusive behaviour in the public areas on site,
- recording evidence of aggressive or abusive behaviour for management to review and take appropriate action,
- ensuring fairness in considering allegation by staff of aggression or abuse from a third party,
- enhancing a feeling of security among workers and visitors.

Incidents of aggression or abuse have increased in the past year. We have had to call the police on occasion. We consider these as significant events and have discussed the possible causes. Many of them arose from misconception about the role of the health service, and we have been able to convey the correct information once the agitated person had cooled down. However, we would much prefer that person asks to discuss a matter in a controlled fashion.

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?

CCTV camera(s) will be installed in the public areas in the surgery – excluding areas of confidential activities such as consulting rooms.

The recordings will be securely saved on a system to be provided by a professional company.

Recordings will not be routinely viewed or shared, but in case an act of aggression or abuse occurs the footage relevant to that time will be reviewed.

If unused after a pre-set period, the recording will be automatically written over by future recording

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?

Video footage will be recorded with CCTV cameras in the reception area/ waiting room/ corridors. It will be passive general views and not focused on any person.

The recording will take place during opening hours. Most people who call at the reception desk may appear in the picture.

All recording will be kept for no more than 31 days – unless it has been required as evidence for police investigation or evidence in court.

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)?

The camera(s) will likely cover all visitors who come through our doors, including our patients and their carers, health workers from other organisations and service personnel.

Persons less able to defend their own rights (including children) may be included. It is borne in mind that the purpose of CCTV is to protect everybody at the surgery, and this benefit extends to vulnerable people.

The practice is well aware of safeguarding of children and adults, and all staff undergo periodic training in these issues.

Surveillance of this type is in common use in other healthcare premises, shops and on the streets. Since the pandemic, increased streaming of gatherings (such as in church) also means people who attend in person being filmed and shared online.

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?

It is widely accepted that the presence of CCTV monitoring inhibits people from displaying aggression or abuse.

Thus it is intended to discourage inappropriate behaviour in front of the public. The direct benefit is to prevent threats to the personal safety or wellbeing of staff and patients alike. The indirect benefit is to foster a culture of restraint and civilized dialogue, which can constructively help the practice grow.

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?

We are holding a virtual consultation with our patient participation group (PPG), which is inclusive of all registered patients.

This will run for one month from the beginning to the end of April. ✓ **completed**

The consultation will be in the form of posing open questions on the PPG webpage and an invitation to speak with administrators about any concerns.

We will be advised by the professional providers of CCTV equipment on physical steps to safeguard the data that it records.

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?

We will treat the CCTV recording as personal data.

We have a legal obligation to staff – to fulfil occupational safety and health.

There is also a legitimate basis – to protect the surgery premises and property from damage, and ensure safety of the public.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
<p>Patient is concerned the NHS will be hacked and recordings are made public.</p> <p>Patient (especially a young person) attends the surgery unknown to family/ parents, and is anxious that they may find out.</p> <p>Patient is accompanied by person unknown to family/ marital partner and fears the episode will be leaked.</p> <p>Patient is dressed in a manner which would not be accepted to his/her community and does not want them to know.</p> <p>Patient has been trying to avoid certain people and worries he/she will be exposed.</p> <p>Patient objects to being photographed due to spiritual beliefs</p> <p>Patient is a well-known personality and worries that the images will be used or shared without permission.</p> <p>[These points incorporate issues raised by stakeholders in our consultation exercise]</p>	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
	Remote	Significant	Low
	Remote	Minimal	Low
	Remote	Significant	Low
	Remote	Minimal	Low
	Remote	Possible	Low
	Probable	Minimal	Medium
	Remote	Significant	Low

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
Objection to being filmed by reason of own beliefs		Eliminated reduced accepted	Low medium high	Yes/no
	Signage before entrance to the monitored areas, informing of CCTV operations.	Accepted	Medium	Yes
	Provide option to enter by side door and take seat in auxiliary waiting area.	Eliminated	Low	Yes
	Add CCTV warning to website, social media and as appendix to everyday texting	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	A.S.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	A.S.	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	A.S.	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Additional measures as above.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	S.H. (deputising)	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	A.S.	The DPO should also review ongoing compliance with DPIA