RISK NOTE

HIROC

Video or Closed Circuit TV (CCTV) Surveillance

OVERVIEW OF ISSUE

Video or closed circuit television (CCTV) surveillance is used for crime prevention/detection, public safety and to enhance the protection and security of occupants or property. Surveillance footage is frequently used as evidence in civil and criminal court proceedings. HIROC has successfully used video footage to defend organizations from slip and fall claims, as well as allegations of misuse of force with patients/clients/residents and visitors.

KEY POINTS

- Develop a clear policy on the use of video and/or CCTV surveillance.
- Do not substitute video surveillance for patient/client/resident supervision and monitoring.
- Ensure that video surveillance is appropriately identified and preserved in a timely manner following an incident.

THINGS TO CONSIDER

Definition

- Video surveillance system refers to a device or collection of devices that enable(s) continuous or periodic video observing and/or recording of an individual or individuals. In this document, the term video surveillance system includes an audio device, thermal imaging technology or any other component associated with capturing the image of an individual (Cavoukian, 2007).

Managing Liability

- Post public signage to inform people that surveillance is or may be in operation on the premises.

Policy

- Develop a standardized policy related to overt and possibly covert (e.g. for use in fraud investigations) video surveillance. Include the purposes of the system and of the collection, use, retention and disclosure of the footage.
- Involve legal counsel and/or insurer and privacy officer before installing covert video surveillance for fraud investigations.
  - When covert video surveillance is used, outline the specific information to be gathered, by whom, and for what length of time the surveillance will occur.
- Ensure the organization's incident reporting system/loss control practice prompts the appropriate sequestering of video surveillance (e.g. patient or visitor slip and fall near main entrances).
- Define who is authorized to view, access and receive copies of footage.

Patient/Client/Resident Safety and Privacy

- Do not record in personal spaces (e.g. locker rooms or washrooms).
- Video surveillance of at-risk patients/clients/residents should not be used as a substitute for direct/in-person observation by healthcare providers. Ensure persons' privacy during the provision of personal care (e.g. toileting) by turning off the camera or directing its focus outside the patient/ client/resident range.

Retention and Disposal

- Establish a system for the review of video surveillance once an incident is reported so that relevant footage can be identified and preserved. Consider not just whether the incident itself is captured but whether there is useful evidence about other factors (e.g. the weather, the presence or absence of salt on the ground, activities by staff).
- Define a standardized retention period for incident related video

Video or Closed Circuit TV (CCTV) Surveillance

surveillance. It is suggested that this period be the amount of time reasonably necessary to discover or report an incident (e.g. consider 30 months) or until the conclusion of an ongoing matter. Consider the need to sequester/lock-up video surveillance required for internal or external investigations.

Access and Disclosure

- Adopt standardized processes for internal and external requests for a copy of the video (e.g. insurance claim or police subpoena).
- Consider whether your video surveillance program should include the means to redact information from the footage if necessary (e.g. blacking out or blurring images, removing the sound of voices).
- Limit the release of the footage to the actual minutes when the incident occurred, unless events immediately prior to or after are relevant.
- Implement a centralized system to track all requests for access and related disclosures of video surveillance.

REFERENCES

- Cavoukian A. (2007). Guidelines for the use of video surveillance cameras in public places.
- ECRI Institute. (2012). Photography, filming, and other imaging of patients. Healthcare Risk Control, Supplement A, Risk and Quality Management Strategies 15.
- Information and Privacy Commissioner of Ontario. (2015). Guidelines for the use of video surveillance.
- Office of the Privacy Commissioner of Canada. (2008). Guidelines for overt video surveillance in the private sector.

Date last reviewed: October 2017