Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

AUDIT & COMPLIANCE REPORT P16-01

Over-collected and Overexposed: Surveillance and Privacy Compliance in a Medical Clinic

Drew McArthur
Information and Privacy Commissioner
for British Columbia

December 8, 2016

CanLII Cite: 2016 BCIPC 56
Quicklaw Cite: [2016] B.C.I.P.C.D. No. 56

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

This is the first audit of a private sector business that my office has undertaken in our Audit & Compliance Program. This audit was conducted at a private medical clinic ("Clinic") in B.C. to determine the organization's compliance with legislative requirements relating to collection, use, disclosure, disposal and overall protection of personal information.

In particular, auditors examined the Clinic's privacy management program and its use of video and audio surveillance. The key finding of this audit is that the organization is not authorized to collect personal information through its video and audio surveillance system.

The Clinic currently has video surveillance cameras in its lobby, hallways, back exits, and fitness room and collects the personal information of its employees, customers, and others on a continuous basis: all day, and every day. I find this use of video and audio surveillance to be excessive.

This scenario is now relatively common. We have all become too accustomed to the presence of surveillance cameras in many parts of our lives. Whether we're catching the bus to work, filling a prescription, or shopping for groceries, surveillance has become ubiquitous. As the technology for video surveillance is inexpensive and easily accessible, many public bodies and private sector organizations have implemented surveillance in an attempt to deter crime, gain evidence to help catch and prosecute criminals, and even to manage employee performance.

I have serious concerns about how often we, as citizens, are being recorded, who's watching our activities, and what they are doing with the video record. In some limited circumstances, video surveillance is justified, as detailed in previous decisions summarized in this report. But in other instances, it is invasive and excessive.

Video surveillance carries social impacts. It affects how we behave when we believe we're being watched, inhibiting our freedom of expression, association, and privacy – freedoms that are essential to a democracy. Individuals have a fundamental right to privacy, enshrined in our private and public sector privacy legislation.

As video surveillance becomes more pervasive, I intend to be vigilant in reminding businesses of their obligations to respect privacy rights.

Ultimately, when organizations collect personal information, they are responsible for its protection, use, disclosure, retention and access, which can create considerable liabilities for the organization. An organization must be prepared to provide extracts of recorded video to individuals who request a copy of their personal information, and should have software to blur faces in order to protect the personal information of any third party whose image may have also been captured. As well, any time a business collects personal information, there is a risk of privacy breach, so a business must have adequate protections in place. Surveillance is also susceptible to misuse by those who can access the system and use the video in unauthorized ways.

This audit report should encourage all private businesses in B.C. to reflect on their own practices and amend them if necessary. If you are a business owner or operator, you need to carefully weigh the loss of privacy when considering the potential use of video surveillance. You should only use video surveillance as a last resort after exploring other less privacy-invasive alternatives. And you should only collect the personal information that is absolutely needed for business purposes. A video camera cannot – and should not – replace adequate employee management.

Drew McArthur
Acting Information and Privacy Commissioner
for British Columbia

EXECUTIVE SUMMARY

Under the authority of section 36 of the *Personal Information Protection Act* ("PIPA"), the Office of the Information and Privacy Commissioner ("OIPC") conducted an audit of privacy management practices and the video and audio surveillance system within a medical clinic ("Clinic") in the lower mainland.

Former Commissioner Elizabeth Denham announced this audit after receiving a complaint in early 2016 related to the Clinic's collection of personal information through video and audio surveillance. Through the course of investigating the complaint, auditors identified concerns related to the Clinic's use of video and audio surveillance; the collection, use, disposal and security of personal information; the potential impact of these practices on employees and patients of the Clinic; and the Clinic's privacy management program overall.

The main objectives of the audit were to:

- review the extent to which the Clinic is in compliance with PIPA, OIPC guidelines and Clinic policies and procedures relating to privacy management, video and audio surveillance, and the protection of personal information;
- identify risk factors in the protection of personal information; and
- make recommendations to strengthen Clinic policies and practice.

The lines of inquiry for this audit comprised whether the Clinic:

1. is authorized to collect personal information via video and audio surveillance cameras;
2. has met its obligations under PIPA relating to policies and practices, consent, and the collection, use, disclosure and retention of personal information;
3. protects personal information as required by s. 34 of PIPA; and
4. has a privacy management program with effective policies, processes and reporting mechanisms.

The methodology included an analysis of Clinic policies, practices and training; an on-site inspection of the Clinic; examination of the video and audio surveillance system; and interviews with key Clinic staff. Assessment criteria and tools were based on PIPA obligations, OIPC guidance documents and orders, and the Clinic's policies on privacy, video surveillance and complaints handling processes.

The Clinic collects personal information about its patients, employees, and others who enter the Clinic. For patients, this includes contact information, date of birth, personal health number, medical history, diagnoses, treatments and information on products or services the patient has purchased. For employees, the Clinic collects contact information, social insurance number, date of birth, criminal record history, banking information for payroll purposes, and information related to the individual's employment history with the Clinic. At the time of the audit, the Clinic also collected through video surveillance the personal images and audio recordings of patients, employees and contractors or others who enter the Clinic. Its eight video surveillance cameras were located throughout the facility in the more public areas, such as the lobby, hallways, back exits and workout room.

Key findings are summarized as follows:

- the Clinic is not authorized under PIPA to collect the personal information of its employees, patients, contractors or others via video or audio surveillance, as there is not enough evidence that a safety or security problem exists or evidence of other significant issues such that it would be reasonable or appropriate for the Clinic to monitor and record employees, patient, contractors, or others.
- the Clinic is not in compliance with s. 6 of PIPA because it does not have the express consent of employees, patients, or others who may enter the Clinic; consent is not deemed to have been provided; and the Clinic is not authorized to collect the personal information without the consent of the individuals.
- the Clinic is not in compliance with its duty under s. 34 of PIPA to protect the personal information in its custody or under its control as there are significant issues with the Clinic's storage, security, and disposal of personal information and no privacy risk assessment has been conducted since the inception of the Clinic.
- the Clinic does not have an effective Privacy Management Program in place. Clinic policies were missing essential components. The Clinic does not maintain a personal information inventory or conduct privacy risk assessments, and staff have not received adequate privacy training and education.

This report makes 12 recommendations to the Clinic. These include immediately ceasing the collection of personal information via video and audio surveillance, ensuring the secure storage and disposal of the other personal information it collects, updating its policies and procedures, developing and conducting privacy risk assessments, and providing regular privacy training to staff.

1.0 INTRODUCTION

The Office of the Information and Privacy Commissioner for B.C. ("OIPC") established the Audit & Compliance Program to assess the extent to which public bodies and private sector organizations are protecting personal information and complying with access provisions under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") and the *Personal Information Protection Act* ("PIPA").

PIPA governs the collection, use and disclosure of personal information by provincially regulated private sector organizations. Under the authority of s. 36 of PIPA, the OIPC conducted an audit of privacy management practices and the video and audio surveillance system within a medical clinic in the lower mainland ("Clinic").

Former Commissioner Denham announced this audit after receiving a complaint in early 2016 related to the Clinic's collection of personal information through video and audio surveillance. Through the course of investigating the complaint, the OIPC identified concerns related to the Clinic's use of video and audio surveillance; the collection, use, disposal and security of personal information; the potential impact of these practices on employees and patients of the Clinic; and the Clinic's overall privacy management program.

1.1 Objectives, Scope and Methodology

This audit focussed on the Clinic's compliance with PIPA provisions relating to the collection and protection of personal information in accordance with ss. 6 through 34 of PIPA. The assessment criteria and tools were based on PIPA obligations, OIPC guidance documents and orders, and the Clinic's policies on privacy, video and audio surveillance and complaints handling processes.

The main objectives of this audit were to:

- review the extent to which the Clinic is in compliance with PIPA, OIPC guidelines and Clinic policies and procedures relating to privacy management, video and audio surveillance, and the protection of personal information;
- identify risk factors in the protection of personal information; and
- make recommendations to strengthen Clinic policies and practice.

Utilizing components of compliance assessment, operational audit, program evaluation, and process improvement methodologies, this review included:

- analysis of Clinic policies, practices and training;
- an on-site inspection of the facility;
- an examination of the video and audio surveillance system; and
- interviews with key Clinic staff.

The lines of inquiry for this audit comprised whether the Clinic:

- is authorized to collect personal information via video and audio surveillance cameras;
- has met its obligations under PIPA relating to policies and practices, consent, and the collection, use, disclosure and retention of personal information;
- protects personal information as required by s. 34 of PIPA; and
- has a Privacy Management Program with effective policies, processes and reporting mechanisms in place.

Auditors used the following OIPC documents as background material to aid in planning the scope of this review:

- *Getting Accountability Right with a Privacy Management Program*
- *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations*
- *Guidelines for Overt Video Surveillance in the Private Sector* 2008
- *Tips for Organizations Responding to a Privacy Complaint under PIPA*
- *BC Physician Privacy Toolkit* (complaints handling)
- *Investigation Report F16-01 Sale of Provincial Government Computer Tapes Containing Personal Information*
- *Order P15-01 Park Royal Medical Clinic*
- *Order P13-02 ThyssenKrupp Elevator (Canada) Limited*
- *Order P12-01 Schindler Elevator Corporation*
- *Order P09-02 Shoal Point Strata Council*

In addition to the examination of requested documents provided by the Clinic, auditors conducted an interview in September 2016 with the physician in charge (the owner of the Clinic) and the Clinic's office manager. The interview included questions on:

- personal information collection;
- access to personal information;
- staff training;
- incident management;
- risk assessment;
- the current complaint to the OIPC;
- the video and audio surveillance system; and
- overall challenges and improvements that may be needed within the Clinic's privacy management program.

2.0 LEGISLATION

The purpose of PIPA is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Organizations are responsible for the personal information they collect and they must designate someone within the organization to be responsible for ensuring compliance with the legislative requirements.

Some of the basic requirements in ss. 5 through 19 of PIPA state that organizations must:

- have policies and practices that show how the organization complies with PIPA;
- have a complaints process, should someone wish to complain about the organization's management of personal information;
- collect, use or disclose personal information only: with the consent of the individual, where PIPA permits collection without consent, or where PIPA deems consent to have been implicit;

- collect personal information without consent only where PIPA permits under s. 12, for example, where the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- inform individuals about the purpose for collecting personal information on or before collecting the information directly from them; and
- collect, use or disclose personal information, with or without consent, only for purposes that a reasonable person would consider appropriate.

With regard to employees, organizations may also collect employee personal information without consent where the collection is reasonable for establishing, managing or terminating the employment relationship. In this case, the organization must notify the employee that they will be collecting, using or disclosing the employee personal information (and the purposes for doing so) before collecting, using or disclosing the personal information.

In addition, s. 34 of PIPA requires organizations to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks. Under s. 35, organizations must retain personal information that is used in a decision that directly affects the individual for at least one year after using it and then must destroy the personal information after it is no longer needed for legal or business purposes.

With regard to the specific issue of collection of personal information via video surveillance, OIPC orders and guidance documents[1] have pointed to, at minimum, the following provisions:

- organizations should only use video surveillance as a last resort after other less privacy intrusive measures to achieve the business purposes have been exhausted;
- organizations need to carefully weigh the benefits of collecting and utilizing personal information through video surveillance against the privacy rights of citizens;
- organizations must be able to demonstrate the purpose and legal authority for such collection or use of personal information;
- organizations must limit the collection of personal information to only that which is necessary for the specified business purpose (as such, if video surveillance is deemed necessary as a result of documented risk, then organizations should limit the use and viewing range of cameras as much as possible);

- organizations should provide reasonable and adequate notice to individuals whose personal information would be collected via video surveillance; and
- organizations should regularly audit the access to, and use of, personal information collected via video surveillance and should periodically evaluate whether there is still need for video surveillance.

3.0 OVERVIEW OF CLINIC PROCESSES

The Clinic offers a variety of medical services to its patients. The physician who owns the Clinic (the "owner") designed and built the facility. Physically, the Clinic is located on a high-traffic street; its doors are open to the public and it has several treatment rooms along with an exercise room for use by Clinic patients.

The Clinic collects personal information about its patients, including contact information, date of birth, personal health number, medical history, diagnoses, treatments and information on products or services the patient has purchased. The Clinic also collects employee personal information necessary for maintaining the employment relationship, for example, contact information, social insurance number, date of birth, criminal record history, banking information for payroll purposes, and information related to the individual's employment history with the Clinic. In addition, the Clinic collects the personal images of patients, employees and contractors who enter the Clinic (such as cleaners) via its eight video surveillance cameras located throughout the facility in the more public areas, such as the lobby, hallways, back exits and workout room. The camera in the lobby also records audio of patients, employees and others who enter the Clinic.

The owner is the privacy officer and is responsible for ensuring that the Clinic complies with PIPA. At the time the audit began, the owner reported that the Clinic did not have written privacy policies in place. However, when submitting records for review under this audit two weeks later, he provided a copy of a privacy policy.[2] During early discussions to prepare for the audit, the owner assured auditors that all employees receive information related to privacy and confidentiality within an employee manual that contains the forms and instructions specific to the various Clinic procedures, and that each staff member is required to sign a confidentiality agreement as part of the hiring process.

The owner noted that the surveillance cameras are visible, that signage is posted to notify patients and others entering the Clinic and that staff are aware of the surveillance cameras. He also reported that the office manager reviews camera recordings only when there is suspicion of a breach or other criminal activity.

4.0 FINDINGS

This section summarizes the extent to which the Clinic is complying with relevant sections of PIPA, OIPC guidance documents, and Clinic policies provided for review. Findings are presented with the associated PIPA requirements.

4.1 Policies and Practices – s. 5(a)

As noted above, at the time the audit began, the owner reported that expectations related to privacy and confidentiality were embedded in an employee manual but that no specific separate privacy policy existed. Section 5 of PIPA requires that organizations have policies and practices that show how the organization complies with the legislative requirements.

The guidance document *Getting Accountability Right with a Privacy Management Program* holds that organizations must maintain policies that address their obligations under the law, policies need to be available to employees, and employees should periodically sign off on them. According to the Alberta, B.C. and Canadian Federal Privacy Commissioners, privacy policies need to address, at minimum:

- collection, use and disclosure of personal information, including requirements for consent and notification;
- access to and correction of personal information;
- retention and disposal of personal information;
- responsible use of information and information technology, including administrative, physical and technological security controls and appropriate access controls; and
- provision of a complaints process.[3]

When collecting records for review, the Clinic provided a copy of a privacy policy. Auditors reviewed the policy and found that it contained some of the essential elements of a good privacy policy but was missing others.

The Clinic's policy contained the following:

- discussion of images of individuals collected by Closed Circuit Television ("CCTV") as part of the personal information the Clinic collects;
- comment regarding a commitment to privacy;

- an explanation of the limits to the collection, use and disclosure of personal information;
- a statement that consent is required for the collection of personal information, specifying that express consent in written form is necessary in all circumstances;
- details about the right to withdraw consent;
- information on retention of personal information;
- a statement that individuals have a right to access their own information, including to request correction, and how they may do so;
- information on how to make a complaint or raise concerns with the organization relating to its privacy and security measures; and
- name and mailing address for the privacy officer and the OIPC.

The Clinic's policy did not contain:

- any mention of audio surveillance (collected via the CCTV equipment);
- reference to or explanation of PIPA;
- a description of the personal information, including health information, collected from staff or patients;
- a description of the purposes or reasons for collecting or using personal information (policy simply directed the reader to a privacy statement posted at the Clinic, but auditors could not locate such a statement);
- sufficient detail about how or when personal information may be disclosed to other parties;
- mention of the PIPA requirement to retain, for at least one year, personal information used to make a decision that directly affects an individual;
- sufficient detail relating to security measures; or
- an accurate explanation of who can access video or audio recordings.

The Clinic did not provide any evidence that employees had reviewed the policies. This could be accomplished, for example, with a signed confidentiality agreement that includes a statement that employees read and understood the Clinic's privacy policy. There was also no evidence that the Clinic employed many of the practices detailed in the privacy policy.

The policy referred to a written privacy statement, a disclosure consent form, and annual security and privacy audits and noted that only the privacy officer may access the CCTV equipment. Auditors were unable to locate such forms. They were also unable to find evidence that the Clinic had conducted any audits. They did find, however, that staff other than the privacy officer had access to the CCTV monitors and equipment to retrieve extracts.

RECOMMENDATION 1: The Clinic should update its privacy policy to:

a. state that personal information is collected in accordance with provisions set out in PIPA;

b. include a definition of personal information that is consistent with B.C. legislation;

c. accurately describe:
   i. the personal information it collects from patients and employees,
   ii. the purposes for doing so,
   iii. occasions where the personal information may be disclosed,
   iv. provisions under PIPA for retaining personal information, and
   v. the privacy and security measures used to protect against unauthorized disclosure of personal information (including accurately reflecting access provisions and any physical or technological security controls in place);

d. ensure that provisions outlined in the policy for obtaining consent for the collection, use or disclosure of personal information accurately reflect the Clinic's practices;

e. ensure that the forms, documents and processes listed within the policy reflect actual forms, documents and processes used by the Clinic, or update the policy to remove these; and

f. include additional contact information for the privacy officer, such as an email address or telephone number.

RECOMMENDATION 2: The Clinic should formally review its privacy policies at a minimum of every three years to ensure policies are relevant and up-to-date.

4.2 Complaints Process – s. 5(b)

PIPA requires that organizations have a complaints process in place. In the *BC Physician Privacy Toolkit*,[4] an accessible and effective process for responding to privacy complaints is a key function of the privacy officer and an important part of managing privacy risks within a practice, and it helps to promote accountability, openness, and trust.

The *Toolkit* suggests that physicians develop and document the complaint procedure and consider developing a complaint form to assist in recording the complaint and collecting the necessary information required to investigate and respond. Physicians are to ensure that the complaint process is fair, impartial, and confidential and should document the investigation. They should notify complainants of the outcome of the investigation and the steps taken to rectify their concerns. In addition, physicians should inform complainants of their right to appeal to the OIPC if they are not satisfied with the response to their complaint. These same principles apply to any organization.

As noted, the OIPC received a complaint from a former employee about the Clinic's collection of the employee's personal information via video and audio surveillance. Correspondence between the complainant and the owner suggested that the Clinic did not have a complaint management process in place at the time of the complaint, nor did it appear that the Clinic conducted any type of investigation into the former employee's privacy complaint.

PIPA does not specifically require policies or processes to be written. However, as noted in Order P15-01,[5] organizations must at least be able to demonstrate that they have considered what the process for handling a privacy complaint would be. Written policies or procedures would also provide evidence, if an organization needed to demonstrate that a complaints process exists. The OIPC guidance document on investigating complaints under PIPA recommends a three-step process: clarifying the complaint, getting information and making findings, and taking action.[6] Ultimately, the Clinic's handling of the complaint did not satisfy the requirements for dealing with complaints in s. 5 of PIPA.

As noted previously, the Clinic developed a written privacy policy during the course of the audit. The policy includes basic information on how to make a complaint or raise concerns with the organization about the handling of personal information and notes that the Clinic would investigate and respond to such complaints or concerns. It also includes contact information for the owner, as well as the OIPC.

4.3 Collection of Personal Information – ss. 6-10, 12, 13

Section 6 of PIPA prohibits organizations from collecting, using or disclosing personal information about an individual except in certain circumstances, such as where the individual has consented to its collection, use or disclosure. It follows that, if an organization is not permitted to collect personal information about an individual, it would therefore not be permitted to use or disclose that personal information either.

In accordance with ss. 7, 8 and 12 of PIPA, organizations may collect personal information in circumstances where they have obtained the consent of the individual, where PIPA deems consent to have been implicit, or where PIPA permits collection without consent. A key component of consent is that the individuals from whom personal information will be collected are aware of the purposes for the collection of their personal information.

In the *Guide to PIPA*, the OIPC provides basic principles for organizations to consider when determining what personal information to collect:

- You must limit the collection of personal information to that which is necessary for the purposes you identify.
- You can only collect, use or disclose personal information if it is reasonable in regards to the sensitivity of the personal information in the circumstances.
- You cannot require someone to consent to the collection, use or disclosure of personal information beyond what is necessary to provide him or her with a product or service.
- Personal information should be collected by fair and lawful means.[7]

As noted above, the Clinic collects personal information about its patients (including medical history, diagnoses and treatments, date of birth, personal health number) and employees (including social insurance number, date of birth, criminal record history, and banking information). In addition, the Clinic collects images and voice recordings of both patients and employees via its video and audio surveillance system.

4.3.1 Provision of Consent

In order to obtain consent for the collection of an individual's personal information, s. 7 of PIPA sets out two requirements. First, the organization must provide the individual with notification of the purposes for the collection of the information before or at the time consent is sought. Notification can be provided verbally or in writing and, as per s. 10(1), should be sufficiently detailed for the individual to understand the reasons and means for the collection. The second

requirement is that the individual's consent is provided in accordance with the Act. PIPA considers consent to be valid only if it is informed by the purpose for which the information will be collected.

The complainant who raised the concern about the Clinic's procedures with the OIPC alleged that, at the time of their employment, the Clinic did not have privacy policies in place or other written materials to notify employees about the collection of their personal information. The policies the Clinic provided for review during the audit indicate that CCTV is used to collect information. Nevertheless, the policies do not mention the audio recording, nor do they provide detail as to the types of personal information collected or the purposes for how such information would be used.

The owner claimed that the Clinic informed all employees about the existence of video surveillance and that the employees understood that it was for security purposes. Two staff members provided letters related to video surveillance for review. In the letters, the staff members expressed appreciation for the existing surveillance for security purposes and for one occasion where a staff member had miscounted money.

In addition to general security, the owner provided the following additional reasons for the collection of personal information via video surveillance at the Clinic:

- liability protection and client protection – by documenting how injuries occur in the exercise room and who is at fault, and the ability to prevent injuries if improper use of exercise equipment is observed;
- monitoring staff – to determine whether staff miscounted money and monitoring for occasions where staff may leave during or before their shift is over; and
- security of equipment and merchandise – expensive equipment and products are accessible to staff, visitors, and cleaning contractors after hours.

Whether or not the employees were aware of or appreciated the existence of the video or audio surveillance, there was no evidence to show they were aware of all the ways their personal information collected via video or audio surveillance would be used.

As such, the Clinic has not provided sufficient notice to its employees. The Clinic could attempt to obtain express consent from its employees through, for example, the use of a comprehensive written privacy policy and a signed express consent form.

With regard to patients, contractors, or others who may enter the premises, the Clinic does not have appropriate information available about the purposes for collection of their personal information via video or audio surveillance nor how such information would be used. The purposes for collection were not included in the privacy policy, there was no privacy statement at the Clinic, and patients were reportedly only asked to provide consent for specific procedures and not for the collection of their personal information.

In addition, the signage at the Clinic entrance was insufficient to notify individuals of the existence of surveillance cameras and did not mention audio recording at all. The wording on the signage at the Clinic entrance stated simply that video surveillance is provided by a certain security company and included contact information for that company. However, as it did not describe the purposes for the Clinic's collection of personal information and did not mention the collection of audio, it is not sufficient notification under s. 10 of PIPA.

Even if the wording of the signage were appropriate, there would need to be signs posted at all external entrances and elsewhere inside the Clinic where it is not obvious that surveillance exists. Even with appropriate signage, the Clinic has not obtained the express consent of each individual prior to their entry into areas covered by video recording.

4.3.2 Implicit Consent

Section 8 of PIPA provides for deemed consent to the collection of personal information if, at the time consent is deemed to have been given, the purpose for collection would be considered obvious to a reasonable person and the individual voluntarily provides their personal information to the organization for that purpose.

With regard to information such as patient medical history and personal health number, patients understand that the collection is for the purposes of diagnosis, treatment and billing. For employee personal information, employees understand that the collection of information is for screening during the hiring process and for managing payroll and tax deductions. In these circumstances, the Clinic may deem that individuals have provided consent for the collection and use of their personal information for these purposes.

However, the purposes for collecting images and audio recording via the Clinic's video and audio surveillance of patients, employees, contractors or others entering the Clinic, are not obvious.

Furthermore, the Clinic uses the personal information collected via video and audio surveillance for purposes beyond security, including liability protection, monitoring staff, and auditing for internal losses. Relevant case law has found that in some circumstances video surveillance is appropriate for the purposes of security and protection of property. There are no precedents in support of using it for purposes of liability protection or managing employees.

Even if the purposes for collection and use were appropriate, not all of the purposes for which the Clinic collects and uses the personal information would be obvious prior to an individual's entry into the Clinic. As such, the Clinic cannot rely on s. 8 provisions of PIPA to ensure that it has deemed consent for the collection of personal information.

4.3.3 Collection without Consent

In reality, consent is never an authority for collection of personal information via video surveillance because it is not practical to obtain the consent of everyone whose image is captured prior to their image being captured. In cases where video surveillance is authorized, it is where organizations meet the criteria to collect personal information without consent in accordance with s. 12 of PIPA

Section 12(1) of PIPA allows for collection without consent in certain circumstances, for example:

> (a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way,
>
> (b) the collection is necessary for the medical treatment of the individual and the individual is unable to give consent,
>
> (c) it is reasonable to expect that the collection with the consent of the individual would compromise the availability or the accuracy of the personal information and the collection is reasonable for an investigation or a proceeding…

None of the circumstances outlined in s. 12(1) apply to the context of the Clinic's collection via video or audio surveillance.

In accordance with s. 13 of PIPA, organizations may collect employee personal information without the consent of the individual, if s.12 allows for the collection without consent. Section 13 also permits collection, after appropriate notification, if the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual. As noted above, the Clinic's privacy policies did not include the purpose for such collection, nor did they contain an express consent form, or otherwise provide appropriate notification to inform employees that their personal

information would be collected through video and audio surveillance. In any event, it would not be reasonable to use video or audio recordings for establishing, managing or terminating an employment relationship in this context. As such, the provisions of s. 13 of PIPA do not apply to allow collection without consent.

In summary, the Clinic does not have consent for the collection of personal information as per ss. 7 and 8 of PIPA and is also not authorized under s. 12 of PIPA to collect personal information without the consent of the individuals. The Clinic does not have the consent of employees, patients, or others who may enter the Clinic in accordance with s. 7 and s. 6(2)(a) and none of the provisions of s. 8 and s. 6(2)(c) apply that would give authority for the Clinic to consider it had implicit consent for the collection. The Clinic is also not authorized under ss. 12(1)(a) or 6(2)(b) to collect personal information without the consent of the individuals involved.

4.4 Limitations on Collection and Use – ss. 11 and 14

Even if the Clinic was able to obtain consent for the collection from all individuals, it would still have to ensure that the collection and use of personal information is appropriate before collecting that personal information.

Under ss. 11 and 14 of PIPA, organizations may collect or use personal information only for purposes that a reasonable person would consider appropriate in the circumstances, and that fulfill the purposes that the organization identifies under s. 10(1) or are otherwise permitted under PIPA. This is known as the “Reasonable Person Test”.

There is, in effect, a two-part test that an organization must meet before it is authorized to collect personal information or employee personal information. It must meet both parts of the test. The first part is that it must have authority through:

- Consent from the individual;
- Implicit consent; or
- Authority to collect without consent.

The second part of the test is that a reasonable person also must consider the collection to be appropriate.

4.4.1 Reasonable Person Test

Even where a person consents, PIPA prohibits organizations to collect the personal information unless, as assessed against an objective standard and in context, the purposes for which it is collected are appropriate.

OIPC orders P12-01 and P13-02 provide direction for determining what is appropriate.[8] These considerations and their applicability to the current context include:

- ***The sensitivity of the personal information***

Generally personal information collected through video surveillance in public areas is not particularly sensitive compared to other types of personal information, such as medical or criminal history, with perhaps the exception of surveillance in the Clinic's exercise room. However, when viewed over time and collected with corresponding audio surveillance, these recordings contain a large amount of information about employees and patients and can inadvertently capture very sensitive personal information.

- ***The amount of personal information collected or used***

The Clinic's surveillance system records audio and video non-stop, all day, every day. It is reasonable to expect that this continuous, real-time collection of video and audio information would have personal and social effects on employees while they are under surveillance. An employer must limit collection or use of employee personal information to that which is reasonably required for the employer's purpose.

- ***The manner of collection***

Despite the lack of appropriate notification, employees were likely aware of the video and audio surveillance. However, patients, contractors and others entering the premises may not have been aware of the video system, nor that audio recording existed in the lobby area.

- ***The use of the personal information***

The owner reportedly monitors the CCTV live in his own office (which is not accessible to the public or patients), as opposed to being viewed only after a triggering event. In addition, while employees, patrons or others would not likely assume the recordings would be used for anything other than for security, video recordings were used for monitoring staff, to limit business liability in

documenting potential injuries, and for protection against theft by patients, employees and contractors. However, personal information may only be used for purposes for which individuals have been notified and which a reasonable person would consider appropriate. In addition, video surveillance should not be used to replace adequate training, education, and supervision of employees.

- ***Whether less intrusive alternatives have been attempted***

Video surveillance should only be used as an avenue of last resort after other possible solutions have been exhausted. While other security measures exist at the Clinic, including a panic button, no alternatives were attempted prior to the installation of the video and audio surveillance, which occurred as part of the construction of the Clinic building. In addition, with regard to liability protection, monitoring staff, and auditing for internal losses, the Clinic had not reviewed or implemented less privacy invasive alternatives in the five years it has been operating.

- ***The likelihood of effectiveness in achieving its purpose***

In order to determine the likelihood that video and audio surveillance would be effective for achieving the purposes for which personal information is collected, one must consider the severity of the issue it is intended to prevent, the frequency of the issue occurring with regard to each purpose, the sensitivity of the information being collected, and the ability of surveillance to act as a deterrent.

These criteria have determined the outcome in other cases that have examined whether video surveillance is authorized by law. There are a number of cases that have found video surveillance to be authorized. One case under the federal *Personal Information Protection and Electronic Documents Act* is *Eastmond v. Canadian Pacific Railway*.[9] This case involved video surveillance of a rail yard, where there was clear evidence of a significant problem that could not be addressed by other means. The rail yard covered 432 acres. There had been 148 incidents of “break-ins, thefts, trespassers, mischief, workplace violence, harassment, tampering with equipment, vehicle accidents and personal injury.” The collection of personal information was limited.There were only two cameras located at the entry points. Access to the recordings was restricted and limited. The records were not viewed unless there was a report of an incident requiring investigation.

There was another case under the Alberta *Personal information and Protection of Privacy Act*.[10] This one concerned the use of video surveillance in a men's changing room at a fitness club. The fitness club had installed the cameras only after more than 900 incidents of theft and property damage over a three-year period and only after it had tried other measures to prevent such incidents that had failed. Incidents of theft declined from 400 per year to ten per year over the two years after the equipment was installed. The Alberta Commissioner found that the level of theft and property damage created a legitimate issue and that the organization had gone to great lengths to find alternative solutions before resorting to video surveillance.

PIPA authorizes the implementation of video surveillance in accordance with the reasonable person test only where there is a real and serious threat to personal safety or the security of property, the organization has tried all reasonable alternatives without success, and there is a reasonable prospect that the video surveillance will address those threats. As the above examples demonstrate, these conditions must exist prior to the implementation of the video surveillance. Organizations must not collect personal information through video surveillance, proactively, prematurely, out of an abundance of caution, or "just in case".

The Clinic is currently using the video surveillance for a variety of purposes. They are listed below with an analysis as to whether they meet the criteria of the reasonable person test.

Security: While, in some cases, the presence of video surveillance may act as a deterrent to potential criminals, there is no evidence to suggest that the Clinic would experience repeated break-ins, robberies, other theft of products, supplies or money, or injury to persons without video surveillance. Since 2011, there has only been one such incident, and the presence of video surveillance did not prevent the crime nor did it assist in finding the individual responsible. Given that the Clinic did not have signs in place to notify individuals of the existence of video surveillance until after July of 2015[11] it is unlikely that potential criminals would have been aware of its existence.

Liability protection and client protection in the exercise room: Most individuals using the exercise equipment are reportedly accompanied by a personal trainer. Considering that individuals are not often alone in the exercise room, and that, as noted by the owner, there is often only one patient at a time in the Clinic; it is unlikely that individuals would tamper with the exercise equipment. Even if they did, the severity of the issue is not likely to be very high. In addition, businesses with exercise equipment must expect normal wear and tear and the risk of

occasional injury. The Clinic has provided no evidence of either wilful or excessive damage to its equipment or of serious or repeated injuries occurring. There is no reason to expect that video surveillance would reduce business liability associated with a potential patient injury in the exercise room or the potential for vandalism.

Monitoring staff: While the presence of video surveillance may deter an employee from stealing money from the till, it will not deter the miscounting of money. This is also an infrequent event. The owner noted that there had only been one occasion where an employee miscounted money (in this case $100). According to the owner, had the video surveillance not aided in determining that a miscount occurred, as opposed to money missing from the till, he would have terminated the employee. However, the severity of the issue, even if $100 were missing, is negligible especially when taken on balance with the invasiveness of the video and audio surveillance. The loss of privacy is disproportionate with the loss of $100. With regard to "time theft," the owner noted that video showed one instance where the former employee who complained to the OIPC ignored phone calls and abandoned the building for five minutes. As such, the presence of video surveillance did not deter the employee. Either way, it is not appropriate to use video surveillance as a way to replace proper management and supervision in this context.

Security of equipment and merchandise: Again, while the presence of video surveillance may deter employees, patients, contracted cleaners, or others from stealing merchandise, the frequency with which such theft occurs is infrequent and relatively minor. The Clinic noted that there had only ever been one incident where a sample product went missing and, in that instance, they determined it was not of sufficient value to review video recordings in an attempt to determine who was involved or how the sample went missing.

In applying the above tests to determine whether the installation of video and audio surveillance is reasonable or appropriate, the current circumstances of this Clinic do not warrant the intrusiveness of video and audio surveillance. There is not enough evidence that a serious safety or security problem, or other significant issue, exists that would render it reasonable or appropriate for the Clinic to collect and record the images of employees, patient, contractors, or others through video surveillance.

As noted in OIPC Order P09-02:

> Decisions about whether to implement video surveillance should not be swayed unduly by the general appeal of technological solutions. They should be based on an assessment, in the circumstances of each case, of the real need for surveillance of this kind, its reasonably expected

> benefits and the impact of its use on privacy. Video surveillance should be used only in response to a real and significant security or safety problem.[12]

Therefore, based on the analysis above, the Clinic is not authorized under ss. 11, 12 or 13 of PIPA to collect the personal information of its employees, patients, contractors or others by video or audio surveillance. The collection of this personal information does not meet the first part of the two part test. The Clinic does not have the consent of every individual who is captured on the records. Nor does the provision of implicit consent apply. There is no authorization to collect personal information without consent. In addition, it has not met the second part of the test, as a reasonable person would not consider the collection to be appropriate.

The fact that the Clinic has collected and subsequently used personal information for purposes beyond what a reasonable person would consider appropriate, and that they have not provided adequate notification as described under s. 10(1), means that the Clinic is in direct violation of ss. 11 and 14 of PIPA. Consequently, the Clinic should immediately cease further collection or use of personal information or employee personal information by video or audio recording.

RECOMMENDATION 3: The Clinic should immediately cease the collection of personal information via video and audio recording equipment.

The OIPC also suggests that the Clinic disable and remove video and audio recording equipment and destroy all existing records containing personal information collected via video or audio surveillance.

In future and prior to any re-installation of CCTV, the Clinic would have to justify the need for video surveillance. The Clinic should document any serious and substantial issues that occur, and first attempt to address them through less intrusive means. Only if it has exhausted other methods, may the Clinic implement CCTV, and only for the purposes of addressing the serious and substantial problem(s). Should the Clinic have need in future to collect personal information via CCTV, the owner must provide appropriate notification and consent, as PIPA requires. The Clinic may only capture and use the minimum amount of footage necessary to address the documented problem(s). It should not reinstall audio surveillance.

4.5 Disclosure – ss. 17-19

Part 6 of PIPA sets out provisions for the disclosure of personal information about an individual. Relevant sections include ss. 17 through 19, which restrict disclosure to:

- purposes that a reasonable person would consider appropriate and fulfill the purposes that the organization discloses under s. 10(1);
- limited circumstances if the organization does not have consent from the individual; or
- purposes of establishing, managing or terminating an employment relationship between the organization and the individual.

During the inspection and interview with Clinic staff, the owner noted that, with one exception, the only disclosures of personal information occur where the patient has consented and consent forms have been provided to the Clinic (for example, involving requests by the Insurance Corporation of British Columbia or by the patient for their own records). The exception noted by the owner was when the Clinic provided video and audio evidence to the police in response to the robbery that occurred at the Clinic.

With regard to the complaint received by the OIPC, the complainant asked whether the Clinic had shared their personal information collected via video and audio surveillance with anyone. The owner and office manager noted that they were the only two individuals to have reviewed footage involving the complainant and that they did not provide access to or disclose the information to any other individual.

4.6 Retention of Personal Information – s. 35

Organizations must destroy personal information (including employee personal information) once it is no longer needed for legal or business purposes, unless they have used the personal information in a decision that directly affects an individual. If used in such a decision, they must retain the personal information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

According to the Clinic owner, paper records relating to patients are scanned into their electronic patient information system and subsequently destroyed, with the only paper record remaining being a simple folder with a patient's contact information, date of birth, personal health number and the dates that the patient visited the Clinic. The Clinic uses electronic patient records for business

purposes and for providing historical medical information relating to patients. These records are retained in the electronic system.

With regard to video and audio surveillance recordings, unless an extract is copied, the existing CCTV system retains the records for two to three weeks and then the system automatically overwrites with newly recorded information. The only time extracts were made, according to the owner and the office manager, were after the robbery and during the period where the employment of the person who complained to the OIPC was being terminated.

With the robbery, a copy was provided to police. With the complainant, the office manager saved a copy of relevant footage onto a mobile device and, after viewing with the owner, reportedly deleted the footage from that device approximately two days later.

4.7 Protection of Personal Information – s. 34

Section 34 of PIPA requires an organization to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

Reasonable security arrangements, as discussed by former Commissioner Loukidelis in Investigation Report F06-01 are:

> …to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.[13]

In discussing what reasonable security arrangements entail in a given case, Loukidelis identified the following factors to consider:

- the sensitivity of the personal information;
- the foreseeability of a privacy breach and resulting harm;
- the generally accepted or common security practices in a particular sector or kind of activity;
- the medium and format of the record containing the personal information;
- the prospect of criminal activity or other intentional wrongdoing; and

- the cost of security measures.

The general concept is that the more sensitive the personal information, the greater likelihood of harm resulting from a breach to occur, the stronger security measures that need to be in place. To meet the reasonableness standard for security arrangements, organizations must ensure that they have appropriate administrative, physical and technical safeguards.

4.7.1 Administrative Controls

Administrative controls include internal organizational actions or processes to assure proper management of personal information. Types of administrative controls relevant to the current context included: policies, personal information inventory, risk assessment, and training and education.

- ***Policies***

As noted above, organizations must have policies and practices in place to ensure they can meet their obligations under PIPA. Organizations must also have a complaints process in place, should someone have concerns about handling of personal information. The Clinic adopted privacy policies that included many of the areas that need to be addressed, though revisions need to be made to these policies to include a description of the personal information collected from staff and patients; a description of the purposes for collection, use, or disclosure of personal information; retention periods; and more detail relating to the security measures in place.

- ***Personal Information Inventory***

According to the Alberta, B.C. and Canadian Federal Privacy Commissioners, understanding and documenting the types of personal information that an organization collects and where it is held are critically important. Every organization needs to determine:

- what personal information it holds and where it is held (within the organization or by third parties, for example) and document this assessment;
- why it is collecting, using or disclosing personal information and document these reasons; and
- the sensitivity of the personal information it holds.[14]

At the time of the audit, the Clinic did not maintain a separate inventory, list or document that summarizes types of personal information collected, the purposes for collection, or the sensitivity of the information.

According to the owner, patient information is kept mainly in the Clinic's electronic medical record (EMR) system and the scheduling system. Paper records are also kept relating to the scheduling of patient visits (these typically include patient name, contact information, date of birth, personal health number and date of appointment). Employee information is retained mainly on the Clinic's network drives and in the system used for scheduling patient appointments.

> **RECOMMENDATION 4:** The Clinic should create and regularly maintain a personal information inventory related to the collection of personal information from patients and employees. This inventory should include a list of each type of information collected; where it is stored; the reasons for collection and how the Clinic intends to use or disclose the information; and the sensitivity of the information.

- ***Risk Assessment***

Privacy risk assessments are internal or external reviews of an organization's compliance with relevant legislation and organizational privacy policies and procedures. These risk assessments also include a review of the need for collection of each type of personal information and of the safeguards employed to ensure that an organization is adequately protecting the personal information it collects.

The owner opened the Clinic after designing and building it with security in mind. Privacy risk assessments of organizational practices and personal information safeguards have never been conducted. While the privacy policy states that the Clinic conducts regular risk assessments, the owner noted during the interview that he designed the Clinic so that he would not have to. He further stated that the video surveillance may be helpful in case of an incident and that he ensures that systems are in place and properly functioning on a daily basis. The owner, however, was referring to systems geared more toward theft protection than the protection of employee or client privacy with regard to their personal information.

Privacy safeguards may overlap other safeguards, such as procedures employed to protect against theft of money or product. However, privacy risk assessments need to be geared specifically toward the protection of personal information and

need to ensure the organization limits collection to only the types and amount of personal information necessary to accomplish the purposes for collection.

> **RECOMMENDATION 5:** The Clinic should develop formal procedures and conduct, at least annually, privacy risk assessments to ensure that:
>
> a. adequate administrative, physical and technological safeguards are in place to protect the personal information it collects; and
>
> b. collection is limited to only the personal information necessary for the purposes identified.

- ***Training***

Training and general education for employees is essential to protecting personal information. These activities need to occur regularly and the content needs to be periodically reviewed and updated as necessary.

During the audit, there was no specific privacy training program in place at the Clinic. However, in preliminary conversations, the owner reported that he gives employees access to information on privacy expectations within the employee manual, instructs them not to share private information, and requires them to sign a confidentiality agreement as part of the offer of employment.

Upon review of the aforementioned documents, auditors found that the offer of employment did not refer to maintaining confidentiality of personal information, only business information.

In addition, the employee manual contained two references about protecting personal information:

1. The list of job duties for medical office assistants included activities such as answering phones, keeping appointments, checking email, tidying rooms and: “protect[ing] patients' rights by maintaining confidentiality of personal and financial information.”
2. A separate sheet relating to disclosure of patients personal information simply noted that “Patient’s information is not to be disclosed to anyone not involved directly in patient’s care without the patient’s written consent”.

These instructions are still not sufficient to ensure that employees understand, for example:

- The concept of personal information or disclosure within the Clinic setting;
- the Clinic's existing safeguards;
- the Clinic's policies and procedures with respect to privacy protection and individual access to their own records;
- legal obligations and the owner's expectations for protecting personal information, and what can happen if obligations or expectations are not met; or
- procedures for responding in the event of a privacy breach or information incident (such as misdirected faxes or mail, leaving email addresses viewable in group emails, inappropriate disposal of documents, or disclosure of passwords).

The Clinic needs to put more effort into ensuring that employees fully understand the importance of privacy protection and the Clinic's expectations for how that would be accomplished. As well, Clinic staff need initial and refresher privacy training geared toward the protection of personal information, and should be asked to sign a formal agreement that shows they have received and understood the training and agree to abide by the Clinic policies relating to disclosure.

RECOMMENDATION 6: The Clinic should develop and provide regular privacy training and education to all staff, with initial training to occur within three months of receiving this report.

RECOMMENDATION 7: The Clinic should formally review this training and education at a minimum of every three years and update as necessary.

RECOMMENDATION 8: The Clinic should develop and request that all Clinic staff sign an agreement related to the protection of personal information at the completion of privacy training. This agreement should be reviewed and re-signed annually by all Clinic staff.

4.7.2 Physical and Technological Security Controls

Auditors noted several appropriate physical and technological security safeguards either through inspection of the Clinic or during the interview with the owner and the office manager. With regard to technological security, the auditors did not review any security controls within the EMR system.

The owner reported or the auditors observed the following physical and technological security safeguards:

- the CCTV monitor is in the owner's office and cannot be viewed from elsewhere in the Clinic;
- the door to the owner's office is lockable and is kept closed and locked when the owner is not at the Clinic;
- a panic button exists for employee use that, when pressed, alerts a security company of an emergency (this provides an alternative measure for the physical security of employees);
- Clinic staff rarely use paper records and, when they do, they scan pertinent information into the EMR and then dispose of the paper copy;
- the Clinic does not generally transport personal information on portable storage devices (on the occasion where a video and audio extract of the complainant was saved, it had been saved onto a USB and was deleted shortly after making the copy and did not leave the Clinic);
- the computer with employee information for management and payroll is in the owner's office and is reportedly only accessed by the owner and the individual who manages the payroll. Reportedly only the owner and the payroll manager know the password to the computer;
- EMR data are encrypted and housed on a local server at the Clinic;
- role-based access was in place with the medical office assistants only being able to access to a limited amount of patient information; and
- there is no internet access from the Clinic computers which, according to the owner, is for security purposes.

Auditors found the following issues with the Clinic's physical and technological security safeguards:

- Clinic staff manually tear paper records and dispose of them with the regular garbage as the Clinic did not have a shredder;

- paper records are stored on a shelf behind the reception desk, which is separated from the public, but they are not kept in a locked facility;
- the CCTV is live monitored in real-time during the workday as opposed to turning off the monitor and viewing recordings only after an incident;
- the owner keeps the door to his office open and CCTV monitors may be viewed by other staff entering his office;
- the owner and office manager have not kept logs (due to the limited frequency) of when, why and by whom the CCTV or audio recordings may have been accessed, reviewed or disclosed to third parties (e.g., police);
- the owner has not conducted an internal audit of the access to and use of personal information within the Clinic; and
- the owner was unaware as to whether a confidentiality agreement relating to the protection of employee or patient personal information was in place with the software company who manages the Clinic's EMR.

There are significant problems with the Clinic's storage, security, and disposal of personal information. In addition, since the inception of the Clinic, the owner has not conducted a privacy risk assessment to review security safeguards. As such, the Clinic is not in compliance with its duty under s. 34 of PIPA to protect the personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.

RECOMMENDATION 9: The Clinic should shred paper records containing patient or employee personal information when disposing of the records.

RECOMMENDATION 10: The Clinic should store paper records securely in locking cabinets or behind locked doors and lock cabinets and doors when access to records is not necessary.

RECOMMENDATION 11: The Clinic should develop formal procedures and conduct regular audits of access to and use of personal information within the Clinic.

RECOMMENDATION 12: The Clinic should immediately ensure that a confidentiality agreement is in place with its EMR software support company with respect to the protection of employee and patient personal information.

5.0 ACCOUNTABLE PRIVACY MANAGEMENT

In order to aid organizations in understanding expectations for the protection of personal information, the B.C. OIPC partnered with the Alberta OIPC and the Office of the Privacy Commissioner of Canada to provide guidance by developing the following document: *Getting Accountability Right with a Privacy Management Program*.[15]

Accountable privacy management begins with having an appropriate framework or supporting infrastructure in place to ensure the adequate protection of personal information in an organization's custody or under their control. The central tenets of such a privacy management program include:

- **Organizational commitment** – buy-in from the top, establishing a privacy officer, appropriate resources assigned to the privacy office, and reporting mechanisms to ensure the right people know how the privacy management program is structured and functioning;
- **Program controls** – maintaining a personal information inventory, up-to-date policies, risk assessment tools, training and education, breach and incident management response protocols, management of service providers, and external communication relating to individual privacy rights and the organization's program controls; and
- **Ongoing assessment and revision** – reviewing how the organization will monitor and assess the effectiveness of the privacy management program, having a schedule of when policies and program controls will be reviewed, and revising program controls as necessary (including updating the personal information inventory, revising policies, conducting privacy impact and security threat and risk assessments, modifying training and education, reviewing and fine-tuning contracts with service providers and updating external communications).

As evidenced throughout the report, the Clinic is lacking in each of the three main components that make an effective privacy management framework.

Commitment from senior managers is critical to building and maintaining an accountable privacy management program. Compliance with B.C.'s privacy legislation requires organizations to have a governance structure in place, with processes to follow and the means to ensure that they are being followed. An effective privacy management program would make it easier for the Clinic to ensure it has the necessary physical and technological security safeguards to meet its legislative obligations.

6.0 RECOMMENDATIONS

The following recommendations comprise a mixture of best practices that, when implemented, will help ensure the owner is in compliance with his legislative obligations for protecting personal information in the care or under the custody of the Clinic.

To assist with implementation, the recommendations are sorted into the following thematic groupings:

- policy and procedures;
- personal information collection and privacy risk assessments;
- training and confidentiality agreements; and
- storage, disposal and security safeguards.

RECOMMENDATIONS: POLICY & PROCEDURES

1. The Clinic should update its privacy policy to:
    a. state that personal information is collected in accordance with provisions set out in PIPA;
    b. include a definition of personal information that is consistent with B.C. legislation;
    c. appropriately describe:
        i. the personal information it collects from patients and employees,
        ii. the purposes for doing so,
        iii. occasions where the personal information may be disclosed,
        iv. provisions under PIPA for retaining personal information, and
        v. the privacy and security measures used to protect against unauthorized disclosure of personal information (including accurately reflecting access provisions and any physical or technological security controls in place);
    d. ensure that provisions outlined in the policy for obtaining consent for the collection, use or disclosure of personal information accurately reflect the Clinic's practices;

e. ensure that the forms, documents and processes listed within the policy reflect actual forms, documents and processes used by the Clinic, or update the policy to remove these; and

f. include additional contact information for the privacy officer, such as an email address or telephone number.

2. The Clinic should formally review its privacy policies at a minimum of every three years to ensure policies are relevant and up-to-date.

RECOMMENDATIONS: PERSONAL INFORMATION COLLECTION & PRIVACY RISK ASSESSMENTS

3. The Clinic should immediately cease the collection of personal information via video and audio recording equipment.
4. The Clinic should create and regularly maintain a personal information inventory related to the collection of personal information from patients and employees. This inventory should include a list of each type of information collected; where it is stored; the reasons for collection and how the Clinic intends to use or disclose the information; and the sensitivity of the information.
5. The Clinic should develop formal procedures and conduct, at least annually, privacy risk assessments to ensure that:
   a. adequate administrative, physical and technological safeguards are in place to protect the personal information it collects; and
   b. collection is limited to only the personal information necessary for the purposes identified.

RECOMMENDATIONS: TRAINING AND CONFIDENTIALITY AGREEMENTS

6. The Clinic should develop and provide regular privacy training and education to all staff, with initial training to occur within three months of receiving this report.

7. The Clinic should formally review this training and education at a minimum of every three years and update as necessary.

8. The Clinic should develop and request that all Clinic staff sign an agreement related to the protection of personal information at the completion of privacy training. This agreement should be reviewed and re-signed annually by all Clinic staff.

RECOMMENDATIONS: STORAGE, DISPOSAL AND SECURITY SAFEGUARDS

9. The Clinic should shred paper records containing patient or employee personal information when disposing of the records.

10. The Clinic should store paper records securely in locking cabinets or behind locked doors and lock cabinets and doors when access to records is not necessary.

11. The Clinic should develop formal procedures and conduct regular audits of access to and use of personal information within the Clinic.

12. The Clinic should immediately ensure that a confidentiality agreement is in place with its EMR software support company with respect to the protection of employee and patient personal information

7.0 CONCLUSION

The key findings detailed in this report included:

1. The Clinic is not authorized to collect any personal information via video and audio surveillance cameras and should immediately cease further collection or use of such personal information.

2. The Clinic is not in compliance with s. 6 of PIPA as it has not met its obligation to ensure it has consent for the collection, use, or disclosure of personal information.

3. The Clinic currently is not protecting personal information as required by s. 34 of PIPA, as there are significant gaps in the Clinic's administrative, physical and technological security controls.

4. The Clinic does not have an effective Privacy Management Program in place.

The owner of the Clinic and the office manager acknowledged during the interview that the Clinic policy needed to be updated, the purposes for collection of personal information need to be reviewed and listed, and that annual training of staff related to privacy policies and issues should take place.

Since reviewing this report, the owner of the Clinic has updated the privacy policy. The new policy meets most of the criteria included in Recommendation 1. The Clinic still needs to amend the new policy to include a description of the personal information the Clinic collects from patients and employees. As well, the Clinic should update the new policy after it implements the report recommendations to reflect the changes with regard to removing video and audio surveillance.

The recommendations in this report point to:

- updating and putting into practice Clinic policy and procedures,
- ensuring appropriate collection of personal information and conducting privacy risk assessments,
- providing regular training to staff and having them sign confidentiality agreements, and
- protecting personal information in the Clinic's custody or under its control through improved storage, disposal and security safeguards.

In order for the Clinic to be in compliance with its legal duties under PIPA, it is essential that the owner of the Clinic implement the recommendations of this report and work to better understand his legal obligations and cultivate a privacy-respectful culture within the Clinic.

The Commissioner has requested that, within three months, the Clinic provide a written status update related to its implementation of the recommendations contained in this report.

8.0 ACKNOWLEDGEMENTS

I would like to thank Tanya Allen, Senior Investigator, and Justin Hodkinson, Investigator, who conducted the audit and drafted this report.

December 8, 2016

ORIGINAL SIGNED BY

Drew McArthur
A/Information and Privacy Commissioner
for British Columbia

Endnotes

[1] OIPC. 2009. *Order P09-02: Shoal Point Strata Council*. pp.18-19, par 72. https://www.oipc.bc.ca/orders/1417.
OIPC. 2012. *Order P12-01: Schindler Elevator Corporation*. https://www.oipc.bc.ca/orders/1491.
OIPC. 2013. *Order P13-02: ThyssenKrupp Elevator (Canada) Limited*. https://www.oipc.bc.ca/orders/1565.
and BC OIPC, Alberta OIPC and Privacy Commissioner of Canada. 2008. *Guidelines for Overt Video Surveillance in the Private Sector*. https://www.oipc.bc.ca/guidance-documents/1453.
[2] During the interview, the physician stated that the policy had been in place before the audit. However, the auditors did not find evidence to suggest that this statement was accurate. The physician had initially reported that there was no policy, and many of the documents and procedures referred to in the subsequently submitted policy were not found to be in place at the Clinic. As well, the policy referred to Ontario Medical Association and legislation.
[3] BC OIPC, Alberta OIPC and Privacy Commissioner of Canada. 2012. *Getting Accountability Right with a Privacy Management Program*. https://www.oipc.bc.ca/guidance-documents/1435. p.10.
[4] OIPC. 2009. *BC physician privacy toolkit*. https://www.oipc.bc.ca/guidance-documents/1470 or https://www.doctorsofbc.ca/resource-centre/physicians/managing-practice/privacy-toolkit.
[5] OIPC. 2015. *Order P15-01: Park Royal Medical Clinic.* https://www.oipc.bc.ca/orders/1783.
[6] OIPC. 2004. *Tips for Organizations Responding to a Privacy Complaint under the* Personal Information Protection Act*.* https://www.oipc.bc.ca/guidance-documents/1443.
[7] OIPC. 2015. *A Guide to B.C.'s Personal Information Protection Act for Businesses and* Organizations. p.9. https://www.oipc.bc.ca/guidance-documents/1438.
[8] OIPC. 2012. *Order P12-01: Schindler Elevator Corporation*. https://www.oipc.bc.ca/orders/1491.
And OIPC. 2013. *Order P13-02: ThyssenKrupp Elevator (Canada) Limited*. https://www.oipc.bc.ca/orders/1565.
[9] *Eastmond v. Canadian Pacific Railway,* [2004] F.C.J. 1043.
[10] Alberta Order P2006-008, [2007] A.I.P.C.D. No. 16.
[11] As noted by the Google Maps Street View image of the Clinic collected in July 2015.
[12] OIPC. 2009. *Order P09-02: Shoal Point Strata Council*. pp.18-19, par 72. https://www.oipc.bc.ca/orders/1417.
[13] OIPC. 20016. *Investigation Report F06-01: Sale of Provincial Government Computer Tapes Containing Personal Information*. https://www.oipc.bc.ca/investigation-reports/1232. p.14, par.49.
[14] BC OIPC, Alberta OIPC and Privacy Commissioner of Canada. 2012. *Getting Accountability Right with a Privacy Management Program*. https://www.oipc.bc.ca/guidance-documents/1435. pp. 9-10.
[15] BC OIPC, Alberta OIPC and Privacy Commissioner of Canada. 2012. *Getting Accountability Right with a Privacy Management Program*. https://www.oipc.bc.ca/guidance-documents/1435.