

PRIVACY IMPACT ASSESSMENT FOR CCTV INSTALLATION AT CONGLETON DENTAL CENTRE

Step one: Identify the need for a PIA

Rationale for the for installation of CCTV at Congleton Dental Centre:

1-Prevention of crime

Following an arson attack to the dental practice causing over £100k of damages in March 2015. Luckily the arsonist was caught on CCTV from the neighboring pub but we felt that we needed to protect the premises from further damages, should such an incident arise again. We also hope it will act as a deterrent for any incidents of theft or vandalism to the premises.

2-Protection of Staff

We also hope the CCTV will help protect reception staff and patients in case of abuse or attack from members of the public or other patients.

Using CCTV can be privacy intrusive, because it is capable of putting law-abiding people under surveillance and recording their movements as they go about their day to day lawful activities, hence the need for a PIA.

Step two:

Describe the information flows

1 camera has been positioned inside in the reception area of the practice. This is the area we felt staff are most vulnerable to abuse from patients and members of the public. Although a small risk of this presents within the surgeries we felt this was a disproportionate breach of patients privacy to install cameras in these areas.

2 cameras are directed on the rear carpark of the practice. This is the area we had the arson attack in 2015. The cameras cover the back door of the practice and carpark area. This ensures we can see who enters the building or attempts to enter premises by force or any attempts of vandalism of staff vehicles parked here in addition to any further arson attempts or similar.

The cameras were installed by a local company call Synergy, as local company based across the road so they are easily accessible, should we have any problems. Both the owner, Mr Andrew Mellor and the Practice Manager Jenny Furnival are able to view the images should they need too. This can be done remotely from a mobile phone or by the work based computer.

The programme is accessible only by password, so only 2 people can watch and save the data, it is not available for all staff to view. Should any data be needed for a court case or in the case of a dispute by a patient, then it can be retrieved and for a small charge given to the person requesting it by letter to the practice.

The images are backed up every night; they are kept for 30 days before they are taped over. Patients' confidentiality is a priority and we feel we have taken steps to

ensure it is protected. The cameras do not record sounds, so any conversation would not be heard, but we would see by body language alone if the member of staff was under any type of attack.

Step three: identify the privacy and related risks

Key privacy risks from CCTV installation include:

- Capture of clinical record details on camera
- Capture of patients disclosing personal details and medical details on audio recording
- Misuse of recorded data ie recording staff lateness or malingering
- Misuse of recorded data ie disclosing patient attendance to appointments to other members of the public or organisations resulting in a confidentiality breach

Step four: Identify privacy solutions -

Solutions to the risks identified are as follows:

- Clinical records are computerised and unable to be read from CCTV images. Patients medical histories are stored securely once filled in and not left where images of them can be recorded
- No audio recordings are made to avoid recording patient's personal details
- The footage recorded is password protected and only 3 members of staff are able to access this via office computer or mobile device.
- Disclosure of images must be consistent with the purposes for which they were captured. Generally images should only be handled or viewed by the operator and people authorised by the operator in relation to the system's purposes. (Andrew Mellor, Carly Mellor and Jenny Furnival) The operator would not be able to allow someone to view images for another reason, say entertainment.
- The ICO have been informed that the cameras will be used for security and protection of staff from abuse, therefore footage should not be used for any other reason eg. Recording staff lateness etc. This may be classed as a criminal offence.
- The images are backed up every night; they are kept for 30 days before they are taped over
- Signs are displayed within the practice advising patients the premises are monitored by CCTV

Step five: Sign off and record the PIA outcomes

Risks to privacy and solutions implemented have been recorded by:

Andrew Mellor, Carly Mellor and Jenny Furnival

We feel after implementing the above solutions the privacy impact on individuals is minimal in these circumstances. The benefits of protecting staff from abuse and protecting the business and premises from further episodes of arson or theft/vandalism far outweighs the impact on privacy of patients

Step six: Integrate the PIA outcomes back into the project plan

Andrew Mellor, Carly Mellor and Jenny Furnival are responsible for integrating the PIA outcomes back into the project plan and updating any paperwork and for dealing with any privacy concerns, which may arise in the future.

The Information Commissioner must be notified annually of the continued operation of CCTV and failure to do so constitutes a criminal offence.