OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

AUDIT & COMPLIANCE REPORT P19-01

Compliance Review of Medical Clinics

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

September 25, 2019
CanLII Cite: 2019 BCIPC 38
Quicklaw Cite: [2019] B.C.I.P.C.D. No. 38

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

People share some of their most sensitive personal information with physicians and staff at medical clinics. The bond of trust between doctor and patient is critical to the relationship. Key to that trust is ensuring a patient's personal information is properly protected.

The troubling reality, however, is that privacy issues occur regularly within the medical field. My office has received numerous complaints and reported privacy breaches relating to medical clinics in the past few years. Accidental disclosures by email, sensitive information kept in and stolen from doctors' vehicles, and compromised computer systems are a few of the more common manifestations of privacy violations experienced at medical clinics throughout this province. The harms caused by these breaches can be very serious, leaving victims vulnerable to everything from damaged relationships to humiliation, financial loss and more. Increased effort and attention to privacy practices within clinics is needed to establish and maintain trust in physicians, medical clinic staff, and the medical system in general.

I deeply appreciate the strain medical professionals in BC operate under. Amid rising demands and sometimes limited resources, protecting privacy may become a priority only in the wake of a breach. In the meantime, other concerns dominate: the allure of technological convenience may, for example, override a thorough consideration of potential privacy pitfalls.

Where does that leave patients? Finding another family doctor if you are dissatisfied with a clinic's privacy management practices is not a realistic alternative when it is difficult to find a doctor taking on new patients or where there are waiting lists for specialists.

The story revealed in this report discloses that some clinics practice good privacy hygiene while others do not. Clinics have to do better – to devote the necessary resources and take the initiative in building sound privacy programs – both for ethical and business reasons and because it's the law. As private organizations that collect, use and disclose personal information, medical clinics are obligated to abide by the Personal Information Protection Act.

Our aim is to draw attention to both the good and the bad when it comes privacy compliance by organizations. This review builds on the body of resources available for physicians and clinics offered by my office. It is aimed at helping them understand what the obligations are, encourage a look inward, and make the transition to better privacy practices as seamless as possible. Again, my office stands ready to assist in that effort.

It is my hope that this report generates awareness and action for the benefit of all patients in BC and the medical professionals who treat them.

Michael McEvoy
Information and Privacy Commissioner for BC
September 25, 2019

EXECUTIVE SUMMARY

This compliance review, conducted under s. 36 of the *Personal Information Protection* (PIPA), focused on 22 BC medical clinics with five or more licensed physicians. The review assessed the clinics' privacy management programs, privacy policies, and the collection and safeguarding of personal information.

The OIPC selected medical clinics because they handle a significant amount of sensitive personal information, and this group comprises a large number of OIPC complaint and breach files each year.

Methodology for this review included:

1. Examination of clinic websites;
2. Interviews with medical directors, privacy officers, or other such persons; and
3. Review of written policies, staff training and other documents.

While not intended to be representative of all medical clinics in BC, findings do raise issues related to patient privacy that are relevant to all medical clinics across the province. Key findings show that there are gaps in some clinics' privacy management programs and that clinics need to ensure their privacy management programs have:

- adequate funding and resources;
- someone designated as responsible for compliance with PIPA;
- clear internal reporting structures;
- up-to-date personal information inventories;
- documented privacy policies that detail how the clinic will meet its legislated obligations;
- mandatory training as well as signed confidentiality agreements by all individuals who access personal information collected by the clinic;
- established breach reporting and response processes;
- contracts that detail expectations for privacy protection;
- processes to identify and mitigate privacy and security risks;
- regular review of administrative, physical, and technological safeguards;
- regular risk assessment, audit and compliance monitoring activities; and
- annual reviews of the overall privacy management program.

In addition, the OIPC reviewers found that some clinics are collecting sensitive personal information online and recommend that clinics provide patients with unique and secure login information for booking appointments online, ensure adequate notification regarding the purposes for the collection of personal information online, and post privacy policies that detail the collection, use, and disclosure of personal information through the website (including device identifiers).

Overall, this report includes 16 recommendations that will, if fully implemented, aid clinics in ensuring they meet their legal duties under PIPA. Each of the 22 clinics involved in this review will receive a summary of findings and recommendations pertinent to their own clinic.

1 BACKGROUND & METHODOLOGY

The Office of the Information and Privacy Commissioner for BC (OIPC) conducts audits and compliance reviews to assess how effectively public bodies and private sector organizations protect personal information and comply with access provisions under the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act* (PIPA).

This compliance review, conducted under s. 36 of PIPA, focuses on medical clinics with five or more licensed physicians. The review assessed the clinics' privacy management programs, privacy policies, and the collection and safeguarding of personal information.

The OIPC selected BC medical clinics because they handle a significant amount of sensitive personal information. In addition, compared to other groups of private sector organizations in OIPC files, health care services provided by physicians, medical clinics and labs account for the largest number of complaint and breach files received by the OIPC over the past five years.

1.1.1 Objectives

The objectives of this compliance review were to:

1. examine privacy management practices within the clinics;
2. review clinic compliance with PIPA and OIPC guidance; and
3. identify gaps in clinic programs or procedures and make recommendations to address those gaps.

1.1.2 Scope

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

1. Examination of clinic websites for:
    a. the types of personal information collected online;
    b. notification about the purposes for collecting personal information online; and
    c. online privacy policies;
2. Interviews with medical directors, privacy officers, or other such persons; and
3. Review of written policies, staff training and other documents.

The scope of this investigation did <u>not</u> include:

1. an audit or physical inspection of electronic information management systems, storage and retention practices, disclosures, or security safeguards; or
2. an examination of individual client medical files.

1.1.3 Methodology

The College of Physicians and Surgeons (College) provided a list of multi-physician (five or more) medical clinics within select mid-to-large cities in BC.[1] From this list, the OIPC review team selected a random sample of 30 clinics for inclusion in this review. The sample matched the list provided by the College in terms of geographic representation from each city. After making direct contact with the clinics, the OIPC review team determined that eight of the selected clinics employed fewer than five doctors and removed them from the sample, thus leaving the final sample at 22 clinics. While sample size and geographical distribution are insufficient to state that the findings contained in this report represent all clinics across BC, it is fair to conclude these results should be cause for all BC clinics to reflect upon the state of their privacy management programs.

After selecting the sample of clinics, the review team inspected related websites, if they existed, to determine whether the clinic's privacy policies were available online, and conducted interviews via telephone with a key liaison[2] from each clinic. During interviews, the review team requested a description of the personal information collected, used, or disclosed by the clinic; information about each clinic's privacy management program; and copies of privacy and security policies and training materials. The review team reviewed the available policies and training.

The review team used information from interviews, policies, and training materials to assess the extent of compliance with PIPA and the OIPC's guidance on privacy management programs.[3] The review focussed on three specific lines of inquiry; specifically, whether the clinics have:

- a fulsome privacy management program;
- policies and practices, as required by s. 5 of PIPA; and
- reasonable security arrangements to protect personal information as per s. 34 of PIPA.

2 LEGISLATION & GUIDELINES

2.1 *Personal Information Protection Act* (PIPA)

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

[1] The cities included Burnaby, Kelowna, Richmond, Vancouver, and Victoria.
[2] Typically the medical director or a designated privacy officer.
[3] Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada and Office of the Information & Privacy Commissioner for British Columbia. 2012. *Getting Accountability Right with a Privacy Management Program*. https://www.oipc.bc.ca/guidance-documents/1435.

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, use, and disclose and 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 or where PIPA permits collection without consent;
- 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 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. 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 must destroy the personal information after it is no longer needed for legal or business purposes.

2.2 OIPC Guidance

2.2.1 Privacy Management Programs

The Commissioners' joint guidance on privacy management programs[4] and the OIPC's PrivacyRight webinar[5] on the same subject point to at least 10 steps for implementing an organization's privacy management program. These include:

1. **Buy-in from the top**: senior management commitment to supporting privacy, including the provision of staff and resources.
2. **Privacy officer**: having someone specifically responsible for privacy-related duties such as drafting policies, providing training, and advocating privacy across the organizations.
3. **Reporting structures**: appropriate internal reporting structures so the privacy officer and senior management know how the privacy management program is functioning.
4. **Personal information inventory**: an inventory of the types and sensitivity of personal information the organization collects, who it is collected from, how it is collected, why or how it is used and disclosed, and where the personal information is stored.
5. **Policies**: an explanation of an organization's responsibilities for handling the personal information, how the information is protected, and how individuals can request access or make a complaint about the handling of their personal information.
6. **Risk Assessment**: is an internal evaluation of whether an organization has sufficient safeguards in place to protect personal information.
7. **Training**: whether all staff and volunteers who handle personal information are trained on the organization's responsibilities and expectations for privacy management.
8. **Breach response**: protocols for reporting suspected breaches and steps for responding to a breach (containment, evaluation, notification, prevention).
9. **Service provider management**: ensuring service providers or contractors are aware of the organization's expectations for handling personal information.
10. **Review and revise**: regular review of the privacy management program, and making updates or revisions as necessary.

2.2.2 Policies & Practices

Section 5 of PIPA states that an organization must develop and follow policies and practices necessary for the organization to meet its obligations under the Act. A privacy policy should reflect the requirements of PIPA, including:

1. **Accountability**: provide a statement that your organization is accountable for compliance under PIPA, define PIPA, provide the definition of "personal information" and express your commitment to privacy.

---

[4] Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada and Office of the Information & Privacy Commissioner for British Columbia. 2012. *Getting Accountability Right with a Privacy Management Program*. https://www.oipc.bc.ca/guidance-documents/1435.

[5] OIPC. 2019. Webinar 1 – 10 basic obligations under PIPA. https://www.oipc.bc.ca/privacyright/webinars/.

2. **Identifying Purposes & Limiting Collection**: explain when you will collect, use, or disclose personal information, the types of personal information you collect, and the purposes for collection.
3. **Consent:** explain when and how you will obtain consent, the type of consent (implied or express, depending on the sensitivity of the personal information), and the right to withdraw consent.
4. **Limiting use and disclosure**: identify purposes and limitations on collection, use and disclosure of personal information, and any other circumstance for which your organizations discloses personal information.
5. **Retention**: commit to retaining personal information used to make a decision that directly affects individuals for at least one year after you make that decision.
6. **Accuracy**: identify measures to ensure personal information is accurate, and how individuals can correct errors or omissions in their personal information.
7. **Safeguards**: set out administrative, physical, and technological safeguards and the process for responding to suspected privacy breaches.
8. **Individual Access**: identify how individuals can access their information.
9. **Challenging Compliance**: identify how an individual can make a complaint and to whom.
10. **Openness**: identify where to find the privacy policy and that individuals can contact the OIPC.

Please see the OIPC guidance document: Developing a Privacy Policy under PIPA.

2.2.3 Security Safeguards

Under s. 34 of PIPA, organizations must use reasonable physical, administrative, and technological safeguards to protect personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks.

Organizations should employ administrative, physical, and technological safeguards to protect personal information in their custody.

Administrative safeguards are organizational policies, procedures, and maintenance of security measures. Administrative safeguards include employee training, confidentiality agreements, access on a-need-to-know basis, role-based access, and audits.

Physical safeguards are physical measures to protect personal information (including electronic information systems, buildings, and equipment) from natural and environmental vulnerabilities and unauthorized intrusion. Physical safeguards include locking files up, restricting access to areas where files are stored, a clean desk policy, positioning screens away from public view, and adequate disposal processes for paper files and electronic equipment containing personal information.

Technological safeguards are the technological policies and procedures that protect personal information and access to it. Technological safeguards include using strong and secure

passwords, auto log out, firewalls, intrusion detection and antivirus software, and adequate encryption.

Please see OIPC guidance document A Guide to B.C.'s Personal Information Protection Act, pages 36-37.

3 FINDINGS

While the findings in this report reflect the state of privacy management programs within 22 BC medical clinics with five or more physicians, the results do raise issues related to patient privacy that will be of relevance and interest to all medical clinics across the province.

3.1 Privacy Management Programs

Privacy management programs help to foster respect for privacy and to ensure that clinics are meeting their legislative obligations under PIPA (and the *Freedom of Information and Protection of Privacy Act*, where applicable). In assessing the state of privacy management programs in the clinics the OIPC review team relied on interviews with the clinics' medical directors, managers, and privacy officers and a review of the clinics' privacy policies. With the exception of privacy policies, the review team did not independently verify the information provided by the clinics.

Respondents who provided information on behalf of the clinics were often the clinics' medical directors, privacy officers, or others with some responsibility for the privacy function within the clinic. These representatives were generally knowledgeable within their field, as they maintained an average of 10 years of experience within their specific clinics and 16 of the 22 clinic respondents also had previous experience in other clinics or hospitals.

Sampled clinics reported employing or contracting with an average of 13 physicians, nine medical office assistants, nine nurses, and medical students other staff. In total, considering all staff and contractors who may access personal information collected by the clinic, the average was 31 staff and contractors, with a range of anywhere from 12 to 93 staff and contractors. Several clinics also mentioned bookkeepers, information technology contractors, shredding companies, and other contractors who may have access to the personal information clinics collect about their patients and staff and are not included in these numbers. This means that privacy management programs should be robust enough to account for the various individuals and transactions inherent to clinic processing of personal information.

3.1.1 Buy-in from the top

Support from the senior management team of a clinic, including its medical director, is essential for a clinic's privacy management program to be adequate and effective. Medical directors and senior management are accountable for ensuring the privacy function is adequately resourced and that appropriate training and education are provided to all staff and physicians so they

understand their own responsibilities, personal information handling processes are appropriately monitored and audited, and reasonable safeguards are in place to protect personal information the clinic collects. Staff and contractors are far more likely to aid in safeguarding patient information when they know clinic leaders take the issue seriously.

We asked representatives from the 22 clinics to self-rate their clinic's privacy management program on a 10-point scale. On average, clinic representatives self-rated as seven out of 10, ranging from a low of two to a high of nine. Findings throughout the rest of this report support those self-ratings and show that many clinics (in particular, their medical directors and senior management) have work to do in order to meet their legal duties for protecting personal information.

Medical directors, privacy officers, and others who participated in the interviews noted that the biggest challenges they face in performing their duties with respect to privacy management included:

- adequate financial and other resources;
- having the time to do the necessary work;
- a lack of awareness of what their duties are; and
- working with technology and keeping up with technological changes.

Clinics need to dedicate the necessary financial support, resourcing, and time to develop and maintain privacy management programs and ensure that staff, contractors, and others understand and respect privacy obligations.

RECOMMENDATION 1
Clinics should ensure adequate funding and resources for effective privacy management programs.

3.1.2 Privacy officer

PIPA s. 4(3) mandates that all organizations designate one or more individuals to be responsible for ensuring that the organization complies with the Act. Most clinics (18 of 22) reported that someone within the clinic had been designated the role of privacy officer. The remaining four clinics did not have a designated privacy officer, which means there is no one at the clinic responsible for ensuring the protection of personal information. These clinics are failing to comply with PIPA.

The OIPC recommends that every clinic that has not already done so to immediately designate someone responsible for ensuring compliance with PIPA, and that staff are aware of who to contact for any privacy-related matters.

RECOMMENDATION 2

Clinics without privacy officers must immediately designate one or more individuals to be responsible for ensuring the clinic complies with PIPA.

Interviewees from clinics with privacy officers noted that basic job duties for the privacy officer include:

- drafting and maintaining privacy policies and related materials such as privacy agreements;
- ensuring privacy and confidentiality are maintained throughout the clinic;
- providing training and refresher training for staff, along with training manuals;
- learning about PIPA, following College guidelines and the BC Physician Privacy Toolkit;[6]
- reviewing clinic privacy policies, training and processes;
- overseeing technological functions such as access to Care Connect, network, electronic medical records (EMR), levels of access, password usage (often in conjunction with contractors);
- physical security of the clinic premises;
- audits of access to patient records; and
- responding to requests for access to patient records (i.e., by insurance companies and lawyers).

The OIPC agrees these are all important matters for privacy officers. Additional duties that privacy officers are often accountable for that none of the clinic respondents mentioned include:

- investigating and responding to complaints;
- providing information or answering questions about the clinic's privacy practices;
- responsibility for ongoing assessment and revision of policies, training and security safeguards;
- representing the clinic in the event of an investigation by the OIPC; and
- advocating for privacy throughout the clinic itself.

[6] College of Physicians and Surgeons, Doctors of BC, and the Office of the Information and Privacy Commissioner. 2017. BC Physician Privacy Toolkit: A guide for physicians in private practice, 3rd ed. https://www.oipc.bc.ca/guidance-documents/1470.

When asked if the clinics' privacy offices have the necessary resources (such as staff and equipment) to fulfil their job duties, 16 respondents agreed, while the remaining six reported lacking knowledge and time to commit to privacy functions and insufficient resource support.

Clinic staff and physicians may access resources on the College of Physicians and Surgeons of BC, Doctors of BC, and OIPC websites. For example:

- www.cpsbc.ca develops practice standards, professional guidelines, legislative guidance, and other materials for physicians and surgeons to review.
- www.doctorsofbc.ca has a resource centre with tips, educational material, checklists, videos, FAQ, and myriad templates for use, including privacy policy templates, confidentiality agreements, and more.
- www.oipc.bc.ca publishes copies of guidance documents, orders and decisions, educational videos, and webinars.

3.1.3 Reporting structures

Reporting structures are processes that "ensure that the right people know how the privacy management program is structured and whether it is functioning as expected."[7] This includes conducting audits and other activities to monitor compliance, implementing escalation procedures for raising privacy issues, and ensuring that the medical director, privacy officer, senior management, board of directors (if applicable), or others are aware of how the privacy management program is functioning within the clinic. Reporting structures should be documented and clearly communicated throughout the clinic.

The majority of clinics in the review (20 of 22) noted that they have clear and effective reporting mechanisms in place. Of the remaining two clinics that reported they did not have clear and effective reporting mechanisms, one noted that issues with privacy have not occurred (yet) and the other reported that staff would come to her with such concerns or issues.

RECOMMENDATION 3

Clinics should establish, document, and communicate clear internal reporting structures for issues related to privacy management.

[7] Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada & Office of the Information & Privacy Commissioner for British Columbia. 2012. Getting accountability right with a privacy management program. P.8. https://www.oipc.bc.ca/guidance-documents/1435.

3.1.4 Personal information inventory

Clinics collect a vast array of personal information. For example, clinic representatives reported collecting:

- patient and staff identification and contact information;
- patient physical information (such as height and weight);
- patient financial and billing information;
- current and historical patient medical information, including medications;
- current and historical patient and staff occupational or educational information;
- patient family medical history;
- staff financial and tax information;
- device identifiers for those who access clinic websites; and
- images of individuals captured by video surveillance.[8]

The majority of clinics (18 of 22) reported that they did not maintain a personal information inventory that identifies the types and sensitivity of personal information collected, the purposes for collection, or the location where the clinic holds personal information. Two clinics reported relying on the EMR dictionary (which only represents patients' personal information and not staff, physicians, or others who the clinic may employ). The final two clinics reported having a fulsome personal information inventory that reflected the types and sensitivity of personal information the clinics collect, the purposes for collection, and where they store the personal information.

Many of those interviewed were not aware of how or where the personal information of staff, physicians, or others employed by the clinic was stored. In some cases, the clinics share this information with service providers (such as bookkeepers) and the clinic may lack appropriate controls in the form of contracts, training, privacy policies, or other documents to detail the clinic's expectations for how the information is to be handled. Along with staff financial or banking information, other recorded personal information may include documented human resources issues, requests for leave, applications and resumes from potential employment prospects, and other personal information which need to be considered within the clinic's personal information holdings and adequately safeguarded.

[8] Use of video surveillance must be what a reasonable person would consider appropriate in the circumstances (i.e., actual thefts or other incidents) and should only be used as a last resort after exploring other less privacy-invasive alternatives. For information, see OIPC Audit & Compliance report *Over-collected and Overexposed: Surveillance and Privacy Compliance in a Medical Clinic*. https://www.oipc.bc.ca/audit-and-compliance-reports/2111.

RECOMMENDATION 4

Clinics should develop and maintain an inventory of all types of personal information the clinic collects, the purposes for collection, where the information is stored, and its sensitivity.

3.1.5 Policies

Private medical clinics, as organizations under PIPA, are required to have policies and practices necessary to meet their legal obligations. PIPA s. 5 states:

> 5 An organization must
> (a) develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act,
> (b) develop a process to respond to complaints that may arise respecting the application of this Act, and
> (c) make information available on request about
> (i) the policies and practices referred to in paragraph (a), and
> (ii) the complaint process referred to in paragraph (b).

Of the 22 clinics, 16 had privacy policies (and made them available for review), while six clinics failed to meet their obligations under s. 5 of PIPA. Half of the 16 clinics reported making their policies available upon request to patients, three clinics have their full privacy policy posted online, and two noted that they provide a copy of the policy to patients when going through intake processes to become a client of the clinic. Several of the clinics also reported using their privacy policies in their training of new staff and requesting new staff to sign an acknowledgement that they have reviewed and understood the policies.

Clinics need to review policies, as part of the overall privacy management program, on a regular basis (for example, annually) and revise them as necessary. Of the 16 clinics with privacy policies, 11 clinics reported that they have reviewed their policies, three noted that the policies are newly drafted so have not come up for review yet, and two had not contemplated policy review.

When asked how they communicate expectations related to privacy and security of personal information to staff and physicians in clinics that do not have privacy policies, interviewees reported relying on training that medical office assistants and physicians may receive during their schooling and the Physician's Toolkit. While post-secondary training and guidance documents are useful, these do not include personal information handling practices specific to the clinic so, on their own, do not meet the clinic's obligations under PIPA. A fuller review of the content of privacy policies is covered in the next chapter 3.2.

RECOMMENDATION 5

Clinics should develop and maintain policies and practices necessary to meet the obligations under PIPA, including developing a process to respond to privacy complaints.

3.1.6 Training

Most clinics (20 of 22) reported offering at least some training to staff and physicians, while two noted that they do not offer any training. Clinics that do not offer training are failing to meet their obligations to provide reasonable security arrangements under s. 34 of PIPA.

Many of the clinics in this review reported using a variety of training methods, including:

- onboarding training to review clinic policies and procedures;
- review and acknowledgement of the clinic's privacy policies;
- having staff, physicians and contractors sign confidentiality agreements;
- discussions on privacy and security during staff and physician meetings, and one-on-one meetings with staff as part of annual review;
- online training offered by the local health authority;
- review of the Physician's Toolkit; and
- preparation and review of a staffing manual.

When the OIPC review team asked if training is mandatory, 16 clinics reported that the initial training is mandatory for staff and seven clinics reported providing regular refresher training to staff as well. Fewer required physicians to participate in regular training or discussions related to privacy management and the handling of personal information.

RECOMMENDATION 6

Clinics should provide mandatory training and education for all staff, physicians, contractors and others who may access personal information the clinic collects.

In addition to mandatory training, the OIPC recommends all medical clinics implement practices such as having all staff, physicians and others sign a confidentiality agreement and/or sign an acknowledgement that they have reviewed and understood the clinic's privacy policies.

RECOMMENDATION 7

Clinics should ensure that all staff, physicians, contractors, and others who access personal information review the clinic's privacy policies and sign a confidentiality agreement.

Privacy training needs to be ongoing for clinics, as with other organizations, especially considering the changes in technology and systems over time. As noted above, Doctors of BC (www.doctorsofbc.ca) and the OIPC (www.oipc.bc.ca) provide educational materials for use by physicians, staff, volunteers, or others working in a medical clinic.

3.1.7 Breach response

All 22 clinics reported that their staff know how to respond if they suspect there has been a privacy breach, and that this information would be reported to their supervisors and the clinic's privacy officer and/or medical director.

Ten of the 22 clinics had written policies on what staff, physicians, contractors, patients or others should do in the event of a suspected breach and to whom to report the suspected breach. Contemplation and documentation of breach response, including containment, evaluation of risk, notification, and prevention is essential for protecting personal information under s.34 of PIPA.

RECOMMENDATION 8

Clinics should establish, document, and communicate clear breach reporting and response processes.

3.1.8 Service provider management

Sections 17 through 19 of PIPA cover the circumstances for which organizations may disclose the personal information they collect from staff, patients, or others. Generally, clinics may disclose personal information to service providers or contractors for the purposes for which the clinic collected the information and to assist the contracted organization to carry out work on the clinic's behalf. Typical examples from interviews included contracts with physicians, sharing employee information with a bookkeeper for payroll and accounting purposes, and hiring a shredding company for secure destruction of paper records. Clinics may also contract with

others for cleaning services, physical security, and information technology support where they likely will not handle personal information as part of their duties but may inadvertently overhear or view personal information.

During interviews, nine of the 22 clinics reported that they have nothing in place or are unaware of any provisions in contracts or otherwise that detail the clinic's expectations for service providers or contractors to securely handle personal information. Best practice dictates contracts or agreements to be in place that detail clinics' expectations for secure handling of personal information in all cases where clinics disclose personal information directly to, or where personal information is otherwise accessed by, service providers. The OIPC's guidance on *Information Sharing Agreements*[9] may be of assistance.

Clinics, like other organizations, cannot contract out their obligations under PIPA. The clinic is ultimately responsible, should any of their service providers or contractors breach any aspect of the legislation.

RECOMMENDATION 9

Clinics should ensure written contracts and information sharing agreements express expectations for privacy protection.

3.1.9 Risk Assessment

Just over half (12 of 22) of clinic respondents reported that they do not conduct any type of privacy risk assessment, internal audit, or other privacy compliance monitoring activities. When asked how they know whether the clinic keeps personal information secure, some admitted that they rely on assumption, that it is difficult to know, and that they cannot guarantee personal information is kept securely. Others noted that they anticipate the staff or contractors would advise if there are issues, that privacy issues are raised verbally as needed, that individuals are responsible for following policies set out by the College of Physicians and Surgeons, that there are plans in place for future audits.

The 10 clinic respondents who reported engaging in privacy and security risk assessments and the like pointed to daily checklists and walk-arounds, monthly reviews, quarterly environmental

[9] OIPC. 2017. Guidance Document: Information Sharing Agreements. https://www.oipc.bc.ca/guidance-documents/2066.

scans, security threat risk assessments conducted by the IT contractor, formal or informal audits of access to personal information, and yearly overall reviews.

Fewer than half of the clinics (9 of 22) reported conducting privacy impact assessments when they consider implementing new technology or make changes to the systems they use to store the personal information they collect from patients, employees, or others. Ten clinics reported that they have not completed a privacy impact assessment prior to such implementation, and three noted that they have not made any such changes so have not had need to assess impact.

RECOMMENDATION 10

Clinics should develop processes to identify and mitigate privacy and security risks for all clinic processes that involve personal information, including risk assessment prior to any new collection, use or disclosure of personal information.

The OIPC website has useful resources (https://www.oipc.bc.ca/resources/guidance-documents/) to aid in understanding, identifying, and mitigating privacy and security risks.

3.1.10 Review and revise

Regular review of a Privacy Management Program is necessary to ensure that policies and practices for handling and securing personal information are effective. Organizations should reflect on their overall program to determine if they need to make any changes. For example, technology is always changing, are the clinic's policies and practices keeping pace with newer industry standards for information security? If the clinic is implementing a new process or program, have they prepared a Privacy Impact Assessment?

Clinics may also need to amend staff training to incorporate any new privacy implications, and to expand the personal information inventory to incorporate any new types of personal information the clinic will collect. If there has been a restructuring or new staff or physicians hired, will senior management need to communicate new reporting structures?

Just under half (10 of 22) of the clinics reported having reviewed their overall privacy management program within the previous two years. Another nine clinics reported currently undergoing that process, some in response to this review. An additional three noted that they have never reviewed their privacy management program.

RECOMMENDATION 11

Clinics should develop an annual review plan that details how the clinic will monitor and assess the effectiveness of the clinic's privacy management program.

3.2 Privacy Policies

As noted, 16 of the 22 clinics provided the OIPC with copies of privacy policies and related documents for this review. The remaining six clinics reported that they do not have privacy policies and, as such, they have failed to meet the requirements of s. 5 of PIPA.

Policies are essential for any organization to fulfill the basic duties and requirements under privacy legislation. Policies should be in writing and provided to all staff, physicians, contractors or others who may access personal information that the clinic collects about patients, employees or others. In addition, if requested, clinics must make information available about their privacy policies and practices and their processes for responding to complaints about the clinic's handling of personal information. Best practice is to post privacy policies online and to make a copy available at the clinic.

For this review, clinics provided policies relating to the privacy and security of personal information and individual access to their own personal information, staff hiring and training materials relating to privacy, security, and access to personal information, copies of confidentiality agreements, informed consent forms, and personal information release/disclosure authorizations.

Table 1 describes the necessary components of a privacy policy, based on PIPA and OIPC guidance, along with findings on how the clinics incorporated these elements.

The findings in Table 1 suggest that clinic privacy policies frequently failed to address the following important matters:

- A description of PIPA;
- The definition of personal information;
- The right for individuals to withdraw consent;
- Commitment to retain personal information and retention periods;
- Breach reporting response protocols; and
- Contact information for the privacy officer and the OIPC.

In addition, the OIPC review team found that some clinics summarize the privacy policies in one or two documents (i.e., general privacy policy and electronic information policy) and a separate

privacy policy for websites. Other clinics separated privacy-related items across six or more policies. This poses a variety of challenges for staff review and comprehension; the privacy officer in maintaining up-to-date privacy policies; the internal review team to assess compliance with privacy policies, for any external review or audit; and for meeting the s. 5 of PIPA obligation to make information about the policies and practices available upon request (by anyone). Best practice dictates summarizing key aspects of privacy policies into one main document.

TABLE 1: COMPONENTS OF A PRIVACY POLICY

Policy	# Clinics with Component in Policy	Comment
Accountability		
• Compliance with PIPA	13	Two incorrectly pointed to the federal legislation, PIPEDA, as the applicable law
• Brief description of PIPA	5	Four incorrectly referred to other legislation, three note PIPA in other documents but not in clinic privacy policies
• Definition of personal information	7	
• Commitment to privacy	15	
Identifying Purposes & Limiting Collection of Personal Information		
• Stated limits to collection, use or disclosure	15	
• Description of the personal information collected	14	Five clinics reported using video surveillance cameras. One did not have a written policy at all, and four did not include images collected by video surveillance in the description of personal information collected.[10]
• Detail purposes for collection, use, or disclosure	15	As above, five clinics who reported using video surveillance do not have a policy detailing the purposes for collection, use, or disclosure of this personal information.
Consent & Notification		
• Consent is required	15	
• Process for notification about the purposes of collection	13	
• How consent is obtained	16	
• Right to withdraw consent	12	
Limiting use and disclosure of Personal Information		
• Detail how, when, and to whom personal information will be disclosed	14	One additional policy cites disclosure but does not detail to whom they will disclose employee personal information

[10] Consent, or authority to collect personal information without consent, is a key principle of PIPA. Notification about the collecting of personal information, including the purposes for that collection, is a required component for consent. Relying on implicit consent is likely not applicable in this context, as all of the purposes for collecting an individual's image via video surveillance may not be obvious. As well, clinics would likely not have any authority under PIPA to collect such personal information without consent. Considering the sensitivity, amount, use of personal information, the manner of collection, and the likelihood of collection via video surveillance being effective in achieving the purposes, it is unlikely that a reasonable person would consider this collection of personal information appropriate in the context. As such, clinics who use video surveillance may be in violation of ss. 11 and 14 of PIPA. For more information on this topic, see OIPC Audit & Compliance report *Over-collected and Overexposed: Surveillance and Privacy Compliance in a Medical Clinic*. https://www.oipc.bc.ca/audit-and-compliance-reports/2111.

TABLE 1: CONTINUED

Policy	# Clinics with Component in Policy	Comment
Retention of Personal Information		
• Commitment to retain	11	Four cite 16 yrs. past last visit or age of majority. Five cite 10 yrs. past. One cites one year past collection. Additional six note retention but do not include specific timeframe[11]
• Methods for disposal	15	Best practice: list electronic records, date of destruction, sign witness to destruction/ deletion. Cross-shred paper records.
Accuracy		
• How request correction of personal information	15	
Safeguards		
• Administrative	16	Best practice: note the clinic's key administrative safeguards in the privacy policy
• Physical	16	Best practice: note the clinic's key physical safeguards in the privacy policy
• Technological	16	Best practice: note the clinic's key technological safeguards in the privacy policy
• Breach response	10	Best practice: eight policies also contained provisions for responding to breaches: contain, evaluate risk, notify and prevent
Individual Access		
• Right to access one's own personal information	15	
• How to request access	15	
Challenging Compliance		
• How to make complaint	14	
Openness		
• Privacy Officer contact information	9	
• Note that one can contact OIPC	11	An additional three reference the federal or Alberta privacy commissioners. Also, seven of the counted policies mention a privacy commissioner but do not point to the OIPC specifically or provide contact information for the OIPC.

As noted above, recommendation 5 states that all medical clinics should develop and maintain policies and practices necessary to meet their obligations under PIPA, including developing a process to respond to privacy complaints. Best practice is for each clinic their privacy policies

[11] As per BC's *Limitation Act* and s. 3-6(2) of the bylaws under BC *Health Professions Act*, medical records must be retained for a minimum of sixteen years from the date of last entry or from the age of majority, whichever is later, except as otherwise required by law. See https://www.cpsbc.ca/files/pdf/PSG-Medical-Records-Management.pdf.

include the components and detail listed in Table 1 and in OIPC guidance on developing privacy policies.[12]

3.3 Clinic Websites

3.3.1 Collection of personal information online

Of the 22 clinics included in the sample for review, 18 clinics maintain webpages for their business. Of those, six clinics have online booking, another four have a fillable form for website patrons to contact the clinic, one has both online booking and a contact form, and one has an email sign-up to receive their newsletter. In total, 14 of the 22 clinics collect some form of personal information online. This is in addition to typical website collection of device identifiers such as internet protocol (IP) addresses, browsing history, and location information.

The types of personal information clinics collect online include:

- Contact information (name, email, address, phone number);
- Demographics and other identifiers (personal health number, date of birth, age, gender);
- Medical information (reason for visit, urgency of visit);
- Open fields to provide additional information; and
- Secure login credentials (userID obtained by clinic, password).

Fourteen clinics collect some form of personal information online (again, all 18 clinics with websites likely also collect device identifiers) but only seven had online privacy policies.

Further, five of the 18 clinics with webpages also maintain Facebook pages. It is possible that patients may occasionally send personal information through Facebook messenger to the clinics or requests to book appointments. Clinics with social media pages noted that they do not request or disclose any personal information through this stream and, if an individual were to send it to a clinic via social media, they would promptly re-direct them to proper channels. The OIPC agrees with the clinics that Facebook or other social media are not appropriate forums for collecting or disclosing personal information related to treatment or care, and that clinics with social media accounts should refrain from using them for these purposes.

The OIPC recommends that clinics that utilize online booking or who use online fillable forms (such as on "contact us" pages) limit personal information they collect online and provide appropriate security for that information. Organizations should not collect sensitive personal information such as patient demographics or medical information unless the online forum provides secure transmission. Best practices suggest clinics provide unique userIDs and passwords to patients for any online booking.

[12] OIPC. 2019. *Developing a Privacy Policy under PIPA*. https://www.oipc.bc.ca/guidance-documents/2286.

RECOMMENDATION 12
Clinics should limit their collection of personal information online and provide patients with unique userIDs for online booking.

3.3.2 Notification and consent online

As noted in Table 2 below, only seven of the 18 clinics with websites have online privacy policies. Another two clinics had links to privacy pages but the pages were blank. Seven clinics collect sensitive personal information (such as patient demographics or medical information) online. Of these, only four have posted privacy policies; otherwise, there is no other form of notification relating to the collection of such information.

TABLE 2: ONLINE COLLECTION OF PERSONAL INFORMATION & ONLINE PRIVACY POLICY

Collect PI Online[13]	Collected PI is Sensitive	Online Privacy Policy
Yes – 14	7 – Sensitive	4
	7 – Not Sensitive	3
No – 4	4 – N/A	0
No, No Website – 4	4 – N/A	0

PIPA requires organizations to notify individuals about the purposes for collection on or before collecting personal information unless the purpose is obvious and the individual voluntarily provides their information for that purpose.[14] This means organizations should be notifying individuals prior to collecting any personal information online, such as device identifiers, contact information, or any other personal information. Best practice is to notify patrons on the form page where they would enter their personal information and to have privacy policies available in an easy-to-find location online.

[13] In addition to information that may identify the device one uses to access the clinic's webpage.
[14] For clarification of legislative requirements and further information, see *Guidelines for Online Consent* https://www.oipc.bc.ca/guidance-documents/1638 and Practical Suggestions for your *Organization's Website Privacy Policy* https://www.oipc.bc.ca/guidance-documents/1561.

RECOMMENDATION 13
Clinics must notify individuals in clear terms of the purposes for which they are collecting personal information online.
RECOMMENDATION 14
Clinics should post privacy policies online that detail the collection, use, and disclosure of personal information through the website (including device identifiers).

3.4 Security Safeguards

Organizations must use reasonable safeguards to protect personal information from theft, modification, unauthorized access, collection, use, disclosure, and destruction. Safeguards should be appropriate to the sensitivity of the information. Medical clinics, as with other organizations, should review their safeguards on a regular basis to ensure they continue to be appropriate and effective in achieving their purpose.

Twenty of the 22 clinics reported that they have a security officer or someone in charge of physical or IT security within the clinic. In many cases, the general responsibility fell to the privacy officer or another member of the clinic, and some clinics relied on their IT contractor for maintenance of technological safeguards. Responsibility for administrative safeguards, such as privacy policies, generally fell to the privacy officer.

3.4.1 Administrative safeguards

Common administrative safeguards noted within policies and by clinic respondents included:

- confidentiality agreements;
- privacy policy and acknowledgement;
- training for staff and physicians;
- privacy provisions in contracts;
- restricted access policy;
- clean desk policy and keeping voice low when discussing personal information;
- patient consent forms for disclosure to third parties;
- audits of access and monitoring compliance with privacy policies and practices; and

- email reminders on protecting privacy and topics like how to identify phishing scams.

These are all areas of importance appropriately addressed by clinics. However, in some instances, clinic representatives did not know how or where personnel records (whether electronic or paper) were stored or whether the clinic maintained the security of such records. On other occasions, clinics reported that they provide employee personal information to contracted bookkeepers or one of the physicians for payroll and other HR-related processing with reportedly no provisions in a contract or elsewhere that detail the need for security of employee personal information.

In addition, some of the clinics reported that they do not conduct regular risk assessments, audits, and other compliance monitoring activities. Without these activities, there is no means for a privacy officer or clinic director to tell whether the clinic is keeping personal information secure. In addition, some clinics did not have privacy policies, confidentiality agreements, contract provisions, or training for staff, physicians, volunteers, or others who access personal information.

Clinics not conducting these activities have failed to meet their legal obligations to make reasonable security arrangements to prevent authorized access, collection, use, disclosure, copying, modification or disposal, or similar risks.

3.4.2 Physical safeguards

Common physical safeguards noted in policies and interviews included:

- locked cabinets and rooms with paper records;
- computer screens positioned away from public or privacy screens on monitors;
- alarm systems;
- office layout and soundproofing;
- secure shredding or other destruction of records and equipment;
- access card entry;
- printers and faxes in secure area; and
- sprinklers to prevent records destruction in the event of a fire.

Based on review of the written policies provided by the clinics and interviews with their representatives,[15] the review team concluded the clinics employed at least basic physical safeguards. In six of the clinics, privacy officers and medical directors were not aware of where or how the clinic secured employee personal information, including the personal information of physicians, medical office assistants, and other staff. In one instance, the respondent reported that a bookkeeper managed the personnel records and payroll but that they were not aware of how the bookkeeper stored the records and there was no contract in place to detail expectations for privacy and confidentiality of personal information. One clinic respondent, at

[15] The OIPC did not independently verify these safeguards.

the only clinic in the sample that had not acquired an EMR system, was also not aware of how paper files were destroyed.

3.4.3 Technological safeguards

Common technological safeguards and best practices reported by clinics or noted in clinic policies included:

- passwords and authentication for EMR;
- 90-day password expiry;
- key card access to computers;
- portable laptops to access EMR (carried with physicians);
- timed auto-logout for EMR and computers;
- real-time or daily backups to offsite servers;
- storage in Canada;
- regular software updates;
- firewalls and virus scanners;
- encryption for hard drives and mobile devices;
- retention of access logs for audits of electronic user access;
- internet access on a separate computer; and
- secure fax that saves directly in EMR.

Considering the prevalence of digital technology in medical clinics and the shift from paper-based to electronic records, clinics must incorporate technological safeguards in their privacy management programs. Most of the clinics reported employing at least basic technological safeguards. Only one of the clinics included in the sample did not utilize electronic medical records though their policy noted that they maintained unique passwords, firewalls, software updates, and encryption when patients request or purchase a product or service online.

One technological safeguard absent from medical clinic policies and interviews is the use of proactive detection systems for compliance monitoring processes of electronic medical records. Third party providers of electronic systems for medical records can implement audit tools that automatically identify occasions where there is potential for unauthorized access to patients' personal information. Clinics could review reports to determine whether a breach involving personal information has occurred. Examples may include system flags when employees' access:

- personal information of patients with the same last name or the same address;
- an overly large number of records during a given period; or
- personal information of specific patients who may be well-known.

In addition, it is important to conduct random audits of all individuals who accessed electronic medical records during a specified time period. While proactive detection is not specifically stated under PIPA, the legislation does mandate that organizations make reasonable security arrangements to protect personal information from unauthorized access or similar risks.

RECOMMENDATION 15
Clinics should review administrative, physical, and technological safeguards and ensure they are reasonable considering the type and sensitivity of personal information the clinic collects.
RECOMMENDATION 16
Clinics should conduct regular risk assessment, audit and compliance monitoring activities.

4 SUMMARY OF RECOMMENDATIONS

1. Clinics should ensure adequate funding and resources for effective privacy management programs.
2. Clinics without privacy officers must immediately designate one or more individuals to be responsible for ensuring the clinic complies with PIPA.
3. Clinics should establish, document, and communicate clear internal reporting structures for issues related to privacy management.
4. Clinics should develop and maintain an inventory of all types of personal information the clinic collects, the purposes for collection, where the information is stored, and its sensitivity.
5. Clinics should develop and maintain policies and practices necessary to meet the obligations under PIPA, including developing a process to respond to privacy complaints.
6. Clinics should provide mandatory training and education for all staff, physicians, contractors and others who may access personal information the clinic collects.
7. Clinics should ensure that all staff, physicians, contractors, and others who access personal information review the clinic's privacy policies and sign a confidentiality agreement.
8. Clinics should establish, document, and communicate clear breach reporting and response processes.

9. Clinics should ensure written contracts and information sharing agreements express expectations for privacy protection.
10. Clinics should develop processes to identify and mitigate privacy and security risks for all clinic processes that involve personal information, including risk assessment prior to any new collection, use or disclosure of personal information.
11. Clinics should develop an annual review plan that details how the clinic will monitor and assess the effectiveness of the clinic's privacy management program.
12. Clinics should limit their collection of personal information online and provide patients with unique userIDs for online booking.
13. Clinics must notify individuals in clear terms of the purposes for which they are collecting personal information online.
14. Clinics should post privacy policies online that detail the collection, use, and disclosure of personal information through the website (including device identifiers).
15. Clinics should review administrative, physical, and technological safeguards and ensure they are reasonable considering the type and sensitivity of personal information the clinic collects.
16. Clinics should conduct regular risk assessment, audit and compliance monitoring activities.

5 CONCLUSION

Medical clinics collect, use, and disclose vast amounts of people's most sensitive personal information. While new technologies allow for improved handling, storage, retention and disclosure of such information, they also create greater potential risk given the volume and sensitivity of the information. It is therefore imperative that medical clinics work to protect the personal information in their custody or under their control.

These safeguards are necessary to maintain the public's trust and confidence in our medical system.

This compliance review is illustrative of how medical clinics can vary widely in their compliance with the legislated obligations under PIPA. While some have done a good job, others need to attend to developing, implementing, and maturing their privacy management programs. This involves ensuring appropriate resources, policies and procedures, training, and compliance monitoring are in place to safeguard personal information.

Each of the 22 clinics involved in this review will receive a summary of findings and recommendations pertinent to their own clinic. This report also provides 16 general recommendations that will assist those subject to this review, and clinics across BC, in meeting their legal duties under PIPA.

The OIPC encourages medical clinic staff, managers and physicians to seek out additional guidance that is available through the College of Physicians and Surgeons of BC, Doctors of BC, and OIPC.

6 ACKNOWLEDGEMENTS

I would like to thank Tanya Allen, Director of Audit and Systemic Reviews, and Jill Nevile, Policy Analyst, who conducted this compliance review and drafted this report.

September 25, 2019

Michael McEvoy
Information and Privacy Commissioner
for British Columbia