Video Surveillance Guidelines for Public Bodies

These guidelines provide considerations for public bodies when deciding whether proposed or existing surveillance systems are lawful and for ensuring adequate safeguards are in place.

January 2018

Office of the
Saskatchewan Information
and Privacy Commissioner

Video Surveillance Guidelines for Public Bodies

Introduction

Under *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) and *The Health Information Protection Act* (HIPA) public bodies are responsible for adequately safeguarding the personal information and personal health information in its possession or control. This includes collection, storage, use, disclosure and destruction of the information.

These responsibilities are also applicable to the use of video surveillance by public bodies that captures an individual's image.

Video surveillance refers to any video surveillance technology (video cameras, closed circuit cameras, still frame cameras, digital cameras, and time-lapse cameras) that enables continuous or periodic recording (videotapes, photographs, or digital images), viewing, or monitoring of public areas.

I Before Implementing the Use of Video Surveillance

Some considerations for the public body before implementing the use of video surveillance is to determine:

- Is the use of video surveillance lawful?
- Is video surveillance necessary?
- Are there any stakeholders that should be consulted with?

Is the Use of Video Surveillance Lawful?

One of the public bodies' first considerations is whether or not implementing video surveillance would be lawful. Section 25 of FOIP states as follows:

> **25** No government institution shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution.

Section 24 of LA FOIP provides the same clause for collecting personal information for local authorities. Section 24 of HIPA provides provisions for trustees regarding the collection of personal health information.

When public bodies are determining whether or not they have authority to use video surveillance, it will need to determine if the purpose of collecting the information falls within this section to be lawful under FOIP/LA FOIP.

Public bodies will also want to consider the use and disclosure provisions at sections 28 and 29 of FOIP, sections 27 and 28 of LA FOIP and section 26 and 27 of HIPA to ensure it has appropriate authority to use and/or disclose the information for the purpose of which it is being collected.

Is Video Surveillance Necessary?

Before implementing the use of video surveillance, public bodies should consider if there are other less privacy invasive options to reach the same goal. Before implementing the use of video surveillance, a public body should consider undertaking a privacy impact assessment (PIA). You can learn more about PIAs and find worksheets on our website at: https://oipc.sk.ca/resources/resource-directory/.

The PIA should first address what the purpose of the video surveillance is and whether or not there is a less privacy intrusive option other than using video surveillance for the public body's purpose. If the public body chooses to go forward with video surveillance, the PIA should also address collection, safeguards, use, disclosure, destruction and access to information.

Are there any Stakeholders that Should be Consulted with?

Before implementing the use of video surveillance, public bodies should determine if consultations should occur with relevant stakeholders and representatives of those potentially impacted to ensure the need of video surveillance is debated and determine if there will be public support of this practice.

Public bodies should also consider providing adequate warning of their intentions to implement the use of video surveillance prior to the practice starting.

II Once the Decision to Implement the Use of Video Surveillance is Made

Some considerations for the public body once the decision is made to implement the use of video surveillance is to determine:

- Is the duty to protect being met?
- What measures can be taken to minimize the impact to personal privacy?
- What safeguards should be put in place to properly protect the personal information?
- How will access to information requests for video surveillance footage be handled?

Is the Duty to Protect being Met?

The Freedom of Information and Protection of Privacy Act (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), *The Health Information Protection Act* (HIPA) and their Regulations provide the rules on when public body/trustee to collect, use and disclose personal information or personal health information. Any collections, uses or disclosures unauthorized by FOIP or LA FOIP would be a privacy breach. Also, these statutes have an explicit duty on public bodies/trustees to protect personal information or personal health information (see section 24.1 of FOIP/23.1 of LA FOIP/16 of HIPA).

Section 24.1 of FOIP/23.1 of LA FOIP/16 of HIPA requires that a public body have administrative, technical and physical safeguards to protect personal information or personal health information.

Administrative safeguards are controls that focus on internal organization, policies, procedures and maintenance of security measures that protect personal information or personal health information. Examples include written policies and procedures, annual training for employees, confidentiality agreements, agreements with information management service providers (IMSPs), auditing programs, records retention and destruction schedules and access restrictions.

Technical Safeguards are the technology and the policy and procedures for its use that protect personal information or personal health information and control access to it. Examples include separate user identifications, passwords, firewalls, identification and authentication controls, virus scanners and audit capabilities in digital systems.

Physical Safeguards are physical measures, policies, and procedures to protect personal information or personal health information and related buildings and equipment, from unauthorized intrusion and natural and environmental hazards. Examples include locked filing cabinets, offices and storage rooms, alarm systems and clean desk approaches.

Section 24.1(a) of FOIP/23.1(a) of LA FOIP/16(a) of HIPA indicates that a public body must protect the integrity, accuracy and confidentiality of the personal information or personal health information in its possession or under its control;

Integrity refers to the condition of information being whole or complete; not modified, deleted or corrupted.

Confidentiality implies a trust relationship between the person supplying information and the individual or organization collecting or using it.

Section 24.1(b) of FOIP/23.1(b) of LA FOIP/16(b) of HIPA indicates that public bodies must protect against any reasonably anticipated:

- threat or hazard to the security or integrity of the personal information or personal health information in its possession or under its control;

- loss of the PI/PHI in its possession or under its control; or
- unauthorized access to or use, disclosure or modification of the personal information or personal health information in its possession or under its control;

Threat means a sign or cause of possible harm.

Hazard means a risk, peril or danger.

Security means a condition of safety or freedom from fear or danger.

Unauthorized access occurs when individuals have access to personal information or personal health information that they do not need-to-know, either by accident or on purpose. This would also qualify as either an unauthorized use or unauthorized disclosure.

A need-to-know is the principle that public bodies and their staff should only collect, use or disclose PI/PHI needed for the purposes of the mandated service. personal information or personal health information should only be available to those employees in an organization that have a legitimate need-to-know that information for the purpose of delivering their mandated services.

An unauthorized collection occurs when personal information or personal health information is collected, acquired, received or obtained by any means for purposes that are not allowed under sections 25, 26, 27, 28 or 29(2) of FOIP/24, 25, 26, 27 or 28(2) of LA FOIP/23, 24 or 25 of HIPA.

Unauthorized use refers to the use of personal information or personal health information for a purpose that is not authorized under sections 27, 28 or 29(2) of FOIP/26, 27 or 28(2) of LA FOIP/26, 27, 28, 29 or 30 of HIPA.

Unauthorized disclosure refers to the act of revealing, showing, providing copies, selling, giving, or relaying the content of personal information or personal health information in ways that are not permitted under sections, 29 or 30 of FOIP/28 or 29 of LA FOIP/27, 28, 29, 30 of HIPA.

Section 24.1(c) of FOIP/23.1(c) of LA FOIP/16(c) of HIPA indicates that public bodies should have education programs in place for their employees which addresses the public body's duties under FOIP/LA FOIP, safeguards the public body has established, the need-to-know and consequences for violating HIPA. The IPC has indicated that annual training is best practice. Annual training should include reminders about mobile security.

This document describes best practices for video surveillance.

What measures can be taken to minimize the impact to personal privacy?

Collection occurs when an individual's image is captured by the video surveillance system. Public bodies who are implementing the use of video surveillance will need to ensure they have proper authority under FOIP/LA FOIP for collecting the personal information of individuals. Some things public bodies should consider:

- Where in the facility will the video surveillance occur? Public bodies should ensure that certain areas with heightened expectation of privacy such as washrooms are not included in video surveillance.
- Is there a policy in place regarding the collection? And has the policy been communicated to staff?
- How will the public body notify individuals of the surveillance/collection of their personal information? Public bodies should ensure notification is posted in high traffic areas where surveillance is in use and have information on who to contact with questions or concerns regarding the video surveillance.
- How will the public body limit the collection of personal information based on the purpose for the collection? Public bodies should consider what hours it is necessary to conduct video surveillance for the purpose it is collecting it in order to minimize the risk of over-collection.
- How will the public body handle potential over-collections of personal information?

What Safeguards Should be put in Place to Properly Protect the Personal Information?

Once public bodies have collected this personal information, they will need to ensure that they are storing the information in a proper manner and have sufficient safeguards to protect it from improper use or disclosure.

- Ensure proper policies are in place for the collection, use, disclosure, destruction and access to information of video surveillance data
- Ensure proper technical safeguards are in place to adequately protect the personal information of individuals collected by video surveillance
- Training for employees that will have access to video surveillance footage
- Determine frequency of audits and what will the audit look for (such as user accesses)
- Need-to-know – limit the number of employees that can access the video surveillance data to those that have a legitimate business need to know the information

How Will Access to Information Requests for Video Surveillance Footage be Handled?

Once a public body has collected an individual's personal information through video surveillance, it would be a record that individuals could submit access requests for. Just as with other records, public bodies will need to determine how they will provide individuals with their right to access this information while protection the personal information (or images) of other individuals captured by video surveillance. Software that allows the ability to blur out images of others may be an option that public bodies want to explore for these purposes.

III AFTER THE IMPLEMENTATION OF VIDEO SURVEILLANCE

Some considerations for the public body after implementing the use of video surveillance is to determine:

- Evaluation and audit of video surveillance programs

Evaluation and Audit of Video Surveillance Program

Once a public body has implemented the use of video surveillance it will need to ensure it is regularly completing audits of this practice and addressing any incidents it encounters. As well, the public body will want to ensure that the practice of video surveillance is regularly evaluated to ensure that it is still a necessary practice. The evaluation could consider the locations of the video surveillance, the hours it is conducting video surveillance or if the surveillance is still necessary for the purpose it was implemented.

IPC Consultation Process

If you are considering the implementation of video surveillance, you can submit your materials for our office's consultation process. Examples of the type of material our office could provide comment on are policies, procedures and/or PIA. While our office prefers that we are provided the opportunity to provide consultative advice prior to the implementation of a program of practice, our office may provide comments on programs or practices already in place. For more information on the consultation process, please see consultation request form under the resource directory at: https://oipc.sk.ca/resources/resource-directory/.

Contact Information

If you have any questions or concerns about these guidelines or if you would like to request an investigation or review involving video surveillance, please contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

intake@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC