Office of the Information and
Privacy Commissioner of Alberta

Investigation Report P2021-IR-04

***Investigation into LifeLabs Inc.'s compliance with the* Personal Information Protection Act**

October 13, 2021

LifeLabs Inc.

Investigations 014711 and 014712

Table of Contents

Background

[1] On December 16, 2019, LifeLabs Inc. (LifeLabs or the Organization) notified the Office of the Information and Privacy Commissioner (OIPC or the Commissioner's office) of a privacy breach. The Commissioner opened a breach notification file (Case File #014221) and also opened investigations into compliance under section 84(1)(a) of the *Health Information Act* (HIA, Case File #014711) and under section 36(1)(a) of the *Personal Information Protection Act* (PIPA, Case File #014712). The Commissioner delegated to me the power to require notification of any breaches, and the power to conduct the investigations and to issue orders in the investigations, if that became necessary.

[2] On December 17, 2019, LifeLabs publicly announced a cyberattack it incurred that resulted in unauthorized access to customer information. LifeLabs indicated that the information "could include name, address, email, logins, passwords, date of birth, health card numbers, gender, phone numbers, password security questions and lab test results." LifeLabs said the information relating to approximately 15 million customers was potentially affected by this breach and that the "vast majority of these customers are in B.C. and Ontario". LifeLabs also said that a relatively small number of customers in other provinces may have been affected, including Albertans.

[3] On January 9, 2020 LifeLabs reported the following to the Commissioner's office:

> Through the proactive surveillance of our IT systems, LifeLabs identified a cyber-attack involving unauthorized access to some of our computer systems. Immediately upon discovering the incident we engaged world-class cybersecurity experts to isolate and secure the affected systems, and determine the scope of the breach. … The attack primarily involved two webservers and two databases operated by LifeLabs. The vast majority of the affected customers are in B.C. and Ontario, with relatively few customers in other locations.

[4] On March 17, 2020, I issued Breach Notification Decision P2020-ND-036 to LifeLabs under PIPA. On that same date, I sent a letter to LifeLabs, explaining why I had issued Breach Notification Decision P2020-ND-036 under PIPA and not under the HIA.

[5] Subsequently, I proceeded with the compliance investigation. On June 3, 2020, I sent written questions to LifeLabs. LifeLabs responded to my questions and provided policy documents. On July 7, 2020, I sent follow-up questions to LifeLabs.

[6] In an email dated July 28, 2020, LifeLabs raised the issue about the Commissioner's jurisdiction. On July 29, 2020, LifeLabs provided answers to my follow-up questions, as well as more fulsome comments about jurisdiction.

[7] On August 20, 2020, I asked LifeLabs for evidence regarding jurisdiction. On September 4, 2020, LifeLabs provided me with a document (the September 4, 2020 document), which it marked as privileged and confidential.

[8] I subsequently finalized a written draft of the investigation report.

[9] As a matter of procedural fairness, it is the practice of the Commissioner's office to send the draft of the investigation report to the person under investigation, so that the person can inform the Commissioner of any factual errors and comment on any such errors the person identifies.

Consequently, on March 4, 2021, I sent a draft of the investigation report to LifeLabs, who requested an extension of time to respond. I granted that extension.

[10] On April 1, 2021, LifeLabs provided me with, among other things, a 26-page table in which it identified the relevant passages (paragraph references to the draft investigation report) and set out the "correction, clarification or additional context" for each of those passages. LifeLabs also provided me with a letter that set out the following:

- its objection to the inclusion of any information contained in the September 4, 2020 document, on the basis that privilege or confidentiality applied to the information contained in that document (LifeLabs also provided affidavits to support its claims of privilege and confidentiality);
- its further comments as to whether or not the Alberta OIPC should assert jurisdiction in this matter; and
- its comments on whether the Alberta OIPC should publish the final investigation report.

[11] I will comment here that receiving a draft of an investigation report for fact checking is not an invitation for a party to seek to have an investigation report rewritten as a party might prefer. Consequently, while I have considered and assessed everything that LifeLabs provided to me on April 1, 2021, I have not found it necessary in this final investigation report to include or comment on everything that LifeLabs says is "clarification" or "additional context". Also, I have not included anything on the issue of publishing, as that is a matter for the Commissioner to decide under section 38(6) of PIPA.

Jurisdiction

***Health Information Act* (HIA)**

[12] The Commissioner has jurisdiction to conduct compliance investigations under the HIA.

[13] The applicable provisions of the HIA read:

> 84(1) In addition to the Commissioner's powers and duties under Divisions 1 and 2 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure its purposes are achieved, and may
>
> (a) at the request of the Minister or otherwise, conduct investigation to ensure compliance with any provision of this Act or compliance with rules relating to the destruction of records set out in an enactment,
>
> (b) make an order described in section 80 whether or not a review is requested,…

[14] The HIA applies to "custodians" as defined, in respect of "health information", as defined.

[15] LifeLabs operates four business divisions – LifeLabs, LifeLabs Genetics, Rocky Mountain Analytical and Excelleris. These divisions provide services directly to health practitioners such as physicians or naturopaths and on behalf of organizations such as The Alberta School Employee Benefit Plan.

[16] In my March 17, 2020 letter that I sent to LifeLabs (along with Breach Notification Decision P2020-ND-036), I said in part:

> "Custodian" is defined in section 1(1)(f) of the HIA, and includes a health services provider who is designated in the regulations as a custodian, or who is designated within a class of health services providers that is designated in the regulations for the purpose of subclause (ix) of section 1(1)(f).
>
> LifeLabs is not included in the list of custodians in section 1(1)(f), and is not included in the regulations as a designated custodian: see *Health Information Regulation*, AR 70/2001, section 2. Therefore, LifeLabs is not a custodian, and the HIA does not apply so as to require LifeLabs to notify under section 60.1(3) of the HIA.
>
> …
>
> "Affiliate" is defined in section 1(1)(a) of the HIA, and includes a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian.
>
> To begin, I note that naturopaths and the Alberta School Employee Benefit Plan, both of which use LifeLabs, are not custodians under the HIA. Neither is any other regulated health professional under the *Health Professions Act* who is not included as a designated custodian in section 2 of the *Health information Regulation* (for example, acupuncturists, laboratory and X-Ray technologists, medical laboratory technologists, medical diagnostic and therapeutic technologists, paramedics, physiotherapists and psychologists). Therefore, LifeLabs cannot be in an affiliate relationship with these entities, for the purposes of the HIA.

LifeLabs says that it has contracts with custodians. It provided me with the following two documents: Healthcare Professional (HCP) Registration Form (the Registration Form), and Healthcare Professional (HCP) Credit Card Authorization (the Credit Card Authorization).

The Registration Form is primarily about the payment options for laboratory tests and who is going to pay for those tests, whether the healthcare professional (Option 1) or the patient (Option 2). The Agreement in the signature block of the Registration Form reads:

> I have read the payment options and understand how each option works. I will abide by the terms and conditions of the option I have selected. I understand that this option will apply unless I submit a request to change my preferences. I further certify that I am a member of a regulated health profession and I am competent to evaluate test results that are applicable to my scope of professional practice.

The Credit Card Authorization reads in part:

> I authorize Rocky Mountain Analytical and LifeLabs to bill my credit card (personal or clinic) for the requested laboratory services. If for any reason my credit card is not accepted I understand that I am financially responsible to Rocky Mountain Analytical and LifeLabs and that Rocky Mountain Analytical and LifeLabs may bill me based on the full price for the laboratory work performed.

LifeLabs conducts laboratory tests for individuals and refers to those individuals as its "customers". Given the Registration Form and the Credit Card Authorization, it is not clear to me how conducting laboratory tests for patients (its "customers") would be a service for a custodian so as to bring LifeLabs within the definition of "affiliate", particularly if the patient pays for the service (Option 2).

Moreover, the "identifying health information" that was accessed without authority (including laboratory test results) has to be in the custody or control of a custodian in order to bring LifeLabs within the definition of "affiliate". The information that was accessed was in LifeLabs' databases. There is no evidence before me that the identifying health information was in the custody or control of a custodian, as required by section 60.1(1).

Furthermore, if LifeLabs were an affiliate, section 60.1(1) of the HIA requires that it notify all custodians to whom it is providing services, and not the affected individuals. I have no evidence that LifeLabs has notified custodians, as it would be required to do if it were an affiliate of those custodians. It is an offence under section 107(1.2) of the HIA for an affiliate to fail to comply with section 60.1(1).

Finally, no custodians have notified the Commissioner as they would be required to do under section 60.1(2) of the HIA if LifeLabs, as the affiliate of the custodians, had notified the custodians. It is an offence under section 107(1.1)(b) of the HIA for a custodian to fail to comply with section 60.1(2).

In my view, the legal status of LifeLabs under the HIA is far from clear. Therefore, to the extent that LifeLabs is an affiliate of a custodian and identifying health information is in the custody or control of the custodian, LifeLabs must notify the custodian, who must then notify me (the delegate of the Commissioner), the Minister and the affected individual under the HIA.

[17] To the extent that LifeLabs is not an affiliate of a custodian and the personal information is in its control, then LifeLabs itself must notify me (the delegate of the Commissioner) and affected individuals under PIPA.

[18] At that time, LifeLabs did not respond to the contents of my March 17, 2020 letter about the HIA not applying and PIPA applying. Instead, on March 30, 2020, it asked to notify indirectly under PIPA.

[19] Based on the analysis in my March 17, 2020 letter and no further evidence from LifeLabs that it is a custodian under the HIA, I find that, in this investigation, the HIA does not apply to LifeLabs.

***Personal Information Protection Act* (PIPA)**

[20] The Commissioner has jurisdiction to conduct compliance investigations under PIPA.

[21] The applicable provisions of PIPA read:

> 36(1) In addition to the Commissioner's powers and duties under Part 5 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may
>
> (a) conduct investigations to ensure compliance with any provision of this Act;
>
> (b) make an order described in section 52 whether or not a review is requested;…

[22] PIPA applies to "organizations" as defined, in respect of "personal information", as defined.

[23] In Breach Notification Decision P2020-ND-036, I found that LifeLabs was an "organization" as defined in section 1(1)(i) of PIPA. I also found that the breach involved "personal information", as defined in section 1(1)(k), consisting of: name, gender, phone number, address, email address, date of birth, login and password, Alberta Health Care number and lab results. I further said that to the extent this information was collected in Alberta and was in the control of LifeLabs, PIPA applied.

Issue About Jurisdiction

[24] In an email dated July 28, 2020, LifeLabs raised the issue about the Commissioner's jurisdiction, and followed up with more fulsome comments on July 29, 2020. LifeLabs said that, based on its analysis:

- all of the data sets involved in the attack related to services performed outside of Alberta under the auspices of other privacy and health privacy laws; [footnote omitted]
- none of the data contained in the data sets was related to health services that were performed in Alberta;
- the cyber-attack impacted only those Albertans who travelled out of the province and received services in British Columbia, Ontario or Saskatchewan; and
- no Albertan had lab tests or results impacted.

[25] LifeLabs stated: "In light of these facts, we therefore respectfully request that the OIPC carefully consider what (if any) subject-matter under consideration falls under its jurisdiction."

[26] On August 20, 2020, I asked LifeLabs for evidence that Albertans' health [sic] information was not affected. On September 4, 2020, LifeLabs provided me with a document that was marked privileged and confidential. LifeLabs said:

> Attached is a confidential data analysis conducted at LifeLabs in order to address the request below. It contains sensitive confidential business information and is provided for the sole purpose of conducting your jurisdictional analysis. LifeLabs provides this information on the basis that it will be held in confidence by the OIPC and will not be quoted from or in any other way disclosed outside the OIPC.

[27] On April 1, 2021, after LifeLabs had reviewed the draft investigation report that I had provided, LifeLabs provided me with a letter in which it outlined its claims of privilege and confidentiality over the information contained in the September 4, 2020 document, and provided two affidavits to support its privilege and confidentiality claims. LifeLabs reminded me that it had disclosed the September 4, 2020 document "…solely for the purpose of permitting the Alberta OIPC to conduct its jurisdictional analysis."

[28] LifeLabs claimed solicitor-client privilege and litigation privilege over the information contained in the September 4, 2020 document, and provided an affidavit from its General Counsel. In deciding whether information or records are subject to solicitor-client privilege, the Supreme Court of British Columbia, in *British Columbia (Minister of Finance v. British Columbia (Information and Privacy Commissioner)*, 2021 BCSC 266, at paragraph 86, said that an affidavit from a lawyer that asserts solicitor-client privilege is entitled to "some deference", as "…the lawyer's conduct is subject to the standards of the Law Society. It would be a professional error for a lawyer to misrepresent the nature of solicitor-client communications to an agency like the IPC…" I note that, under section 59(1)(e) of PIPA, it would also be an offence to make a false statement to or mislead or attempt to mislead the Commissioner.

[29] LifeLabs said that it did not waive privilege when it provided the September 4, 2020 document to the Commissioner, relying on section 38.1 of PIPA, which provides that there is no waiver of privilege if privileged information is disclosed to the Commissioner. LifeLabs maintained that "To publicly disclose either the [September 4, 2020 document], its contents, or the conclusions drawn from the OIPC's analysis of the [September 4, 2020 document] would undermine the rationale for solicitor-client privilege by inhibiting necessary communication of information between client and lawyer."

[30] Nevertheless, LifeLabs is relying on the September 4, 2020 document to support its position that I have no jurisdiction over LifeLabs. It also maintains that I cannot publicly disclose the conclusions that I draw from the information contained in the September 4, 2020 document.

[31] To be clear, if I found that information or a record were subject to solicitor-client privilege, I would not publicly disclose it. However, I do not find it necessary in this investigation to decide whether the information contained in the September 4, 2020 document is privileged and therefore confidential, or whether there has been some kind of a waiver based on LifeLabs' reliance on the information. I simply do not find it necessary here to publicly disclose any information contained in the September 4, 2020 document because of Breach Notification Decision P2020-ND-036, which has been published.

[32] In Breach Notification Decision P2020-ND-036 issued on March 17, 2020, I found that I had jurisdiction over LifeLabs under PIPA. My decision was based on the evidence that LifeLabs had provided to date, as is the case with all breach notifications, which are issued on an expedited basis because of the necessity to notify. Furthermore, I am *functus officio* in relation to that decision and cannot change it.

[33] Breach Notification Decision P2020-ND-036 was also based on the Exemption Order (see below), which is applied in every breach notification decision of the Commissioner's office.

[34] The *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219 (the Exemption Order) states:

> An organization, other than a federal work, undertaking or business, to which the *Personal Information Protection Act*, S.A. 2003, c. P-6.5, of the Province of Alberta, applies is exempt from the application of Part 1 of the *Personal Information Protection and Electronic Documents Act*, in respect of the collection, use and disclosure of personal information that occurs within the Province of Alberta.

[35] The matter raised in the Exemption Order about the circumstances in which *Personal Information Protection and Electronic Documents Act* (PIPEDA) does and does not apply is not relevant here. What is relevant is the circumstances in which PIPA applies. The Exemption Order is specific as to the collection, use and disclosure of personal information within Alberta. It makes it clear that any collection, use or disclosure of personal information within Alberta brings an organization such as LifeLabs under the Commissioner's jurisdiction for that collection, use or disclosure. The Exemption Order does not require that an organization be in Alberta when it collects, uses or discloses personal information within Alberta. The Exemption Order also does not make any distinction about whether an individual receives services in Alberta or where the Organization stores the personal information that it collects in Alberta.

[36] I observe only that there is nothing in the September 4, 2020 document that alters my initial decision in Breach Notification Decision P2020-ND-036 about my having jurisdiction under PIPA over LifeLabs' collection of personal information in Alberta. I also observe that the September 4, 2020 document supersedes and contradicts what LifeLabs said in its July 28 and 29, 2020 emails to me, which I have set out above. Consequently, I do not find it necessary to consider what LifeLabs said in those emails.

[37] In its April 1, 2021 letter, LifeLabs argued that I have no jurisdiction to "render findings based on aspects of the cyber-attack that did not affect any person who received services in Alberta", and requested that I "… withdraw all findings other than those necessary to render a decision in respect of the single database connecting to the services provided to the … individuals in Alberta."

[38] First, I disagree with LifeLabs' seeming view that this investigation is focused on the cyberattack. This investigation is not limited to the cyberattack and is focused more broadly on compliance with PIPA, as allowed by section 36(1)(a) of PIPA.

[39] Second, I disagree with LifeLabs' premise that my jurisdiction is confined to persons "who received services in Alberta". PIPA is concerned with personal information collected, used or disclosed in Alberta, and not with whether services were received in Alberta.

[40] Moreover, an organization that collects, uses or discloses personal information in Alberta must comply with Alberta privacy legislation, and this includes all aspects of compliance, as provided by section 36(1)(a) of PIPA. If an organization collects, uses or discloses personal information in Alberta, practices throughout the organization must comply with PIPA.

[41] Third, the argument about whether a given database contains personal information of Albertans, or not, has no bearing on whether LifeLabs as a whole must comply with PIPA by virtue of collecting personal information in Alberta. Further, it is typical for cyberattacks to begin in one compromised organizational system where a foothold is established, followed by lateral movement[1] to other systems as a threat actor propagates their attack across an organization. It would be prudent for an organization to establish and follow policies, practices, and safeguards (in compliance with PIPA), that protect the privacy and security of information collected in Alberta, by mitigating against the risk of a threat actor moving laterally through a compromised network.

[42] As such, I have jurisdiction and will comment on and make recommendations pertaining generally to compliance with PIPA in relation to the collection, use and disclosure of personal information in Alberta, regardless of where that information is sent and regardless of any particular system in which the information may be stored. This approach is consistent both with the liberal interpretation that is to be given to legislation such as PIPA and with the approach that the Court has taken in *Reference re Subsection 18.3(1) of the Federal Courts Act*, 2021 FC 723, in which the Court rejected a "microscopic look" at a particular aspect of an organization's business model in assessing whether federal privacy legislation applied to the organization (paragraph 59).

[43] LifeLabs further argues that I should consider a "real and substantial connection" test when deciding jurisdiction. However, as explained above, the Commissioner applies the Exemption Order and does not consider a "real and substantial connection test" (a decidedly federal test: see paragraphs 25-35 of Investigation Report P2021-IR-01, available on the OIPC's website) or any other test when deciding jurisdiction under PIPA. As I previously said, I applied the Exemption Order in Breach Notification Decision P2020-ND-036 and found that I had jurisdiction over LifeLabs' collection of personal information in Alberta.

[44] I therefore conclude that I have jurisdiction to conduct this investigation under PIPA. The Exemption Order gives me jurisdiction over LifeLabs' collection, use and disclosure of personal information in Alberta.

[45] LifeLabs also requested that I decline jurisdiction based on the "principles of comity, order and fairness". I understand that the basis for this request is that the British Columbia and Ontario Commissioners have already issued their investigation report and recommendations for the vast majority of impacted individuals (99%) and that LifeLabs is also "addressing the non-binding recommendations made by the Saskatchewan OIPC". I understand that its view is that I ought

[1] *"Lateral movement refers to the techniques that a cyberattacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools."* Crowdstrike, https://www.crowdstrike.com/cybersecurity-101/lateral-movement/ retrieved July 14, 2021.

not to "exercise jurisdiction over matters that may take place in the territory of other states". LifeLabs also expressed concern about the possibility of "inconsistent results".

[46] The collection, use or disclosure of personal information within Alberta is not a matter that takes place in the territory of British Columbia, Saskatchewan or Ontario. Because that collection, use or disclosure occurs within Alberta, Alberta legislation (PIPA) applies according to the provisions of that legislation, which may very well be different from the legislation of other provinces. It is not unusual that organizations operating in more than one province will have to meet the requirements of legislation that is not identical from one province to the next. An investigation under the legislation of one province can conceivably and not surprisingly yield different results from that of another province.

[47] I also want to touch on the "fairness" matter that was raised as the basis for me to decline jurisdiction. In my view, declining jurisdiction would impact any rights of affected individuals to have a resolution to the breach.

[48] Therefore, I will not decline jurisdiction.

Other Matters

[49] In addition to its privilege arguments contained in its April 1, 2021 letter and affidavit of its General Counsel, LifeLabs argues that the policy documents (which it provided to me in response to my June 3, 2020 questions) are "highly confidential cybersecurity documents provided on a confidential basis for the sole purpose of helping the Alberta OIPC to understand the background to the cyber-attack."

[50] In its April 1, 2021 letter, LifeLabs further says:

> The details described in the Draft Investigation Report would give anyone who chooses to review the decision (including malicious actors) detailed insights into the cybersecurity posture of LifeLabs. Even superseded polices provide details as to the strategic choices made to defend LifeLabs' systems against malicious attacks. The policies should not be described in disaggregated manner: even the titles of the policies reveal the security choices made by LifeLabs to defend the sensitive information in its systems.
>
> As further supported by the attached affidavit of [LifeLabs' Chief Information Security Officer], extended portions of the Draft Investigation Report also provided extended details and commentary on LifeLabs' post-attack security strategies, including details of ongoing remediation efforts. The decision to provide a detailed analysis of these strategies and efforts puts LifeLabs at risk of a new attack.

[51] The affidavits of LifeLabs' General Counsel and Chief Information Security Officer both make similar assertions about the policies being "highly confidential commercial information" (including the titles of the policies), the disclosure of which would create a security risk.

[52] In examining LifeLabs' claim that that content and titles of its policies are "highly confidential commercial information" that must not be publicly disclosed, I have first considered section 6 of PIPA. The relevant provisions read:

6(1) An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act.

…

(3) An organization must make written information about the policies and practices referred to in subsections (1) and (2) available on request.

[53] In my view, a statutory requirement for an organization to make information about its policies available on request is a full answer to and negates LifeLabs' position about disclosing information about its policies, including the titles of its policies. As examples of published information about policies, including the titles of policies, see Investigation Reports H2021-IR-01 and P2021-IR-02, which are available on the Commissioner's office's website.

[54] However, if I am wrong and must consider the harm alleged to result from disclosing information about, including the titles of, LifeLabs' policies that are alleged to be "highly confidential commercial information", then as an analogous standard I look to the evidence that the Court says is appropriate to demonstrate harm that could reasonably be expected to result from disclosure of information, including third party commercial information, in access requests.

[55] In *Qualicare Health Service Corporation v. Alberta (Office of the Information and Privacy Commissioner)*, 2006 ABQB 515, at paragraph 66, the Court said:

> The Commissioner's decision did not prospectively require evidence of actual harm; the Commissioner required some evidence to support the contention that there was a risk of harm. At no point in his reasons does he suggest that evidence of actual harm is necessary.
>
> The evidentiary standard that the Commissioner applied was appropriate. The legislation requires that there be a "reasonable expectation of harm." Bare arguments or submissions cannot establish a "reasonable expectation of harm." When interpreting similar legislation, courts in Ontario and Nova Scotia have held that there is an evidentiary burden on the party opposing disclosure based on expectation of harm: [citations omitted].

[56] In *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31, at paragraphs 52 and 54, the Supreme Court of Canada said:

> …As this Court confirmed in *Merck Frosst*, the word "probable" in this formulation must be understood in the context of the rest of the phrase: there need be only a "reasonable expectation" of probable harm. The "reasonable expectation of probable harm" formulation simply "captures the need to demonstrate that disclosure will result in a risk of harm that is well beyond the merely possible or speculative, but also that it need not be proved on the balance of probabilities that disclosure will in fact result in such harm": para. 206.
>
> …
>
> This Court in *Merck Frosst* adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in Merck Frosst emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibly of harm in order to reach that middle ground: paras. 197 and 199. This inquiry of course is contextual and how much evidence and the quality of evidence needed to meet this standard will ultimately depend on the nature of the issue and "inherent probabilities or improbabilities or the seriousness of the allegations of consequences: [citations omitted].

[57] In *Park Place Seniors Living Inc. v. Alberta Health Services*, 2017 ABQB 575, at paragraphs 138-139, the Court agreed that "Mere assertions or opinion, without more, are insufficient." The Court agreed with the evidentiary standard set out in the *Qualicare* decision above.

[58] The point that the Courts in the cases cited above are making is that it is not sufficient to make bald assertions or statements about harm, which is all that I have from LifeLabs. Consequently, I am not prepared to accept that disclosing information about LifeLabs policies, which section 6(3) of PIPA requires, could reasonably be expected to harm LifeLabs. I am also not prepared to accept that disclosing the titles of LifeLabs' policies could reasonably be expected to harm LifeLabs.

[59] Finally, the legislation itself determines the use to which information provided to the OIPC may be put and the disclosure of that information. Section 41(2) of PIPA reads:

> 41(2) The Commissioner may disclose, or may authorize anyone acting for or under the direction of the Commissioner to disclose, information that is necessary for the purposes of
>
> (a) conducting an investigation or inquiry under this Act, or
>
> (b) establishing the grounds for findings and recommendations contained in a report under this Act.

[60] This is the provision that gives me the authority to disclose information. It also contains the rules that I must follow when writing an investigation report in which I rely on submissions and evidence provided to me, in order to justify any findings and recommendations that I make. In many cases, I will have to reproduce parts of submissions and evidence provided to me, or summarize that information. I cannot know in advance of writing an investigation report what information will be necessary to include in the investigation report.

[61] Consequently, barring common law requirements to not disclose information (e.g., solicitor-client privilege) or other requirements to maintain the confidentiality of information because, based on evidence that a party provides, disclosure could reasonably be expected to cause harm, I am not bound by and will not accede to an attempt to restrict what information I may include in an investigation report.

Issues

[62] I identified the following issue for the investigation:

- Did the Organization protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction in accordance with section 34 of the *Personal Information Protection Act* (PIPA)?

[63] In considering under section 34 whether the Organization made reasonable security arrangements, I also considered whether the Organization complied with section 6 of PIPA (policies and practices) and with section 35 of PIPA (retention and destruction of information).

[64] I did not consider section 60 of the HIA because I have found that LifeLabs is not a "custodian" as defined in the HIA. It is custodians who have duties under section 60 to protect health information. Any custodians who contract with LifeLabs would have those duties. This investigation is not about those custodians.

Methodology

[65] I took the following steps during the course of this investigation:

- Referenced the LifeLabs' breach notification decision of real risk of significant harm under PIPA (Breach Notification Decision P2020-ND-036).
- Sent written questions to LifeLabs and reviewed the responses and documents provided (e.g., policies) for the purpose of the compliance investigation.
- Sent follow-up questions to LifeLabs, including questions about the documents provided, and reviewed the responses.
- To be procedurally fair, provided LifeLabs with a draft investigation report for fact checking and comment on March 4, 2021, considered feedback and finalized the investigation report.

Analysis, Findings and Recommendations

Issue: Did the Organization protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction in accordance with section 34 of the *Personal Information Protection Act* (PIPA)?

[66] Section 34 of PIPA states:

> 34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

[67] Reasonable security arrangements under section 34 of PIPA include administrative, technical and physical safeguards. Reasonable security arrangements for an organization must include all three to mitigate unauthorized access to personal information.

[68] Administrative safeguards include policies, procedures and processes that manage and regulate the implementation of security measures to protect an organization's technical infrastructure. Technical safeguards are the tools used to follow and adhere to the administrative safeguards. Physical safeguards are the safeguards in place to physically protect an organization and its electronic information systems from environmental hazards and unauthorized intrusion into the organization's buildings or equipment.

[69] LifeLabs described the incident as a cyberattack. Cyberattacks are technical in nature and rarely result from a lack of physical safeguards, (although it is possible). Therefore, I focused my review on administrative and technical safeguards only. However, I acknowledge that physical safeguards, such as physical access restrictions, are referenced in a number of policy documents provided by LifeLabs.

[70] I requested copies of LifeLabs's policies regarding its technical, administrative, and physical safeguards relevant to protecting the privacy and security of personal information in its custody or under its control, in effect at the time of the incident. LifeLabs provided a policy suite that was for its operations across Canada. It included:

- 12[2] "draft" policy documents that according to LifeLabs "[w]hile not formally approved at the time of the incident, … were representative of the information security safeguards employed by LifeLabs" (the drafts), and

- approximately 50 "formally adopted privacy policies and supportive materials," including "information security acceptable use policy (see AB2-7), an information technology security policy (see Exhibit AB2-46) and a remote access approval policy (Exhibit AB2-61) that had

[2] AB2-8, AB2-9, AB2-10, AB2-11, AB2-12, AB2-13, AB2-14, AB2-15, AB2-16, AB2-17, AB2-18, AB2-69

been formally adopted and were in force at the time of the incident" as stated in LifeLabs' April 1, 2021 response.

[71] Below is a non-exhaustive listing of the policies and procedures provided and an indication of whether they reference Alberta privacy law and if the policy was a draft or formally adopted at the time of the incident.[3]

Policy	**Alberta reference**	**Status**[4]
IT Policy 9007 Information Security Acceptable Use (January 31, 2019) (Exhibit AB2-7)	Notes that "In certain cases LifeLabs is required by legislation and/or regulating authorities to be able to track which individuals make changes to particular kinds of information."	Adopted
IT Security Policy - Acceptable Use (Exhibit AB2-8)	None	Draft
IT Security Policy - Data Security (Exhibit AB2-9)	None	Draft
IT Security Policy - Vulnerability Management (Exhibit AB2-10)	None	Draft
IT Security Policy - Patch Management (Exhibit AB2-11)	None	Draft
IT Security Policy - Logging, Monitoring and Auditing (Exhibit AB2-12)	None	Draft
IT Security Policy - Software Development (Exhibit AB2-13)	None	Draft
IT Security Policy - Third-Party Policy (Exhibit AB2-14)	None	Draft
IT Security Policy - Access Control (Exhibit AB2-15)	None	Draft
IT Security Policy - Disaster Recovery (Exhibit AB2-16)	None	Draft
IT Security Policy - Incident Management (Exhibit AB2-17)	None	Draft

[3] Policies provided to me by LifeLabs that were superseded by newer documents were not included in the table. Other policies provided for review also did not refer to Alberta legislation; for brevity, many were not included in the table.

[4] As characterized by LifeLabs when provided during the investigation.

IT Security Policy - Malware (Exhibit AB2-18)	None	Draft
Privacy Program Overview (Exhibit AB2-19)	None	Adopted
Access and Correction Procedure (March 2019) (Exhibit AB2-20)	HIA and reference to "PIPA," however it is not clear if this is AB PIPA or BC PIPA. "LifeLabs privacy obligations are defined in applicable privacy legislation, in particular the *Personal Information Protection and Electronic Documents Act, 2000* (PIPEDA), *Personal Health Information Protection Act, 2004* (PHIPA), *Personal Information Protection Act, 2003* (PIPA), *Health Information Act, 2001* (HIA), *Health Information Protection Act, 2003* (HIPA), the province's public sector privacy legislation where LifeLabs is providing services to a provincial ministry and in its comprehensive set of privacy policies and procedures that are associated with the *LifeLabs Master Privacy Policy*."	Adopted
Confidentiality Pledge To LifeLabs For Employees (April 19, 2018) (Exhibit AB2-26)	None	Adopted
Master Privacy Policy 2019 (Exhibit AB2-27)	HIA: "HIA means *the Health Information Act, 2001* and sets out the rules for the collection, use, disclosure and protection of health information that is in the custody or under the control of a custodian in Alberta."	Adopted
Preliminary Privacy Assessment Template (January 2019) (Exhibit AB2-31)	None	Adopted
Privacy Assurance and Risk Framework (January 2019) (Exhibit AB2-32)	HIA and reference to "PIPA," however it is not clear if this is AB PIPA or BC PIPA. "LifeLabs privacy obligations are defined in applicable privacy legislation, in particular the Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA), Personal Health Information Protection Act, 2004 (PHIPA), Personal Information Protection Act, 2003 (PIPA), Health	Adopted

	Information Act, 2001 (HIA), Health Information Protection Act, 2003 (HIPA), the province's public sector privacy legislation where LifeLabs is providing services to a provincial ministry and in its comprehensive set of privacy policies and procedures that are associated with the LifeLabs Master Privacy Policy."	
Privacy Complaints and Inquiries Procedure (March 2019) (Exhibit AB2-36)	HIA and reference to "PIPA," however it is not clear if this is AB PIPA or BC PIPA. LifeLabs privacy obligations are defined in applicable privacy legislation, in particular the Personal Information Protection and Electronic Documents Act,2000 (PIPEDA), Personal Health Information Protection Act, 2004 (PHIPA), Personal Information Protection Act, 2003 (PIPA), Health Information Act, 2001 (HIA), Health Information Protection Act, 2003 (HIPA), the province's public sector privacy legislation where LifeLabs is providing services to a provincial ministry and in its comprehensive set of privacy policies and procedures that are associated to the LifeLabs Master Privacy Policy.	Adopted
Privacy Data Request Template (May, 2017) (Exhibit AB2-37)	None	Adopted
Privacy Governance Framework (January 2019) (Exhibit AB2-38)	HIA and reference to "PIPA," however it is not clear if this is AB PIPA or BC PIPA. "LifeLabs privacy obligations are defined in applicable privacy legislation, in particular the Personal Information Protection and Electronic Documents Act,2000 (PIPEDA), Personal Health Information Protection Act, 2004 (PHIPA), Personal Information Protection Act, 2003 (PIPA), Health Information Act, 2001 (HIA), Health Information Protection Act, 2003 (HIPA), the province's public sector privacy legislation where LifeLabs is providing services to a provincial ministry and in its comprehensive set of privacy policies and procedures that are associated to the LifeLabs Master Privacy Policy."	Adopted

Privacy Webpage (2019) (Exhibit AB2-42)	"LifeLabs policies are governed by the Personal Health Information Protection Act, 2004 (PHIPA) in the province of Ontario, the Personal Information Protection Act (PIPA) in the province of British Columbia and the Health Information Protection Act (HIPA) in Saskatchewan."	Adopted
IT Policy 9016.00 Information Technology Data Centre Security (June 10 2011) (Exhibit AB2-46)	None	Adopted
IT SOP 1065 Remote Access Approval (April 9 2019) (Exhibit AB2-61)	None	Adopted
ISMS 5.1 Cybersecurity Policy (Draft June 4 2020) (Exhibit AB2-69)	Notes that "LifeLabs must comply with all relevant data-related legislation in those jurisdictions within which it operates."	Draft
RMA Access Request Form (Exhibit AB3-2)	Alberta-specific access request form "Request for Access to Personal Health Information for RMA [Rocky Mountain Analytical]."	Adopted

Administrative Safeguards

[72] Organizations, such as LifeLabs, are required under section 6(1) of PIPA to both develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act. Section 6(1) of PIPA states:

> 6(1) An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act.

[73] The obligations under PIPA include the obligation to make reasonable security arrangements to protect personal information, as provided by section 34.

[74] Therefore, PIPA specifically requires organizations to develop policies and practices that include administrative safeguards.

[75] Administrative safeguards include frameworks, policies and procedures for the management of an organization's IT infrastructure. They are developed by an organization to create rules and processes for staff, contractors and others working with the organization, and set the overall tone of the organization with respect to how information is to be protected.

[76] The administrative safeguards in place at LifeLabs or in draft at the time of the incident are set out in the table above. The following sections deal with some of the issues with those administrative safeguards.

No Alberta-specific Policies and Practices

[77] Many of the draft and formally adopted policies provided by LifeLabs fail to reference the applicable Alberta law, PIPA. Privacy laws vary across the country and it is important for all organizations that operate in more than one jurisdiction to know, understand and follow the laws within each of the jurisdictions in which they collect, use or disclose personal information.

[78] I recommend LifeLabs create Alberta-specific policies and practices as appropriate in accordance with Alberta PIPA.

Policies and Practices in Draft at Time of Incident, and Those in Force Not Followed

[79] I note that in order for an organization's policies and practices to be effective, they must be formally adopted by the organization, which should include executive sign off. Draft policies are typically still under review, subject to change and executive approval and thus cannot be relied upon as an effective administrative safeguard.

[80] In reviewing the draft policy documents, I note they each generally contain a requirement to monitor policy compliance.

[81] I asked LifeLabs to account for discrepancies between its responses to my questions and the policies provided, including requesting audit and compliance reports to demonstrate that the organization acts in a manner compliant with its written policies.

[82] LifeLabs reiterated the following in responses to my queries:

> As indicated in our response letter of June 17, 2020, the [draft policies] … were not final or formally approved at the time of the incident. Accordingly, LifeLabs could not logically have "followed" policies that were not yet in place.

[83] LifeLabs added:

> As per LifeLabs' response to [OIPC] Question 4 above, the referenced policies were in draft form and therefore not subject to audits.

[84] Its position appears to be in conflict with its own statement I previously cited:

> [W]hile not formally approved at the time of the incident, these policies were representative of the information security safeguards employed by LifeLabs

[85] Despite having a draft policy explicitly titled "IT Security Policy – Logging, Monitoring and Auditing" that states:

> LifeLabs implements logging, monitoring, and auditing systems to identify and track issues within corporate systems or applications

[86] I was not provided with any further audit, monitoring, or compliance records as they pertain to IT security, beyond the initial technical notification of the breach to LifeLabs from its security vendor (exhibit AB2-3).

[87] On April 1, 2021, LifeLabs clarified that they have safeguards in place to identify unauthorized staff access to certain information systems. Despite this, LifeLabs said it was not possible to provide compliance records due to the nature of the tool.

[88] LifeLabs did provide a spreadsheet containing a log of completed "Preliminary Privacy Assessments", or "PPAs", demonstrating compliance with its Privacy Assurance and Risk Framework (January 2019), adopted policy labelled exhibit AB2-32. This framework states:

> **Privacy Assessments**
>
> LifeLabs will conduct privacy impact assessments (PIAs) to demonstrate operational compliance and to identify privacy risks that an initiative, program or technology solution poses to PI/PHI that will be collected, used and/or disclosed through the initiative.
>
> A Preliminary Privacy Assessment will be conducted for all initiatives, programs or technology solutions governed by the project lifecycle process.
>
> All PIAs conducted by LifeLabs will include an inventory of the privacy risks identified as a result of the PIA.
>
> LifeLabs subsidiaries will conduct PIAs in accordance with their own privacy policies and procedures but privacy risks identified as a result of the PIA will be included in the inventory of identified risks.
>
> PIAs will not be conducted where existing programs or systems are changed, or new programs or systems are implemented, but no PI/PHI is involved.

[89] It is unclear whether the data repositories or systems impacted in this breach were reviewed in a manner compliant with its Privacy Assurance and Risk Framework. For example, it is unclear if the policy would have applied to the Patient Wait Time (PWT) system impacted in the breach as it was "acquired from a third party" and could be characterized as an "existing program[] or system[]" pursuant to the above citation.

[90] In my view, in balancing the characterization of the policies as "draft", with the claim that such policies are "representative of the … safeguards employed by LifeLabs", it would be reasonable to expect substantial compliance with the policies and practices as written, including the subsections that describe policy compliance.

[91] Such practices are part of reasonable security arrangements to protect the privacy and security of data under the custody or control, an obligation under section 34 of the Act.

[92] LifeLabs did not meet its obligations under section 6(1) of the Act to both develop and follow policies and practices that are reasonable to meet its obligations under section 34. It is unclear which security policies and practices were consistently followed at the time of the incident.

[93] I recommend LifeLabs formally adopt its draft policies and practices, and develop a process to ensure compliance with its privacy and security policies and practices that are in force.

Retention and Disposition of Information

[94] Policies and practices for the retention and disposition of personal information are important because they provide organizations with rules on when and how information stored by

organizations can safely be destroyed. In the incident reported by LifeLabs, the personal information at issue was stored electronically on two databases that were no longer in use by LifeLabs.

[95] Acknowledging the importance of appropriate records management and disposition, section 35 of PIPA requires organizations to only retain personal information for as long as reasonably required for legal or business purposes:

> **Retention and destruction of information**
>
> 35(1) An organization may retain personal information only for as long as the organization reasonably requires the personal information for legal or business purposes.
>
> (2) Within a reasonable period of time after an organization no longer reasonably requires personal information for legal or business purposes, the organization must
>
> (a) destroy the records containing the personal information, or
>
> (b) render the personal information non-identifying so that it can no longer be used to identify an individual.

[96] In its responses to me, LifeLabs provided a number of "formally adopted" policies regarding information retention practices. LifeLabs also provided several draft policies, which are characterized as "representative of information security safeguards" employed by LifeLabs at the time of the incident. Specific references included:

- IT Security Policy – Data Security (not formally adopted) (Draft, AB2-9) states:

> **4.4 Data Storage**
>
> Data must only be stored for the set limit of time required by LifeLabs policy
>
> Archived data must be stored off site, away from a production environment
>
> **4.5 Data Disposal**
>
> Access control mechanisms must be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights during the disposal process
>
> The Information Security team must develop and implement procedures to ensure the proper disposal of various types of data

- Master Privacy Policy 2019 (Adopted, AB2-27) states:

> Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.
>
> …
>
> (e) LifeLabs will destroy, erase, or make anonymous PI/PHI that is no longer permitted or required to be retained. LifeLabs will maintain policies and implement procedures and procedures to govern such destruction, erasure and anonymization of PI/PHI.

- Document Retention Policy – Ontario states (Adopted, AB2-49; policy for Alberta was not provided):

> Records are stored in a suitable environment to prevent loss, unauthorized access, damage or deterioration due to temperature, water or fire.
>
> Records that contain patient information are stored in an appropriate secure location to protect privacy and personal information.
>
> In order to protect confidential information, records that become eligible for destruction are appropriately destroyed by shredding or secure electronic deletion[.]
>
> Management ensures that records are stored appropriately and destroyed in compliance with the retention times noted in the charts attached.

- Record Management Process – BC states (Adopted, AB2-50; policy for Alberta was not provided):

> Records will be:
>
> retained … in accordance with legislation, regulatory, licensing and accreditation requirements
>
> destroyed … as specified in the Record Retention Schedule … by … secure electronic deletion to protect confidential information

[97] The compromised data set containing personal information collected in Alberta was characterized by LifeLabs as "decommissioned" or "stale." LifeLabs explained on June 17, 2020:

> "the only 'live' data returned was from the Patient Wait Time environment. The other three data sets returned from the perpetrator were out of date, incomplete and/or related to **decommissioned systems**. This suggests that those three data sets were extracted from **stale working files** contained within the LifeLabs system, rather than from an active database, data server or live production environment." [emphasis added]

[98] I asked LifeLabs to explain why the referenced stale data set was available, in apparent conflict with its retention policies, draft and adopted, as described above as well as its June 17, 2020 response which stated that databases with patient information are encrypted.

[99] LifeLabs initially did not provide clarification on why the referenced data set, described as "decommissioned" and "stale", was available on its network, remained individually identifiable, and provided no explanation regarding whether or not the data set ought to have been destroyed, in accordance with its adopted retention policies.

[100] On July 29, 2020, LifeLabs reiterated:

> As indicated in our response letter of June 17, 2020, the draft information security safeguards policies that were set out in Exhibits AB2-8 to AB2-18 (including AB2-10 IT Security Policy – Vulnerability Management) were not final or formally approved at the time of the incident. Accordingly, LifeLabs could not logically have "followed" policies that were not yet in place.

[101] On April 1, 2021, LifeLabs clarified that the stale data was "likely" retained after a data migration, and its retention appeared to be consistent with policies at that particular time. It

was not indicated to me which policy applied at that time nor was additional documentary evidence provided for review.

[102] I find that LifeLabs did not retain personal information only for as long as reasonably required for legal or business purposes, as required by section 35. As a result, it did not meet its obligations under section 34 to make reasonable security arrangements to protect against, for example, unauthorized access, use, disclosure or copying.

[103] I recommend that LifeLabs complete a thorough review of all personal information maintained by the Organization to ensure compliance with its records retention and disposition policies.

Technical Safeguards

[104] Technical safeguards are the technology in place to protect the personal information collected, used and disclosed by an organization. The hardware and software within an organization must be properly secured from unauthorized access, viruses, and system failure. As implied above, the administrative safeguards set the framework for the implementation of the technical safeguards. The two safeguards work hand in hand to protect an organization's technical infrastructure and the personal information therein.

[105] As stated, LifeLabs described the incident in its breach report to this office as:

> Through the proactive surveillance of our IT systems, LifeLabs identified a cyber-attack involving unauthorized access to some of our computer systems. Immediately upon discovering the incident we engaged world-class cybersecurity experts to isolate and secure the affected systems, and determine the scope of the breach.

[106] LifeLabs provided its Information Security Acceptable Use (Adopted, AB2-7) policy document for my review and, in its responses, briefly listed a number of more specific technical safeguards in place prior to the breach. These include:

> conducting vulnerability scans and external penetration tests
>
> encrypting databases with patient data
>
> upgrading email security software
>
> implementing User Based Analytics to prevent against unauthorized access to patient data by staff
>
> retaining [3rd party] to support Incident Response
>
> launching network tools to detect attacks

[107] In order to determine whether LifeLabs met its obligations with respect to the development and management of its technical safeguards under the Act, I reviewed its administrative policies and compared them to the relevant technical safeguards in place at the time of the incident.

Encryption

[108] Encryption an important technical safeguard for personal information both in transit and at rest. I reviewed LifeLabs responses and policies, and note the following with respect to its consideration and use of encryption as a safeguard:

- LifeLabs indicated they have policies entitled "Encryption Policy" and "Encryption Security". However, these policies were not provided to me for my review, citing that they are still in draft.
- The LifeLabs' "Master Privacy Policy" references the use of encryption as a method of protecting personal information.
- Draft policy entitled "IT Security Policy – Data Security", section 4.4 Data Storage prescribes the use of cryptography (secure communications) in accordance with its encryption policies.
- LifeLabs also indicated to me in written responses to my questions dated June 17, 2020, that the practice of "encrypting databases with patient data" was in place "prior to the incident".

[109] Despite the technical safeguards mentioned above, LifeLabs advised in its July 29, 2020 responses that "[t]he 'Patient Wait Time System' servers and databases were not encrypted at the time of the breach". These were the two servers affected by the breach incident reported to this office. It is also unclear whether the other compromised data sets were encrypted at the time of the incident, in particular, a "stale" data set from a "decommissioned system[]" that is referred to elsewhere in this analysis.

[110] I recommend that LifeLabs implement the technical components contained in its draft and adopted policies, and that LifeLabs encrypt data.

Patch Management

[111] Administering regular patch management is a key security control for an organization. Patch management, or regularly applying updates to software to correct vulnerabilities, errors or bugs with the system is an important practice to be completed regularly to protect an organizations infrastructure from exploitation such as hacking or ransomware. LifeLabs provided the following policies with respect to this technical safeguard:

- LifeLabs' policy on "Information Security Acceptable Use" (AB2-7) refers to update management and compliance. The policy includes a requirement to "not disable these automatic updates by any means"
- Draft policy "IT Security Policy - Patch Management" (AB2-11) provided an overview of a patch and update management practice, including provisions for documented, approved exceptions.

[112] However, LifeLabs, in its July 29, 2020 responses indicated to me that "critical and high [sic] vulnerabilities of external facing systems and critical infrastructure" were patched as part of its "response to the incident", and "as part of its ongoing efforts to align its practices with the

target state set out in draft policy document AB2-11 [IT Security Policy – Patch Management]". This leads me to believe that that patch management policies may not have been followed.

[113] I requested clarification on the apparent inconsistency between the patch management policy and the incident response action of patching "critical and high vulnerabilities", in its post-breach remediation. I also requested that LifeLabs provide a report on any risk mitigation alternatives to patching that were in place if patching exceptions were active. In response, LifeLabs again cited that the referenced policy on patch management is in draft and that practices in AB2-11 IT Security Policy – Patch Management are "target state".

[114] While it is impractical to expect every critical and high impact vulnerability to be patched, as not all are known to an organization, I observe that critical patching was completed after the incident, and that LifeLabs did not provide compliance records or risk mitigation actions to compensate for unpatched vulnerabilities, even though I requested this information.

[115] I recommend that LifeLabs formally adopt and follow best practices for patch management.

Conclusion

[116] In general, having "draft" IT Security policies (almost all of which reference technical safeguards) that were not followed as they were not "formally approved", despite being "representative" of practices at the time of the breach, demonstrates a failure to adequately safeguard. Because of these unresolved issues with administrative and technical safeguards discussed above, I find that LifeLabs did not protect personal information that is in its custody or under its control by making reasonable security arrangements in accordance with section 34 of the *Personal Information Protection Act*.

Summary of Findings

[117] LifeLabs did not meet its obligations under section 6(1) of the Act to both develop and follow policies and practices that are reasonable to meet its obligations under section 34. It is unclear which security policies and practices were followed at the time of the incident, nor was it clear whether policies and practices were consistently followed.

[118] LifeLabs did not retain personal information only for as long as reasonably required for legal or business purposes, as required by section 35. As a result, it did not meet its obligations under section 34 to make reasonable security arrangements to protect against, unauthorized access, use, disclosure or copying.

[119] LifeLabs did not protect personal information that is in its custody or under its control by making reasonable security arrangements in accordance with section 34 of the *Personal Information Protection Act.*

Summary of Recommendations

[120] I recommend that LifeLabs:

- create Alberta-specific policies and practices as appropriate in accordance with PIPA.
- formally adopt its draft policies and practices, and develop a process to ensure compliance with its privacy and security policies and practices that are in force.
- complete a thorough review of all personal information maintained by the Organization to ensure compliance with its records retention and disposition policies.
- implement the technical components contained in its draft and adopted policies, and encrypt data.
- formally adopt and follow best practices for patch management.

LifeLabs' Response to Recommendations

[121] In its April 1, 2021 letter, LifeLabs agreed to implement, or had already implemented during the course of the investigation, the following recommendations:

- "LifeLabs agrees that organizations should be aware of all applicable privacy laws and take them into account in their privacy policies by ensuring that relevant policies and processes adopt a uniform "highest standard" approach to compliance."
    - "LifeLabs will implement a unified set of national policies and practices that are based on the "highest standard" principle, ensuring compliance with all applicable privacy laws including the Alberta PIPA."
- LifeLabs agrees with the OIPC recommendation to "formally adopt its draft policies and practices, and develop a process to ensure compliance with its privacy and security policies and practices that are in force."
    - LifeLabs has "completed its review of the draft information security policies … [and adopted] policies that are aligned to current best industry practice and recognized international information security standards."
- LifeLabs agrees with the OIPC recommendation to review all personal information maintained by the Organization to ensure compliance with its records retention and disposition policies. The review is in progress.
- LifeLabs agrees to encrypt data in accordance with its adopted encryption policy. Further, LifeLabs is encrypting data in consultation with external consultants.
    - LifeLabs further commits "to ensuring that it is encrypting more and more data elements going forward."

- LifeLabs "agrees to implement technical components … in its adopted policies, but considers that it should not be formally required to comply with draft policies."
    - "LifeLabs has now formally adopted final versions of the suite of draft IT security policies that had previously been provided to the Alberta OIPC) [sic]."
- LifeLabs agrees with the OIPC recommendation to formally adopt and follow best practices for patch management.
    - LifeLabs "recognizes the need to apply security patches in a timely manner as identified in the then-draft policy document" and "has since formally adopted a patch management standard."

Closing Comments

[122] I would like to thank Lifelabs for their cooperation throughout the investigation. I would also like to recognize their work to address the recommendations made in this report.

[123] It is important for organizations to recognize the sometimes unique jurisdictional requirements within each province across Canada. Organizations should ensure their policies and procedures reflect these differences be formally approved, and followed by the organization.

Rachel Hayward
Director, Compliance and Special Investigations