Protecting privacy. Promoting transparency.

Order P15-01

PARK ROYAL MEDICAL CLINIC

Hamish Flanagan
Adjudicator

April 14, 2015

CanLII Cite: 2015 BCIPC 20
Quicklaw Cite: [2015] B.C.I.P.C.D. No. 20

Summary: A complainant alleged that a named employee of the Park Royal Medical Clinic disclosed information in a patient's records contrary to PIPA. The complainant also alleged that the Clinic's complaint investigation did not satisfy the requirements for dealing with complaints in s. 5 of PIPA and that the Clinic did not have reasonable security arrangements to protect the patient's personal information in its custody as required by s. 34 of PIPA. The complainant's allegation that the Clinic's employee made an unauthorized disclosure of the patient's information was not supported by the evidence. However the adjudicator found the Clinic did not have a complaint process that complied with s. 5 of PIPA. The Clinic also did not have reasonable security arrangements to protect the patient's personal information in its custody as required by s. 34 of PIPA. The Clinic was ordered to comply with ss. 5 and 34 of PIPA.

Statutes Considered: BC: *Personal Information Protection Act*, ss. 5, 18, 34. **AB**.: *Personal Information Protection Act*, s. 6.

OIPC BC Orders Considered: Order F14-01, 2014 BCIPC 5 (CanLII); Order P06-04, 2006 CanLII 37938 (BC IPC); Order P13-02, 2013 BCIPC 24 (CanLII); Investigation Report F13-02, 2013 BCIPC 14 (CanLII).

AB.: Order P2006-004, 2006 CanLII 80865 (AB OIPC); Order P2010-001, 2010 CanLII 98623 (AB OIPC).

INTRODUCTION

[1] This inquiry arises from a complaint that a named employee of the Park Royal Medical Clinic ("Clinic") disclosed a patient's medical information without consent, and without complying with the *Personal Information Protection Act* ("PIPA"). The complainant, who is the patient's parent, also alleges that the Clinic did not comply

with the requirements for dealing with complaints in s. 5 of PIPA. Also at issue in this inquiry is whether the Clinic has reasonable security arrangements to protect personal information in its custody as required by s. 34 of PIPA.

ISSUES

[2] The issues in this inquiry are whether:

1) a named employee of the Clinic disclosed patient personal information without consent in circumstances that breached s. 18 of PIPA;
2) the Clinic met its obligation under s. 5 of PIPA to develop and follow a process for responding to complaints;
3) the Clinic had reasonable security arrangements to protect the patient's personal information as required by s. 34 of PIPA.

[3] PIPA is silent about the burden of proof.[1] As previous orders have stated,[2] it is therefore in the interests of each party to provide argument and evidence to justify its position.

DISCUSSION

[4] **Background**—The patient visited the Clinic for a medical consultation. On arriving, the patient discovered she knew one of the Clinic employees (the "Employee"). The patient proceeded with her medical consultation and obtained a diagnosis of her medical issue. Concerned about the privacy of her personal information she requested that the doctor keep her personal medical information, including her diagnosis, from the Employee.

[5] The patient subsequently discovered that several people knew of her medical diagnosis.

[6] The patient's parent verbally complained on the patient's behalf to the Clinic, alleging the Employee had disclosed the patient's information without consent and contrary to PIPA. The Clinic's privacy officer requested the complaint in writing. After investigating the complainant's written complaint, the Clinic's Medical Director responded in writing to the complaint. Unsatisfied with the Clinic's response, the complainant requested the Office of the Information and Privacy Commissioner for BC ("OIPC") review the Clinic's actions. OIPC mediation did not resolve the outstanding issues and the matter proceeded to an inquiry under s. 50 of PIPA.

---

[1] Section 51 of PIPA.
[2] See for example Order F14-01, 2014 BCIPC 5 (CanLII) at para 2.

Preliminary Matters

[7] *Delay* - In its initial submission the Clinic said it reserved the right to argue that the Clinic has been denied procedural fairness and suffered prejudice as a result of time delays prior to this inquiry.[3] It stated it would address the issue as necessary once it received the complainant's evidence. In its reply submission the Clinic stated that the pursuit of the complaint did not proceed with due diligence and the resulting delay prejudiced the Clinic.[4] In particular it said that some of the complainant's evidence was supplied after a significant delay. Ultimately, the Clinic did not request any particular remedy, but instead emphasised that the delay reduces the credibility and reliability of the complainant's evidence.

[8] I will consider all of the submissions provided by the parties to this inquiry, including those of the Clinic about the weight to be given to the evidence.

[9] *Oral hearing* - In their submissions, both parties said they reserved the right to request an oral hearing once they received full submissions from the other party. An oral hearing would examine credibility issues at the heart of the differing accounts of events, particularly whether the Employee disclosed the patient's medical information. However, in the end, neither party requested an oral hearing.

[10] An oral hearing can be useful when issues of witness credibility are in issue, as they are in this inquiry. While I do have discretion to hold an oral hearing, the parties did not pursue one in this matter, and I can appreciate that they may have good reasons for deciding not to do so. These reasons may include that an oral hearing would duplicate, or at least render partly redundant, the significant investment the parties (who are both represented by lawyers) have made in preparing written submissions. Also, as the Clinic notes in its submissions, significant time has elapsed since the events in issue. Both parties also note the stress that this process has created on those involved. An oral hearing would further extend the time to obtaining finality on this matter and place additional stress on the parties. There may also be other considerations in the parties' decision to not pursue an oral hearing. In summary, I accept that based on a weighing of various factors, the parties opted not to pursue an oral hearing, but instead to have the issues decided based on their written submissions. Accordingly, I will proceed to determine the issues in this inquiry based on the written submissions before me.

Unauthorized disclosure— s.18

[11] The complainant alleges that the Employee disclosed some of the patient's medical information without the patient's consent. The Clinic's complaint investigation concluded that the alleged breach did not occur. The Clinic says that the evidence, including its own investigation, does not support the allegation.

---

[3] Clinic initial submission summary at para 4(a).
[4] Clinic reply submission summary at para. 8.

[12] Section 18 of PIPA contains exceptions to the general rule that disclosure of an individual's personal information without consent is prohibited. It is common ground between the parties that if the complainant's allegation is true, such a disclosure would not comply with s. 18 of PIPA. What is in dispute is whether an employee of the Clinic made a disclosure of the patient's information.

[13] The complainant alleges that the Employee disclosed sensitive personal information comprising a medical diagnosis about the patient to third parties in a social setting. It is clear that if such a disclosure did occur, it was without the patient's consent and would be a breach of s. 18 of PIPA.

[14] The patient argues that because various individuals learned of her medical diagnosis without her telling them, their knowledge must have come from an unauthorized disclosure by the Employee. The patient says that the Employee disclosed her diagnosis to five named individuals.[5]

[15] The complainant's evidence comprises an affidavit of the patient, a printed copy of a text message exchange between the patient and a male friend, and a notarized statement by another friend ("Friend").

[16] The patient's affidavit says that the patient was told by the Friend that the Employee looked at the patient's medical records and disclosed the patient's diagnosis to the Friend and others at a party. This affidavit is supported by a notarized statement from the Friend stating that the Employee made the disclosure.

[17] The text message exchange is between the patient and a male friend who is one of the five named individuals the patient says the Employee disclosed the patient's diagnosis to. In the exchange, the male friend confirms that the Employee made disclosures about the patient's medical problems in his presence.

[18] The Clinic submits that the complaint is based on unreliable hearsay evidence, and that there is no evidence to support the patient's statement that the Employee made an unauthorized disclosure of the patient's information. It also says that the Friend's unsworn statement is contradicted by affidavit evidence from the other named individuals who the patient alleges the Employee disclosed her personal information to. The Clinic says that the text message exchange is hearsay and its meaning is vague. It also says that portions of the patient's affidavit are inconsistent with the documentary evidence and with the sworn affidavit evidence of others.

[19] The Clinic's evidence comprises affidavit evidence from:

1) the Employee who allegedly made the disclosure;
2) the Clinic Medical Director who investigated the disclosure complaint;
3) the Clinic's privacy officer;

[5] Exhibit D to the patient's affidavit.

4) the Clinic employee who trained the Employee; and
5) three of the four named individuals the patient identifies as having been present when the disclosure occurred.

[20] The Clinic also supplies Clinic documents created at the time of the patient's visit, a record created by the privacy officer at the time the complainant first phoned to complain about the alleged disclosure, and a printout of a social media conversation that discusses the patient.

[21] The parties' positions, are in direct conflict and cannot be reconciled. Mediation having been unsuccessful, this inquiry requires me to prefer the evidence of one party over another. For the reasons that follow I find that the evidence as a whole supports the Clinic's version of events and that there was no unauthorized disclosure of the patent's information.

[22] The complainant's evidence comprises almost entirely unsupported assertions or hearsay statements about what the Friend told the patient about unauthorized disclosures of the patients' information. The evidence that is not hearsay is the Friend's notarized statement that the Employee made unauthorized disclosures in the presence of her and several others. The notarized statement does not identify who those individuals were. In her affidavit, the patient names four other individuals, in addition to the Friend, who she knows were aware of her medical diagnosis. The Clinic has provided sworn affidavits from three of them, in which they deny both that the incident occurred and that the Employee ever disclosed any of the patient's personal information to them. The Clinic notes that it has been unsuccessful in reaching the remaining named individual, who is the male friend who was a party to the text message exchange provided by the complainant.

[23] In addition to the affidavit evidence of the three named individuals who dispute the patient's account of what took place, the Clinic provided an affidavit from the Employee, in which she denies making the alleged disclosure. Further, the Clinic's investigation also concluded that the alleged disclosure did not occur, though I put little weight on that finding due to shortcomings in the Clinic's complaint investigation process that I discuss below.

[24] Another issue with the complainant's evidence is that portions of it are inconsistent with documentary evidence created at the time of the events. For example, the patient's evidence about which doctor she saw during her consultation is contradicted by the Clinic's records, which show that the doctor the patient said they saw was not working that day. Details of the patient's interactions with the Employee are also contradicted by documentary evidence created at the time of those events. For instance, the patient's statement about what was disclosed to the Employee regarding the reason for the patient's visit to the clinic is contrary to the notes in her patient file taken at the time of the visit. In addition, the complainant's allegation about the Clinic's lack of initial response to her verbal complaint is contradicted by written notes taken by the Clinic's privacy officer on the date of the conversation. The patient acknowledges in

her reply affidavit that she may have been mistaken on some details. While the inaccuracies noted are not determinative of whether the alleged breach occurred, they do cast some doubt on the reliability of the patient's evidence, and the patient was unable to allay this doubt through supporting documentary or other evidence.

[25] I also observe that the Friend's notarized statement is not a sworn statement and it lacks supporting detail such as specific dates and names of the individuals who allegedly heard the disclosure. The fact that the notarized statement was produced some considerable time after the events to which it relates, may explain its lack of specificity. It is evident that repeated requests to the Friend for a statement to support the complainant's allegations were made before the Friend provided the notarized statement. The evidence suggests that this delay was the result of some reluctance by the Friend to provide a statement. These facts diminish the weight that can be placed on the Friend's evidence.

[26] The complainant's other main piece of evidence is the printout of a text message exchange between the patient and the male friend. This evidence is also hearsay and not sufficiently precise or detailed to support the complainant's allegations such that I can give it little weight.

[27] It is also difficult to attribute any of the individuals' knowledge of the patient's diagnosis to a disclosure by the Employee, rather than to other possible sources. The parties agree that the same information allegedly disclosed by the Employee was circulating as a rumour before the patient visited the Clinic. In support, the Clinic submitted a printout of a social media conversation, dated before the patient's visit to the Clinic, which shows this rumour being circulated. Further, the patient acknowledges that she disclosed the information in issue to at least one individual before the alleged unauthorized disclosure, and to others subsequently. While these two facts do not directly contradict that an unauthorized disclosure occurred, it does make it difficult to conclude with any certainty that the patient's medical information was being publicly circulated due to an unauthorized disclosure by the Employee.

[28] In summary, faced with conflicting evidence about whether the Employee disclosed the patient's information I prefer the evidence of the Clinic. For all of the above reasons, I find there is insufficient evidence to support a finding that the Clinic breached s. 18 by making an unauthorized disclosure of the patient's personal information.

Complaint process— s. 5

[29] Section 5 of PIPA provides:

> **Policies and practices**
>
> **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).

[30] The question regarding s. 5, as described in the *Notice of Inquiry* and *Investigators Fact Report* for this inquiry is whether the Clinic met its obligation to develop and follow a process for responding to complaints.

[31] The complainant says that the Clinic's investigation did not comply with s. 5 of PIPA.[6] The complainant says that the Clinic failed to respond properly to her concerns. She disputes that the Clinic even has policies or procedures to deal with complaints because the Clinic has not disclosed what they are. However, if policies and procedures exist, she says they fail to meet the standards required by PIPA. She says that neither the complainant nor the complainant's key witnesses were contacted to participate in the investigation. She says that the Clinic's process for investigating her complaint comprised asking the relevant employee if a breach occurred and, on the basis of the employee's denial, concluding that no breach had occurred and that no further action was required. She says in taking only these steps, the Clinic failed to discharge its obligations to investigate and respond to complaints.

[32] The Clinic says that it did comply with its obligations under s. 5 of PIPA, and explains its process in its submissions and supporting affidavits. It says it took immediate steps to investigate the complaint.[7] In particular, it provides documentary evidence that its privacy officer recorded the patient's name and contact information, the complainant parent's name, and some details of the conversation about the complaint, including the privacy officer's request for a written complaint addressed to the Clinic's Medical Director. The affidavit of the Clinic's Medical Director says that after receiving the complaint (dated January 4, 2013) in writing, he immediately showed the letter to the Employee and the Clinic's privacy officer. The Medical Director says he spoke in detail with the privacy officer and the Employee, then later sent the Clinic's response letter. The Medical Director's February 8, 2013 response letter to the complainant acknowledges the allegations, says the Clinic has completed its investigation, explains the Clinic's position is that no unauthorized disclosure occurred, and describes some of the general safeguards the Clinic has in place.

[33] In assessing whether the Clinic's process complied with s. 5 of PIPA I observe that the wording of the February 8, 2013 letter included in the Clinic Medical Director's affidavit differs from the letter received by the complainant, which is an exhibit to the patient's affidavit. Both letters are dated and signed by the Medical Director. While the letters are the same in many respects, the letter received by the complainant states that "the Clinic's Privacy Officer [named employee] has now concluded her investigation into this matter." The Medical Director's version of the letter uses the more generic language

[6] Complainant initial submission at para 36.
[7] Clinic initial submission summary at point 3.

"We have now concluded our investigation into this matter." For reasons I set out below this is significant in my view in determining the issue of whether the Clinic has met its obligations under s. 5 of PIPA.

[34] Finally, the Clinic responded to the complainant's critique that the Clinic complaint process did not involve speaking to the patient, the complainant or other individuals identified in the complainant's letter of complaint. The Clinic explains that was because of a duty of confidentiality to the patient and to protect the patient's personal information from unauthorized disclosure. It also says the investigator was not approached or requested to speak to the complainant or the patient and others were not interviewed because a common law duty of confidentiality to the patient prevented it.

Requirements and findings— s. 5

[35] The requirement of a PIPA complaint process in s. 5(b) has not been directly considered in any previous orders. However, Alberta orders offer some insight into what is required of a process to respond to complaints under PIPA. Section 6 of Alberta's PIPA, does not require that organizations have a specific complaint process as is the case with BC's s. 5(b). However, it is otherwise similar to s. 5 of BC's PIPA in requiring that organizations develop and follow policies and practices that are reasonable to meet their obligations under PIPA, and that organizations make information about those policies and practices available on request.

[36] In Order P2006-004,[8] the Alberta OIPC considered a complaint about the Law Society of Alberta's failure to provide an individual with a copy of its policy regarding the handling of privacy complaints under Alberta's s. 6 of PIPA, the equivalent provision of s. 5 of BC's PIPA. The Law Society's privacy policy indicated that individuals who had concerns about how the Law Society had administered their personal information should contact the Law Society's Information Officer. The Alberta Commissioner accepted the Law Society submission that the policy was no more specific than that because the steps to be taken by the Information Officer would depend on the nature of the complaint.[9]

[37] In Order P2010-001[10] the Alberta OIPC, after quoting from Order P2006-004, concluded that s. 6 in Alberta's PIPA did not require written policies or practices generally:

> I take from [Order P2006-004] that a policy need not be formally or "officially" approved, so long as it is reasonable and followed by an organization. Further, the duty to provide information about a policy or practice does not impose a requirement that information be written.
> …
> In my view, the duty to develop reasonable policies and practices in order to meet obligations under PIPA does not necessarily require formally setting these policies and practices down in writing. Moreover, section 6 does not require an organization

[8] 2006 CanLII 80865 (AB OIPC).
[9] At para. 27.
[10] 2010 CanLII 98623 (AB OIPC).

> to create a document entitled a "privacy policy" or to make such a document available on request, although this may be a desirable practice.[11]

[38] Orders in BC have also taken the view that ss. 5(a) and (c) do not require written policies or practices. Order P06-04,[12] in discussing the requirement in s. 5(c) to "make information available on request about …the complaint process" required under s. 5(b) said:

> An organization may find that it is easier to simply hand over a copy of its privacy policy or complaint process than to answer questions or otherwise make information available. There is certainly a good business case for organizations to be transparent with customers, employees and others with whom they deal. Openness about good practices and policies will foster trust and thus loyalty, which can translate into repeat business and perhaps even lower employee turnover.
>
> There is, however, no duty under s. 5(c) for an organization to provide anyone a copy of any written policies and procedures, on request or otherwise. The legislative language is clear. It only requires organizations to make "information about" policies, practices and processes available on request. This interpretation both respects the clear legislative language of s. 5(c) and accords with the legislative intent underlying PIPA.[13]

[39] BC Order P13-02,[14] also says that s. 5 does not require an organization to provide information in the form of a written policy in order to comply with its obligations to make information available, and cites Order P06-04[15] as support.

[40] I have considered the Clinic's obligations under s. 5(b) in light of the wording of s. 5 and the Orders above. It is clear that an organization is required to have a complaints process and to follow it. Order P2006-004[16] and the wording of s. 5(b) support my view that having a process requires an organization to have turned its mind to what its process would be if it were to receive a complaint. However, as Alberta Order P2006-004 demonstrates, a complaint process does not have to be detailed or complicated. In my view, and consistent with the interpretation of ss. 5(a) and (c) of PIPA and its equivalent in Alberta, it is not necessary that a complaint process be in writing.

[41] I conclude that the Clinic has not demonstrated that it had a complaint process that satisfied s. 5(b) to deal with the complaint in issue. The Clinic's submissions do not contain any reference to any written privacy policies that cover complaints, or to a specific privacy complaint policy or process, or indeed any other formalized privacy training policies or procedures. While written policies or processes are not required, having written policies or processes would be good evidence of a complaint process. Further, the Clinic does not provide any evidence that it had turned its mind to what its

[11] At paras. 12 and 14.
[12] 2006 CanLII 37938 (BC IPC).
[13] At para. 73-74.
[14] 2013 BCIPC 24 (CanLII) at para. 88.
[15] 2006 CanLII 37938 (BC IPC).
[16] 2006 CanLII 80865 (AB OIPC).

process for handling a privacy complaint would be. The Clinic's submissions instead emphasize the steps it took to respond to the complaint.

[42] In addition, as noted above, the Clinic's letter received by the complainant stated that the Clinic's privacy officer had conducted an investigation, but the evidence of the Clinic itself contradicts that.

[43] The Clinic did not explain why the version of the letter submitted by the Medical Director differs from that received by the complainant. The most likely explanation for the Medical Director's version of the letter is that it was modified to accord with the Clinic's other evidence. The version of the letter submitted by the Clinic Director is consistent with the Clinic's other evidence regarding the steps taken to investigate the complaint while the version received by the complainant is inconsistent with that other evidence. In particular, the affidavit evidence of the privacy officer states that she had no involvement in the investigation after being shown the written complaint by the Medical Director.

[44] The significance of the modification to the Clinic's Medical Director's letter is that it supports a conclusion that the Clinic did not have an established process for investigating the complaint. This is because it shows that the Clinic Director told the complainant that certain investigative steps had been followed when in fact they had not. The Medical Director then appears to have attempted to amend the evidence to accord with the steps the Clinic actually took.

[45] The Clinic lacks evidence that shows it had turned its mind to a PIPA complaints process. The discrepancy in the Clinic's evidence also helps to satisfy me that it did not have an established complaints process. While the Clinic responded to the complaint by taking steps to investigate it as outlined above, those steps do not satisfy the requirements of s. 5 to have a complaint process. I conclude that the Clinic did not have a PIPA complaints process as required by s. 5(b).

[46] Though not part of my findings, I also note that the Clinic's steps to investigate the complaint do not accord with good practice. Good practices in relation to complaints processes can be found in several guidance documents. The OIPC's *Guide to PIPA* of March 2012,[17] discusses PIPA complaint investigation processes and includes a reference to resources on how to develop fair and effective complaint handling procedures. In addition, the June 2004 OIPC publication *PIPA Complaints: Tips for responding to PIPA complaints*[18] contains relevant guidance including recommending a three step process for investigating complaints under PIPA.

[47] Of particular relevance to the Clinic is the *BC Physician Privacy Toolkit* issued jointly by the BC Medical Association,[19] the College of Physicians and Surgeons of BC and the OIPC.[20] The Toolkit was designed as a general guide to assist physicians in

[17] Available at https://www.oipc.bc.ca/guidance-documents/1438
[18] Available at https://www.oipc.bc.ca/guidance-documents/1443
[19] Now called Doctors of BC.
[20] Available at https://www.doctorsofbc.ca/resource-centre/physicians/managing-practice/privacy-toolkit

meeting their obligations under PIPA.[21] The Toolkit sets out ten principles for protecting patient information in physician practices. For instance, "Principle 10: Challenging Compliance" states that there should be a process that allows patients to challenge a practice through a complaints process. The Toolkit also contains a section titled "Ten Steps to Help Physicians Comply with PIPA." Step 10 is about the importance of developing an effective complaints-handling process as part of managing privacy risks within a practice. Finally, the Toolkit includes a document titled "Managing Patient Complaints"[22] containing a section that provides ten steps for managing a complaint.

[48] I note also that proposed legislative changes to PIPA will likely require more accountability for organizations. The first recommendation in the recently published *Report of the Special Committee to review B.C.'s Personal Information Protection Act* (PIPA)[23] is that PIPA be amended to include specific requirements for privacy management and accountability. The Committee's report references and adopts a comment of the OIPC Commissioner who said that in the context of PIPA "accountability is an organization accepting and being able to demonstrate responsibility for personal information under its control."[24]

[49] A robust privacy complaints procedure gives a complainant confidence that their complaint has been properly investigated, and it can potentially prevent a matter escalating further. Therefore, in complying with my order below that the Clinic meet the requirements of s. 5, I encourage the Clinic to consider and adopt, as appropriate, the practices outlined in the guidance documents above.

Reasonable security arrangements — s. 34

[50] Section 34 of PIPA places a positive obligation on organizations to protect personal information in their custody or under their control "by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks".

[51] The complainant says that the Clinic is in breach of s. 34 of PIPA by failing to have reasonable security arrangements to ensure that the patient's personal information was safe from unauthorized access. In particular, the complainant is concerned that the Clinic did not take steps to implement the patient's request that the Employee not be able to view her patient record.[25]

[52] The Clinic says it took adequate steps to ensure the patient's personal information was protected. It says it provided the Employee with:

1) comprehensive training including detailed information about the importance of safeguarding patient confidentiality;

[21] https://www.doctorsofbc.ca/sites/default/files/bc_physician_privacy_toolkit_warning_and_disclaimer.pdf
[22] https://www.doctorsofbc.ca/sites/default/files/managing_patient_complaints.pdf
[23] Tabled in the B.C. Legislature on Feb. 16, 2015.
[24] At p. 10.
[25] Affidavit of patient initial submission at para. 7.

2) access to experienced staff during training for any further information or direction required;

3) a confidentiality agreement the Employee was required to sign after a detailed discussion about the need to protect patient confidentiality.

[53] The Clinic's evidence is that in response to the patient's request, and contrary to regular practice in the Clinic, the Employee was not given the patient's physical file after the patient's consultation. Further, the Clinic says the Employee never saw the patient's file again until shown it as part of the Clinic's investigation.[26]

[54] The reasonableness of security arrangements is measured on an objective basis. While reasonableness does not require perfection, depending on the situation, it may signify a high level of rigour.[27] In discussing what "reasonable security arrangements" entail in a given case, Order P06-04 identified factors to consider including:

- 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.[28]

[55] The first factor is particularly relevant. The OIPC *Guide to PIPA* cites patient records in a medical practice as the example of information for which a reasonable person would expect a high standard of security.[29] Personal health information is recognised as one of the most sensitive categories of personal information.[30] Undoubtedly, the level of sensitivity requires an accordingly high level of physical, administrative and technical security measures for the information.[31]

[56] Physical security is always a critical aspect of reasonable security arrangements. Given that the evidence suggests that the Clinic's patient records are largely paper-based, physical security measures are the main method for securing information. However, I will also consider what the evidence reveals about the Clinic's administrative and technological security arrangements. I will now consider the Clinic's security measures.

---

[26] Affidavit of Employee at paras. 31-32.
[27] Investigation Report F13-02, 2013 BCIPC 14 (CanLII).
[28] P06-04, 2006 CanLII 37938 (BC IPC) at para 80 referring to Investigation Report F06-01, 2006 CanLII 13536 (BC IPC).
[29] At p.38.
[30] Investigation Report 13-02, 2013 BCIPC 14 (CanLII).
[31] Investigation Report 13-02, 2013 BCIPC 14 (CanLII).

[57] In addition to not being given the patient's file after the patient's consultation, the Employee also says that she did not access the file at all until shown it in relation to the Clinic's complaint investigation. However, the Clinic did not provide any information about what, if any specific measures were implemented to secure the patient's file from being accessed by the Employee on an ongoing basis, or what physical security measures the Clinic employs for patient records generally. In my view, specific measures to ensure the Employee had no access to the information after the patient made her specific request of the doctor were required to satisfy s. 34.

[58] As noted above, administrative security, which encompasses policies and training regarding privacy is another important component of reasonable security, particularly given the sensitive nature of the information the Clinic handles.

[59] The Clinic's evidence is that patient confidentiality and privacy were stressed during the Employee's training. The confidentiality agreement signed by the Employee refers to the Clinic having policies and procedures regarding the privacy, confidentiality and security of personal patient information. However, no evidence of any written guidance or instructions relating to privacy are contained in the Clinic's evidence. The Clinic's checklist for training new Clinic employees, while sufficiently detailed to include a checkbox for explaining the process for changing lightbulbs contains no checkbox related to privacy or confidentiality training or guidance. I also note that the Clinic privacy officer says in her affidavit that she is not involved in employee training. Further, the confidentiality agreement signed by the Employee, as the Clinic itself notes, was signed more than four months after the Employee commenced work at the Clinic, and incidentally, after the patient's visit.

[60] The Clinic said the Employee had access to experienced staff during her training period. The Clinic provided detailed employment histories for the Clinic employees who were involved in investigating the complaint and/or training the Employee. None of those employees' employment histories, including the Clinic's privacy officer, contained any reference to having any privacy or security training or experience. The privacy officer's evidence also contains no reference to the Clinic having any privacy training, policies, or practices. Further, the fact that the investigator's response letter to the complainant references the "Privacy Act" rather than the relevant legislation (i.e. PIPA) indicates a general lack of awareness of PIPA and its requirements.

[61] Relevant to the Clinic's administrative measures, I note that the privacy officer's evidence discloses that after the Medical Director showed her the complainant's written complaint letter, he gave her a copy of it to "keep on file".[32] While it is not clear what file that refers to, creating a duplicate of a complaint letter containing sensitive information to keep on file can increase the risks of maintaining reasonable security over sensitive information, because it means the information exists in one more location where it may be accessed by and therefore potentially disclosed by other Clinic employees who do not need access to it.

[32] Privacy officer affidavit at para 21.

[62] Overall, given the sensitive nature of the information the Clinic is required to manage, the evidence does not satisfy me that the Clinic has reasonable security arrangements as required by s. 34 of PIPA. While I would be surprised if they did not follow basic security measures such as locking filing cabinets and doors, the Clinic did not provide evidence to demonstrate how it exercises reasonable security (whether physical or electronic) over patient files like the one in issue. I also find that the Clinic has not demonstrated that it met its obligations under s. 34 regarding the patient's specific request to restrict the Employee's access to her patient records.

[63] In addition to the orders below, I recommend the Clinic review the OIPC's guidance on privacy management programs to ensure it employs reasonable security standards as required under s. 34.

CONCLUSION

[64] I conclude based on the evidence before me that the Clinic did not make an unauthorized disclosure of the patient's information and therefore did not breach s.18 of PIPA. However, the Clinic's response to the privacy complaint did not comply with s. 5 of PIPA, which requires organizations to develop and follow a process for responding to complaints. Further, given the highly sensitive nature of the information the Clinic collects, the lack of evidence about the Clinic's general controls over patient records, particularly the measures taken to prevent the Employee's access to the patient's record means I am not satisfied that the Clinic provides reasonable safeguards to protect personal information from unauthorized access, use, disclosure and other risks. This contravenes s. 34 of PIPA.

[65] To satisfy the requirements of ss. 5 and 34 of PIPA, the Clinic needs to be able to demonstrate that it has an adequate privacy and security program, including having a complaints process that meets the requirements of s. 5(b). I note that taking these remedial steps will put the Clinic in a much stronger position to authoritatively respond to any future complaints about a privacy breach.

[66] I order the Clinic to comply with its obligations under ss. 5 and 34 of PIPA by May 27, 2015. I order the Clinic to provide a statutory declaration to the Commissioner addressing the steps the Clinic has taken to comply with ss. 5 and 34 by this date.

April 14, 2015

ORIGINAL SIGNED BY

Hamish Flanagan, Adjudicator