Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT
398-2019, 399-2019, 417-2019, 005-2020, 019-2020, 021-2020

LifeLabs LP
Saskatchewan Health Authority

June 9, 2020

Summary: In October 2019, LifeLabs LP (LifeLabs) discovered a cyberattack which resulted in the unauthorized disclosure of personal health information of 93,647 Saskatchewan residents. The Commissioner found that the Saskatchewan Health Authority (the SHA) had control of the majority of the personal health information at the time of the attack. Because LifeLabs cannot authenticate the identities of certain individuals, the Commissioner was not satisfied with the notification efforts of LifeLabs and the SHA. He also found that, because a fulsome, detailed report was not provided, LifeLabs did not demonstrate that it fully investigated the breach or adopted appropriate preventative measures. He also commented on various areas where LifeLabs was not compliant with HIPA. The Commissioner made several recommendations, including that the SHA conduct an audit of LifeLabs' response to the breach.

I BACKGROUND

[1] On December 13, 2019, LifeLabs LP (LifeLabs) proactively reported a privacy breach to my office. It indicated that, in October 2019, a proactive surveillance of its information technology (IT) systems identified a cyber-incident involving unauthorized access to the company's servers. At the time, LifeLabs reported that this cyberattack affected approximately 93,390 individuals in Saskatchewan. It also reported that individuals in British Columbia, Ontario and other provinces and territories were also affected. LifeLabs later confirmed that approximately 93,647 Saskatchewan residents were affected.

[2] The Saskatchewan Health Authority (SHA) is the largest trustee in our province. It is also one trustee that contracts with LifeLabs. LifeLabs provides collection and logistic services to the SHA. In other words, LifeLabs collects specimens from individuals and transports them to an SHA facility where testing is carried out.

[3] On December 20, 2019, my office notified both the SHA and LifeLabs that I would be investigating the matter.

[4] Since December 20, 2019, four affected individuals have made formal complaints to my office, resulting in my office opening four additional files.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances and do I have jurisdiction?

[5] *The Health Information Protection Act* (HIPA) applies in full when three elements are present. The first element is personal health information, the second element is a trustee, and the third element is if the personal health information is in the custody or control of the trustee.

Is there personal health information?

[6] Personal health information is defined in subsection 2(m) of HIPA which provides:

> **2** In this Act:
>
> …
>
> (m) "personal health information" means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;

> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or
>
> (B) incidentally to the provision of health services to the individual; or
>
> (v) registration information;

[7] Further, subsection 2(q) of HIPA defines registration information as follows:

> **2** In this Act:
>
> …
>
> (q) "registration information" means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;

[8] When LifeLabs originally reported the breach to my office in December, it estimated that 93,390 Saskatchewan residents were effected. In its response to the breach that it provided to my office at the end of January, LifeLabs reported that 95,855 Saskatchewan residents were affected by the breach and were "mainly" from the patient wait time system. On March 3, 2020, my office asked for more details about the information that was affected outside of the patient wait time system. It responded that the information outside of the patient wait time system was collected to provide lab testing services for Saskatchewan residents either travelling through British Columbia or Ontario or for services purchased privately from LifeLabs. It indicated that 241 individuals from Saskatchewan were affected by the breach outside of the patient wait time system.

[9] On May 27, 2020, at the end of my investigation, LifeLabs requested that my office "consider the new granular facts relating to" the affected systems. It had not previously provided information about these systems in a Saskatchewan context.

[10] LifeLabs indicated that the personal health information of 93,390 Saskatchewan residents affected by the cyberattack were related to its patient wait time system. The patient wait time system refers to the system where individuals can book appointments online. The data elements involved include name, email address, password and security questions and answers. Four months after providing its initial response to my office, LifeLabs indicated that telephone numbers, Internet Protocol addresses (IP addresses) and various information about login attempts were also affected by the breach. Prior to this, LifeLabs did not report all of the data elements in a clear manner in its response to my office.

[11] Additionally, LifeLabs initially indicated that the cyberattack also resulted in the unauthorized disclosure of names, sex, phone numbers, addresses, email addresses, birth dates, user identifications, passwords, security questions and answers, health card numbers, and results of laboratory testing of 241 Saskatchewan residents. As noted, LifeLabs reported that these individuals received services while in British Columbia or Ontario or received private services from LifeLabs.

[12] After May 27, 2020, LifeLabs again provided more specific information about data elements and systems affected. It indicated that one of the affected systems that related to services performed in Ontario contained no test orders or results for Saskatchewan residents. However, at this late stage in my investigation, LifeLabs reported that the demographic information of 15 Saskatchewan residents in this system was affected by the breach. This includes name, date of birth, “patient sex”, address and health card number. It did not provide specific information as to why it collected only demographic information of the 15 Saskatchewan residents in this system.

[13] On May 27, 2020, LifeLabs also noted that the information of 242 Saskatchewan residents that was stored in a system related to services provided in British Columbia was also affected by the breach. Data elements involved included name, date of birth, “patient sex”, address, telephone number, health provider name and health card number.

[14] The affected individuals used LifeLabs’ patient wait time system to arrange an appointment with LifeLabs so that LifeLabs could provide a health care service on behalf of the SHA.

This included name, email address, telephone numbers, passwords and security questions and answers. This qualifies as registration information pursuant to subsection 2(q) of HIPA as they were collected for the purpose of registering individuals for the provision of health services. Further in Review Report 186-2019, Review Report LA-2013-003, my office has indicated that IP addresses can be considered personal information if it can be associated with an identifiable individual. In this case, it appears that the IP addresses and various other login information from the patient wait time system that was affected by the breach can also be considered registration information as it is part of the information collected by LifeLabs to register these affected individuals for health services that they provided on behalf of the SHA pursuant to subsection 2(q) of HIPA.

[15] Similar data elements affected in the other systems, including names, email addresses, sex, telephone numbers, addresses, birthdates and health card numbers also qualify as registration information pursuant to 2(q) of HIPA. Therefore, these elements qualify as personal health information pursuant to subsection 2(m)(v) of HIPA.

[16] Lab results are information with respect to the physical health of an individual and information with respect to a health service provided to an individual. As such, it qualifies as personal health information pursuant to subsections 2(m)(i), (ii) and (iii) of HIPA. However, at the end of my investigation, LifeLabs indicated that the lab results affected in this breach did not relate to Saskatchewan residents, contrary to what had been reported to my office earlier.

Are there trustees?

[17] Subsection 2(t) of HIPA defines trustee. In part, it provides:

> **2** In this Act:
>
> …
>
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> …

> (ii) the provincial health authority or a health care organization;
> …
>
> (viii) a licensee as defined in *The Medical Laboratory Licensing Act, 1994*;

[18] The SHA qualifies as a trustee pursuant to subsection 2(t)(ii) of HIPA.

[19] Subsection 2(e) of *The Medical Laboratory Licencing Act, 1994* (the Licencing Act) provides:

> **2** In this Act:
> …
>
> (d) "licence" means a valid licence granted pursuant to section 6;

[20] Section 6 of the Licencing Act provides:

> **6**(1) The director shall:
>
> (a) consider each application received pursuant to section 5, including any information or materials requested by the director; and
>
> (b) consider the standards of the accreditation program for the medical laboratory that is the subject of the application.
>
> (2) The director shall:
>
> (a) grant the licence if the director is satisfied that:
>
> (i) there is a need, based on factors set out in the regulations, for the medical laboratory that is the subject of the application and for the tests that are to be performed in that laboratory;
>
> (ii) the medical laboratory that is the subject of the application will be operated in compliance with this Act, the regulations and any terms and conditions contained in the licence; and
>
> (iii) granting a licence to the applicant would not be contrary to the public interest; or
>
> (b) refuse to grant a licence.
>
> (3) The director shall notify the applicant in writing of his or her decision.

> (4) The director may include as provisions of a licence any terms or conditions that the director considers appropriate, including, without limiting the generality of the foregoing, any terms or conditions that constitute standards of the accreditation program.

[21] Saskatchewan's Ministry of Health (the Ministry) provided my office with copies of 10 medical laboratory licences where LifeLabs is the licensee for various locations in Regina and Saskatoon. The licences were in effect from October 1, 2019 to March 31, 2020.

[22] As such, LifeLabs qualifies as a trustee pursuant to subsection 2(t)(viii) of HIPA.

Which trustee has custody or control of the personal health information?

[23] Finally, I must consider whether the SHA or LifeLabs has custody or control of the personal health information identified above.

[24] In Investigation Report 255-2017, 256-2017 and Investigation Report 021-2017, 067-2017 & 068-2017 my office defined "custody" and "control".

[25] Custody is the physical possession of a record by a trustee, who has a measure of control.

[26] Control connotes authority. A record is under the control of a trustee when the trustee has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement.

[27] All of the personal health information in question was stored in servers located in Ontario that belonged to LifeLabs when the cyberattack occurred. Therefore, LifeLabs had physical possession of all of the personal health information in question. To find that it has custody of the information in question, I must also find that it has a measure of control.

[28] With respect to the personal health information in the patient wait time system, the SHA and LifeLabs initially expressed conflicting views about which party has control of this personal health information.

[29] On April 13, 2020, LifeLabs indicated that it does not collect personal health information for individuals it serves through the collections agreement with the SHA. It reported that all personal health information that it processes as part of the contract is entered into a system directed by the SHA. My understanding is that LifeLabs is asserting that it has control over the personal health information in the patient wait time system because it is not mentioned in the agreement.

[30] The SHA has provided my office with the *Agreement for the Provision of Community Laboratory Services between Saskatchewan Health Authority and LifeLabs LP* (the SHA Agreement). I believe the systems that LifeLabs is referring to, which are mentioned in the SHA Agreement are the Health Region Hospital Information System (HIS) and the Laboratory Information System (LIS). These systems have not been affected by the breach.

[31] In its investigation report, the SHA stated that it has control of the personal health information entered into the on-line "check in" services.

[32] Neither party provided a further analysis of their positions when responding to my office's request for their investigation reports.

[33] The SHA Agreement does not specifically address the patient wait time system or the personal health information in the patient wait time system.

[34] The SHA Agreement suggests that the personal health information in LifeLabs' patient wait time system would be captured. Clause 8.2 of the SHA Agreement provides as follows:

> **8.0 PROPERTY RIGHTS**
>
> …
>
> 8.2 Data: All data, files, records and other information related to the business of [the SHA] and all documents containing any such data, records and other information related to the business of [the SHA] whether initiated, originated or manipulated by [the SHA] or [LifeLabs] shall be the exclusive property of [the SHA] and shall be delivered to [the SHA] by [LifeLabs] upon request of [the SHA] not more often than

> once per annum or upon termination or expiration of this Agreement. It is understood however, that [LifeLabs] will not disclose its other business records or any financial information associated with [LifeLabs'] costs or profit.

[35] This is a broad statement that can capture a wide variety of information. I also note the following clause found in *Appendix E Data Protection* (Appendix E) in the SHA Agreement:

> 3. Control of and Rights in [personal health information]
>
> Control of [personal health information] shall at all times remain with [the SHA] [LifeLabs] acknowledges and agrees that nothing gives [LifeLabs] any right, title, interest in any [personal health information].

[36] As clause 3 of Appendix E of the SHA Agreement has determined that the SHA has control over personal health information, I find that the SHA is the trustee of the personal health information related to the SHA in LifeLabs' patient wait time system.

[37] As the SHA is the trustee of the personal health information in question in LifeLabs' patient wait time system, I will consider if LifeLabs would qualify as an information management provider (IMSP). An IMSP is defined by subsection 2(j) of HIPA, as follows:

> **2** In this Act:
>
> …
>
> (j) "information management service provider" means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf;

[38] Section 18 of HIPA provides:

> **18**(1) A trustee may provide personal health information to an information management service provider:
>
> (a) for the purpose of having the information management service provider process, store, archive or destroy the personal health information for the trustee;

> (b) to enable the information management service provider to provide the trustee with information management or information technology services;
>
> (c) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee; or
>
> (d) for the purpose of combining records containing personal health information.
>
> (2) **Not yet proclaimed.**
>
> (3) An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).
>
> (4) **Not yet proclaimed.**
>
> (5) If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.

[39] The personal health information was provided to LifeLabs directly by affected individuals by virtue of the fact LifeLabs was providing health services on behalf of the SHA. Because the SHA has control of the personal health information, LifeLabs was a trustee that had the role of an IMSP for the personal health information in the patient wait time system.

[40] At the end of my investigation, the SHA indicated that it no longer believed that it had control of the personal health information in the patient wait time system because it is not specifically mentioned in the SHA Agreement. LifeLabs also expressed this opinion. I am not persuaded. Affected individuals used LifeLabs' patient wait time system to arrange an appointment with LifeLabs so that LifeLabs could provide a health care service on behalf of the SHA. Clause 8.2 of the SHA agreement is broad enough to capture the personal information in the patient wait time system and clause 3 of Appendix E of the SHA agreement indicates that the SHA has control of personal health information. The SHA is the trustee of the personal health information in the patient wait time system.

[41] If LifeLabs and the SHA proceed on the basis that LifeLabs is the trustee of the personal health information, it increases LifeLabs' responsibility for the personal health information. As I will discuss later in this Report, the SHA must make sure that it is satisfied with LifeLabs' response to this breach. Going forward, I recommend that the SHA and LifeLabs specifically address this matter in the SHA agreement and communicate it clearly to the citizens of Saskatchewan.

[42] It is my understanding that LifeLabs has custody or control of the personal health information that is discussed above, but not in the patient wait time system. At the end of my investigation, LifeLabs indicated that privacy legislation in other provinces apply to this personal health information. My role is to interpret HIPA and determine where it applies. As I have found the information in the other systems qualifies as personal health information and that LifeLabs qualifies as a trustee, the only other criteria to determine if HIPA applies to the information in the other systems is whether LifeLabs has custody or control of this personal health information. LifeLabs has indicated that it has physical custody of the records as they reside in LifeLabs' electronic systems. LifeLabs has not provided enough detail to persuade me that other organizations have control of this information or what organization those would be. As such, I conclude that LifeLabs has custody and that HIPA applies to this personal health information.

2. Was there a breach of privacy?

[43] A privacy breach occurs when personal health information is collected, used, and/or disclosed without authority under HIPA. Privacy breaches can also occur when personal health information is not appropriately safeguarded, or collected or used in a way that is not accurate nor complete.

[44] A disclosure is the exposure of personal health information to a separate entity, not a division or branch of the trustee in custody or control of that information.

[45] LifeLabs reported that on October 28, 2019, an unknown source had triggered a monitoring system. In response to the alert, the LifeLabs Security team validated internally that the

event was anomalous and not performed with authorization, and instructed a third party contractor CrowdStrike to put those systems into containment for further investigation. With assistance from CrowdStrike, it was confirmed that suspicious activity was detected in two LifeLabs webservers and two LifeLabs database servers.

[46] On October 31, 2019, LifeLabs received a direct communication from the cyberattacker. The cyberattacker claimed to have data from LifeLabs' servers. The cyberattacker demanded payment in exchange for return of the data. LifeLabs, CrowdStrike and Cytelligence arranged for the return of LifeLabs data, and tried to determine, to the extent possible, how the cyberattacker obtained the data.

[47] Because the personal health information in question was exposed to the cyberattacker, a separate entity, the event qualifies as a disclosure of personal health information.

[48] Subsection 27(1) of HIPA provides:

> **27**(1) A trustee shall not disclose personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section, section 28 or section 29.

[49] The SHA Agreement states:

> 6. Disclosure to Third Parties
>
> Except as specifically permitted by the Agreement (including, without limitation, pursuant to Section 7 of this Appendix below), [LifeLabs] shall not disclose (and will not allow any of its employees, agents or representatives to disclose) in any manner whatsoever any [personal health information] to any third party without the prior written consent of [the SHA] and [LifeLabs] hereby acknowledges that such consent will only be provided if: (a) such disclosure is required in order for [LifeLabs] to perform its service obligations pursuant to the Agreement; (b) such disclosure is permitted under HIPA, LA FOIP or other applicable laws; (c) the third party agrees, in writing, to protect the confidentiality and security of the [personal health information] to at least the extent provided by this Appendix; and (d) [the SHA] is otherwise satisfied, in its discretion, with the status, quality and reputation of the third party.

[50] The SHA and LifeLabs have not informed me that the disclosure was in accordance with the SHA Agreement and HIPA.

[51] I find, then, that the access by the cyberattacker to the personal health information in question was an unauthorized disclosure of personal health information. I find that the disclosure constitutes both a breach of HIPA and of the SHA Agreement.

[52] I will discuss other potential breaches as I review LifeLabs' and the SHA's responses to this breach.

3. Did the SHA and LifeLabs respond to this privacy breach appropriately?

[53] My office suggests that trustees undertake the following five steps when responding to a privacy breach:

- contain the breach;
- notification;
- investigate the privacy breach;
- prevent future privacy breaches; and
- write an investigation report.

[54] Below is an analysis of each of these steps.

Contain the breach

[55] To contain the privacy breach is to ensure that the personal health information is no longer at risk. This may include recovering the record(s), revoking access to personal health information, and/or stopping the unauthorized practice.

[56] LifeLabs indicated that, immediately upon discovering the cyberattack, it engaged with multiple "world-class" cyber security firms to isolate and secure the affected systems and determine the scope of the breach. This included engaging CrowdStrike to apply additional security controls to all servers and systems compatible with available software to protect against further compromise.

[57] The SHA reported that, on October 31, 2019, it was informed by LifeLabs that there was a temporary disruption to the on-line services hosted by the servers in question between

October 28, 2019 and November 5, 2019. As a result, the "SaveMySpot" patient wait time application did not work. This reflects the steps LifeLabs reported it did in isolating and securing the affected systems. The SHA reported that these services were restored on November 5, 2019. LifeLabs did not inform the SHA that the cyberattack was the reason for the disruption in these services until mid-November.

[58] LifeLabs reported that it has "drawn on world-class cybersecurity experts" to conduct an investigation, in order to secure its systems. The investigation began the day the breach was detected. In consultation with these firms, LifeLabs paid to verify the claims of the cyberattacker and retrieve personal health information.

[59] I also note that this is a description of the steps that LifeLabs took to contain the breach after it was discovered. However, LifeLabs also asserted that the cyberattack had been occurring undetected sporadically for almost a year before it was discovered.

[60] I am satisfied that LifeLabs made adequate efforts to contain the breach, although it did not occur for almost a year after it began. The majority of the containment efforts occurred before the SHA was informed of the breach.

Notification

[61] The following is a list of individuals or organizations that may need to be notified in the event of a privacy breach:

- Proactively report the breach to my office;
- If criminal activity is suspected, contact police; and/or
- Contact the affected individuals unless there are compelling reasons why this should not occur.

a. Notification to the SHA

[62] LifeLabs notified the SHA of the breach on October 31, 2019, by indicating that its patient wait time system was not functioning. The SHA reported that it was informed by LifeLabs about the breach in mid-November.

b. Notification to the police

[63] LifeLabs reported that, on November 21, 2019, it reported the cyberattack to the Royal Canadian Mounted Police. It also reported the cyberattack to the Ontario Provincial Police and Toronto Police Service's Cyber Division. LifeLabs informed my office that the Toronto Police Service has jurisdiction in this matter and is continuing to investigate with respect to the criminal activity.

c. Notification to my office

[64] As noted, LifeLabs reported the breach to my office on December 13, 2019. This was more than a month after it discovered the breach.

d. Notification to Affected Individuals

[65] Notifying the affected individuals of the privacy breach is important so that they can determine how they have been impacted and take steps to protect themselves. A notification should include the following:

- a description of what happened;

- a detailed description of the personal information or personal health information that was involved;

- if known, a description of possible types of harm that may come to them as a result of the privacy breach;

- steps that the individuals can take to mitigate harm;

- steps the organization is taking to prevent similar privacy breaches in the future;
- the contact information of an individual within the organization who can answer questions and provide further information;
- a notice that individuals have a right to complain to the Office of the Information and Privacy Commissioner;
- the contact information of the Office of the Information and Privacy Commissioner; and
- where appropriate, recognition of the impacts of the breach on affected individuals and an apology.

[66] In its communication to my office, received on January 31, 2020, LifeLabs indicated that it notified all affected individuals through indirect notification, which was a public announcement on December 17, 2019. Further, individuals who may have had their laboratory test results compromised were notified directly.

[67] Several affected individuals reported to my office that they received emails from LifeLabs notifying them of the breach. I note that the notification emails that my office received from affected individuals state only that they might be affected by the breach. The notification emails do not confirm if the recipient of the email is an affected individual or specifically what data elements are involved. LifeLabs also noted that the email served as a precautionary password reset. The password reset was only sent out six weeks after the breach was discovered.

[68] After LifeLabs notified affected individuals of the breach, four affected individuals contacted my office to formally launch a complaint. Three of these Complainants had unique concerns about the breach.

Complainant #1

[69] Complainant #1 sought confirmation from LifeLabs that they were affected by the breach. Additionally, they wanted to know what specific data elements were breached. They emailed LifeLabs to find out and reported that they did not get a response. Complainant

#1 also noted that when they called the customer call centre, the individual who answered read from a script and could not provide additional, specific information.

[70] In response, LifeLabs indicated that the number that Complainant #1 called was set up to afford affected individuals the opportunity to obtain cyber security protection for one year. It explained that the call centre personnel were also provided with a script that permitted them to answer common questions about the cyberattack.

[71] However, LifeLabs also reported that, in the patient wait time system, it has not collected sufficient information about its customers to be able to reliably verify their identities or to contact them directly. In effect, LifeLabs has no way to reliably confirm to any individual that they were affected by the cyberattack or communicate what specific data elements were involved.

[72] I note that section 16 of HIPA provides:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[73] Subsection 16(a) requires that trustees protect the integrity of personal health information. In Investigation Report 024-2018, I indicated that, with respect to subsections 16(a) and (b)(i) of HIPA, integrity refers to the condition of information being whole or complete; not modified, deleted or corrupted. By not being able to verify the identity of individuals,

I conclude that the SHA and LifeLabs has not protected the integrity or accuracy of the personal health information in the patient wait time system pursuant to subsection 16(a) of HIPA.

[74] Further, sections 12 and 32 of HIPA provide individuals the right to access their personal health information as follows:

> **12** In accordance with Part V, an individual has the right to request access to personal health information about himself or herself that is contained in a record in the custody or control of a trustee.
>
> **32** Subject to this Part, on making a written request for access, an individual has the right to obtain access to personal health information about himself or herself that is contained in a record in the custody or control of a trustee.

[75] I also question the SHA and LifeLabs' ability to comply with Part V of HIPA which indicates how trustees must respond to individuals' rights to access their own personal health information.

[76] LifeLabs responded to this analysis by indicating that it has written policies and procedures that instructs employees on how to respond to access to information requests. It provided copies of those policies to my office. However, if LifeLabs is unable to authenticate the identity of users in its patient wait time system, I question how it would be able to respond to related access requests. LifeLabs also indicated that it followed the data minimization principle by not collecting too much information about individuals, resulting in its inability to authenticate the identity of individuals for the purpose of responding to access requests or verifying who is an affected individual in this breach.

[77] In Investigation Report F-2012-001, my office provided the following guidance:

> Identification and authentication are fundamentally about the management of risk:
>
> - The risk to the organization of, through bad authentication practice, either denying access to a legitimate customer or giving access to an impostor;
>
> - The risk to individuals that their personal information is lost or inappropriately disclosed, and that their identity, finances, and privacy are compromised.

> "Risk" should always be understood to have two aspects: the likelihood of an event occurring and the severity of the consequences if it does occur. Proper risk management requires that both these two aspects of risk are considered.
>
> The stringency of authentication processes should be commensurate with the risk to the information being protected, risk being a function of the sensitivity of the information or service in question, the vulnerability of and the perceived threat to that information or service.

[78] I am not persuaded that LifeLabs balanced these risks appropriately resulting in the inability to give true notification to individuals affected by this breach.

Complainant #2

[79] Complainant #2 reported to my office that they had difficulty registering for the cyber security protection services. They tried to contact the agency providing the services and was unable to resolve the issue. When Complainant #2 called LifeLabs, they indicated that they were told that several others had called in to register the same complaint and that LifeLabs employees were instructed to tell callers that it was the problem for the cyber security protection services company.

[80] LifeLabs responded that it has no information suggesting this is a widespread concern. However, upon learning of this situation from my office, LifeLabs has informed its service provider about the issue and asked it to ensure that other customers do not face the same issues.

Complainant #3

[81] Complainant #3 was concerned about the breach because they were notified about the breach twice by email at the same email address.

[82] In response, LifeLabs provided this reason why Complainant #3 may have been notified twice by email. It indicated that Complainant #3 might have been registered for both an online test results portal as well as the patient wait time system. It also postulated that

Complainant #3 may have received multiple emails because there were duplicate entries associated with their email address or addresses.

[83] However, both emails received by Complainant #3 reference the online patient wait time system and were received by the same email address. I question why LifeLabs has referred to the online results portal when they both refer to the online patient wait time system. LifeLabs' concluded that Complainant #3 would have received an email because they were registered for the online test results portal when LifeLabs also indicated that this system was not affected by the breach, but informed of the situation so that passwords could be reset.

Complainant #4

[84] Complainant # 4 was simply concerned about being notified that they may be an affected individual. They were also concerned that this cyberattack was linked to a cyberattack my office is investigating involving eHealth Saskatchewan. Complainant #4 referred to an "ehealth" portal in its notification email and wondered if it is related to eHealth Saskatchewan. LifeLabs indicated that its ehealth portal does not have anything to do with eHealth Saskatchewan. I see no links between the two breaches at this time.

[85] Overall, I do have concerns about the notification that LifeLabs provided to affected individuals. Although LifeLabs did take steps to notify affected individuals through the media and through direct communications, the notification that each individual received is not specific and is inconclusive because the emails only indicate that the recipient may have been affected by the breach. Further, in relation to the patient wait time system, LifeLabs is unable to confirm that any individual has been affected or exactly what data elements related to a specific individual has been compromised when asked.

[86] For the purpose of breach notification and responding to access requests, I recommend that LifeLabs update the patient wait time system so that it is able to authenticate the identity of individuals for which it has custody or control of personal health information.

[87] LifeLabs also indicated in its notification emails that it was providing cyber security protection services free of charge to all affected individuals for one year. This includes dark web monitoring and identity theft insurance.

[88] In Investigation Report 103-2017, I recommended that the trustee provide a minimum of five years of credit monitoring to affected individuals following a privacy breach. I recommend that LifeLabs and the SHA provide cyber security protection to affected individuals from Saskatchewan for a minimum of five years.

[89] Finally, I also note LifeLabs' communication to my office at the end of January and notification emails indicated that the risk to affected individuals was low. It made this assessment because it believes the risk of financial fraud and identity theft is low given the nature of the information compromised. LifeLabs also indicated the risk was low because it was the goal of the cyberattacker to receive ransom money in exchange for the information. LifeLabs' paid the cyberattacker and received the compromised data in return. I do not agree with LifeLabs' assessment. The data that was compromised included information related to the affected individuals' passwords, security questions and answers and IP addresses. This is the very information that individuals use to identify and protect themselves digitally. It is very sensitive information. Further, even though LifeLabs was able to retrieve the personal health information from the cyberattacker, it is unable to guarantee that the attacker has not retained copies of the data and will use or disclose it in other ways.

[90] I am not satisfied with LifeLabs' efforts to notify affected individuals as I have a number of concerns.

e. Notification efforts of the SHA

[91] The SHA reported that it had an opportunity to review LifeLabs' draft public announcement before it was released on December 17, 2019. It took no other steps. I am not persuaded that the SHA took enough steps to ensure that affected individuals were notified of the breach.

Investigate the privacy breach

[92] Investigating the privacy breach to identify the root cause is key to understanding what happened and to prevent similar privacy breaches in the future.

[93] On January 31, 2020, LifeLabs reported that it had not finished its investigation when my office asked that it provide its report to my office. On March 25, 2020, it told the SHA that it had not completed its investigation. I note that five months after the discovery of the breach, Life Labs had not completed its investigation of the breach. During that time, it did not provide information about why the investigation was not complete, what challenges it was facing or what was left to complete. On April 13, 2020, LifeLabs indicated that it was finished its investigation, but did not offer any further information about its findings at that time.

[94] I am aware of critical incident reports that have been produced for LifeLabs by CrowdStrike as well as any other reports generated by other contracted IT firms. When my office notified LifeLabs of my investigation on December 20, 2019, LifeLabs was asked to provide copies of these reports to my office for the purpose of my investigation. LifeLabs declined to do so on January 31, 2020. My office asked for these reports again near the end of my investigation. On May 11, 2020, LifeLabs, again, informed my office it would not provide the reports.

[95] During my investigations, I expect a fulsome report from trustees that provides granular details about the trustee’s investigation. My office’s resource entitled *Privacy Breach Guidelines for Trustees* outlines the information required by my office in such a report. The information required includes how the breach occurred, what personal health information was affected, what safeguards were in place at the time of the breach, what the root cause of the breach was and what measures the trustee has or intends to take to prevent future breaches. My office requested that LifeLabs provide an internal investigation report by January 31, 2020. As detailed throughout this report, LifeLabs did not provide a report that was in line with the guidance provided. I was not able to ascertain if the reports that LifeLabs refused to provide to my office covered these elements.

[96] Given the circumstances, the SHA must rely on information from LifeLabs in order to complete its investigation.

a. *Policies and procedures*

[97] It is standard for my office to ask trustees and IMSPs for relevant written policies and procedures during our investigation. Throughout my investigation, LifeLabs provided my office with various privacy and IT security policies.

[98] LifeLabs provided my office with eleven policy documents related to IT security. Each one indicates an effective date in January 2019. Later in my investigation, my office learned that the policies provided by LifeLabs are, indeed, in draft form and were never signed and brought in to effect. I cannot accept that draft policies provide LifeLabs' employees with enough guidance to protect personal health information. Having written and approved privacy and security policies and procedures in place is one of the most fundamental safeguards that a trustee should have in place. LifeLabs indicated "technical policies" were implemented as a result of environmental controls built into the security systems at LifeLabs. It explained that in a control system there are technical policies that enforce the actual policy itself from a technology perspective. However, again, there was no actual written policy. This is not in alignment with subsection 16(c) of HIPA.

[99] LifeLabs also provided several policies related to privacy. Clause 15 of Appendix E of the SHA Agreement states that LifeLabs "must have in place, privacy breach management protocols that have been approved by [the SHA] in accordance with the Governance Process in Schedule G." My office specifically asked LifeLabs to provide us with a copy of the protocol. It provided the *Privacy Breach Management Policy* (breach protocol) on March 16, 2020.

[100] LifeLabs' breach protocol had a "release date" of "January 2019". This is similar to the draft IT security policies provided by LifeLabs that indicate an "effective" date also in January 2019, but were not actually in effect. My office asked LifeLabs if its breach protocol also was in draft form. On April 13, 2020, LifeLabs indicated that the breach

protocol was not in draft form. The manner in which LifeLabs indicates which policies are actually in effect is not clear to my office. I question LifeLabs' ability to successfully communicate this to its employees.

[101] My office also requested that the SHA provide a copy of LifeLabs' breach protocol to my office. My office also asked the SHA to confirm that LifeLabs submitted its breach protocol for approval as required by the SHA Agreement. On March 25, 2020, the SHA provided my office with a copy of LifeLabs' breach protocol that it received from LifeLabs on March 25, 2020. The SHA confirmed that it did not previously approve LifeLabs' privacy breach protocol as required by the SHA Agreement. Therefore, what LifeLabs provided to my office was not a final approved protocol.

[102] As LifeLabs did not have key written and approved privacy and security policies in place, and could not have ensured that its employees were acting in compliance with HIPA, I find that LifeLabs was not in compliance with subsection 16(c) of HIPA. This in itself constitutes a breach of privacy.

[103] This is also a requirement of subsection 23(2) of HIPA which provides:

> **23**(2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.

[104] I also note that the SHA Agreement states:

> 12. Security and Segregation of [Personal Health Information]
>
> [LifeLabs] shall have in place reasonable policies, procedures and safeguards to protect the confidentiality and security of [personal health information].

[105] Because LifeLabs did not have reasonable policies and procedures in place, it also breached the SHA Agreement.

b. Other Safeguards

[106] In addition to reviewing policies and procedures, trustees and IMSPs should also review all other relevant safeguards in place at the time of the privacy breach. After this review, trustees are in a better position to determine if the safeguards were effective and what needs to be added or modified in order to prevent future breaches.

[107] LifeLabs' reported that it had employed skilled security personnel whose mandate was to plan and implement enterprise IT system defenses against security breaches and vulnerability issues, to audit existing procedures, and to put in place security policies, procedures and standards. Because LifeLabs did not have written and approved policies and procedures in place, I am not persuaded that the security personnel fulfilled its mandate successfully.

[108] LifeLabs indicated that it also engaged different independent service providers in order to maintain an appropriately safeguarded system. It was one of these service providers that discovered the breaches as a part of its security assessment of LifeLabs' systems.

[109] LifeLabs reported that it models its service commitments and systems requirements on the trusts services criteria set forth in the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria. LifeLabs indicated it did so to be in compliance with its regulatory and contractual agreements. LifeLabs provided no details to demonstrate how it meets the AICPA Trust Services Criteria. However, late in my investigation, LifeLabs provided documents related to an independent audit of its security systems from May 2019 that showed how LifeLabs was in compliance with the Trust Services criteria as well as LifeLabs' plan for remediation in some cases. The audit documents also noted that LifeLabs' IT security policies were in draft form.

[110] During the course of my investigation, I learned of critical patches that were not applied to LifeLabs' IT systems. This was not mentioned in its January 2020 response to my office. My office specifically asked LifeLabs to provide information about these patches.

LifeLabs did not initially comply with this request. It was not until May 27, 2020 that LifeLabs provided more information.

[111] LifeLabs advised that there was a code-level third party vulnerability. The vulnerability was not caught by the third party vulnerability management system/dashboard. The vulnerability management system should have recognized the need to patch the third party software in order to address common vulnerabilities and exposures. Further, LifeLabs indicated that, prior to the cyberattack, it contracted with another third party to do a vulnerability scan which did not detect the vulnerability. LifeLabs reported that its internal investigations have revealed that the only information that could possibly have led LifeLabs to the proper patch was a single unsolicited email message that was diverted into the junk mail folder of a developer at LifeLabs. The developer was not part of the security team at LifeLabs and was not required to search their junk mail folder for such emails as part of their duties to the company. LifeLabs indicated that the developer was unaware of the existence of this message prior to the discovery of the cyberattack. LifeLabs commented that having non-security personnel searching in email for such messages does not constitute a common practice in the security field.

[112] LifeLabs did not indicate if it was a common practice for the third party to communicate patches in this manner or if it missed any other patches because it was seemingly directed to a random person in the organization. LifeLabs did not indicate if this occurrence deviated from the "technical policies" it claimed to have in place at the time of the breach.

[113] LifeLabs did not provide any other information about other factors it considered that may have contributed to the breach or safeguards that may have been in place during the breach.

c. The SHA Agreement

[114] As part of my investigation, I examined the SHA Agreement. In this Report, I have already discussed the initial difference in understanding between the parties on the fundamental issue of who has control of the information. The SHA Agreement is clear that the SHA has control. I have also discussed how LifeLabs did not have written policies and

procedures in place and did not get the SHA's approval for its privacy breach protocol. These are both violations of the SHA Agreement.

[115] Also, during my investigation, I examined the duties of both the SHA and LifeLabs in the event of a breach. Appendix E of the SHA Agreement provides:

> 14. Assistance with Access Request & Complaints/Investigations
>
> [LifeLabs] shall co-operate with, and assist in, any access request or investigation of a complaint that any [personal health information] has been collected, used or disclosed contrary to HIPA, LA FOIP or other applicable laws, whether such investigation is conducted by the [the SHA] itself or a body having the legal authority to conduct the investigation. For greater certainty, the foregoing shall apply in respect of any formal or informal review or investigation conducted by the Office of the Information and Privacy Commissioner of Saskatchewan.

[116] As noted, the SHA has control of the personal health information in the patient wait time system. As such, it is also the SHA's responsibility to investigate and ensure that any deficiencies in safeguards are identified and addressed. In its investigation report, the SHA indicated that it had an understanding that the breach of privacy was the prime responsibility of LifeLabs within their contract with the SHA. The SHA did not explain how it reached that conclusion, especially when LifeLabs' privacy breach protocol was not approved by the SHA.

[117] LifeLabs notified the SHA about the breach in mid-November 2019. The SHA reported to my office on January 17, 2020, that it requested written information about the breach from LifeLabs twice in November. It reported that it received a written briefing note from LifeLabs on December 16, 2019. I have reviewed this briefing note, and it only provided high level information. On March 13, 2020, the SHA reported that it asked LifeLabs again for its investigation report. On March 25, 2020, LifeLabs provided the SHA with a two page briefing note. Again, LifeLabs' indicated that its investigation was not complete. My office has reviewed this briefing note and, in my opinion, it does not constitute a fulsome privacy breach report. However, the SHA has not demonstrated that it has been assertive in requiring additional information from LifeLabs.

[118] I note clause 14 of Appendix E of the SHA Agreement requires LifeLabs to cooperate with an investigation by my office. As discussed above, I requested the investigation reports that were created by third parties on behalf of LifeLabs. It refused to provide them to my office. Further, what LifeLabs has provided to my office does not provide enough detail to persuade me that the breach has been properly investigated. I am not persuaded that LifeLabs has satisfied clause 14 of Appendix E of the SHA Agreement.

[119] I note that clause 15(c) of Appendix E of the SHA Agreement allows the SHA to require LifeLabs to contain and remedy the breach within a specific time period.

> 15. Breach of Privacy.
> …
>
> c) If [LifeLabs] has breached any term or condition contained in this Appendix, [the SHA] may by notice in writing to [LifeLabs], require [LifeLabs] to contain the breach as quickly as possible and where possible, using best efforts, remedy the breach within a specified period of time, but in no event less than thirty (30) days.

[120] The SHA did not take this step.

[121] Further, as noted earlier in this Report, LifeLabs would have difficulties responding to access requests because it is not set up to verify the identities of individuals. LifeLabs cannot meet its obligations under clause 14 of Appendix E of the SHA Agreement, noted above.

[122] Clause 11 of Appendix E of the SHA Agreement indicates that any personal health information must be stored in Saskatchewan unless LifeLabs receives permission from the SHA. LifeLabs stores the information related to the patient wait time system on servers located in Ontario. Clause 11 is as follows:

> 11. Location of the [personal health information]
>
> [LifeLabs] may possess and maintain the [personal health information] only at [the SHA's] facilities in the Province of Saskatchewan.

> The [personal health information] may not be possessed, stored or maintained at any other location without the prior written consent of [the SHA], which consent will not be unreasonably withheld.

[123] The SHA indicated that it did not have conversations about where the personal health information would be stored. LifeLabs did not receive the written consent of the SHA to use the servers in Ontario.

[124] Clause 12 of Appendix E of the SHA Agreement indicates that personal health information should be segregated from any other information owned by LifeLabs or other parties, as follows:

> 12. Security and Segregation of [personal health information]
>
> [LifeLabs] shall have in place reasonable policies, procedures and safeguards to protect the confidentiality and security of the [personal health information]. [LifeLabs] shall ensure the physical security of the [personal health information] by making reasonable security arrangements against such risks as unauthorized access, collection, use. disclosure or disposal. Such security arrangements shall include, without limitation, reasonable technical, physical and administrative safeguards. Without limiting the generality of the foregoing, [LifeLabs] shall take reasonable steps to ensure that all [personal health information] is securely segregated from any information owned by [LifeLabs] or third parties, including access barriers, physical segregation and password authorization.

[125] When asked if the personal health information in question in LifeLabs patient wait time system was mixed with personal health information of other parties, LifeLabs responded by indicating that it does not collect personal health information for patients it serves through the SHA Agreement. As described in this Report, my view is that the SHA does have control of the personal health information in question. I am not persuaded that LifeLabs is in compliance with clause 12 of Appendix E of the SHA Agreement.

d. Other concerns

[126] Additionally, LifeLabs indicated that the earliest evidence in its system of compromise from the cyberattack, that has been found so far, is from November 2018. My expectation is that, in its report to my office, LifeLabs would have addressed why the sporadic

cyberattack went undetected in its systems for nearly a year. In the information it provided about the breach to my office, LifeLabs did not address the monitoring safeguards that were in place during this time. However, LifeLabs did note this is a common security challenge for all organizations.

[127] The information I received from LifeLabs did not provide enough detail about the breach or how it occurred. LifeLabs did not provide information about the specific technical safeguards that were in place or the root cause of the breach. The piecemeal manner in which LifeLabs provided my office with information has not given me fulsome understanding of what caused the breach, if there were adequate safeguards in place at the time of the breach or how LifeLabs arrived at its conclusions.

[128] I find that LifeLabs has not demonstrated that it has properly investigated this breach. I also find that LifeLabs has not demonstrated that it had reasonable safeguards in place at the time of the breach in accordance with subsection 16(b) of HIPA. I further find that the SHA has not taken steps to ensure the breach has been properly investigated.

Prevent future privacy breaches

[129] Preventing future breaches means to implement measures to prevent similar breaches from occurring.

[130] On the subject of prevention, in January 2020, LifeLabs simply reported that:

> We enforced a least privileged model on our compromised servers. We added our privileged and service accounts. We enforced stronger passwords requirements for those accounts.

[131] I questioned why LifeLabs did not have a least privileged model in place during the time of the breach. My understanding of the least privilege principle in IT is that a subject should only be given those privileges needed for it to complete its task. This is similar to the need-to-know principle related to HIPA. The need-to-know principle is the principle that trustees and their staff should only collect, use or disclose personal health information

needed for the diagnosis, treatment or care of an individual or other authorized purposes. Personal health information should only be available to those employees in an organization that have a legitimate need-to-know that information for the purpose of delivering their mandated services. A trustee should limit collection and use of personal health information to what an employee needs-to-know to do their job, not collect or use information that is nice to know. The need-to-know principle originates from section 23 of HIPA, which provides:

> **23**(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
>
> …
>
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

[132] On April 13, 2020, LifeLabs clarified as follows:

> The "least privilege model" has always been used by LifeLabs for framework controls. We referenced this as we ensured during the implementation of the new environment, a least privilege model was carefully re-enforced enforced [sic] to provide assurance.

[133] This seems to contradict LifeLabs' original statement which indicated that it intended to prevent future breaches by "enforcing a least privileged model on [its] compromised servers". LifeLabs provided more information on May 27, 2020 and asserted that it demonstrated that a least privilege model was already enforced during the breach.

[134] In effect, when LifeLabs provided its response to my office in January 2020, it did not provide any new substantial measures it undertook to prevent future breaches.

[135] In response to questions from my office throughout the investigation, LifeLabs provided more information about measures it intended to take to prevent future breaches. It provided

a final list on May 27, 2020. For security reasons, I will not reproduce the list in this Report.

[136] The prevention measures that LifeLabs provided through out the investigation did not provide granular detail about what specific actions must be taken to implement these measures, who is responsible to implement these measures and by what date LifeLabs is committing to implement these measures. Further, without a comprehensive report from LifeLabs, the list of preventative measures makes me wonder if the long list of measures reflects deficiencies in LifeLabs security practices at the time of the breach.

[137] Late in my investigation, LifeLabs indicated its Chief Information Security Officer was responsible for implementing the measures. It also noted that as the organization improves its security posture, industry best practices also continue to evolve and therefore, the target maturity state in any given assessment may change over time. LifeLabs was unwilling to commit to timeframes.

[138] I recommend that the SHA request this list from LifeLabs as well as regular updates on its progress of implementation of the prevention measures identified.

[139] Additionally, I note that the most fundamental safeguard, developing and formalizing written policies and procedures, was not addressed as a prevention measure until May 27, 2020.

[140] I recommend that LifeLabs make developing, formalizing and updating its written privacy and security policies a priority and do it in accordance with the SHA Agreement and HIPA. LifeLabs indicated that this was in progress.

[141] Without having an understanding of what the root cause of the breach was or any factors related to why the cyberattack was successful and went undetected for so long, I am unable to assess if LifeLabs' prevention measures are reasonable and adequate.

[142] I am not persuaded that LifeLabs is doing enough to prevent similar breaches from occurring in the future. I am similarly not persuaded that the SHA has done enough to ensure the personal health information in its control is protected from future breaches.

Write an investigation report

[143] Documenting privacy breaches and the trustee's investigations into the breaches is a method to ensure the trustee follows through with plans to prevent similar breaches in the future.

[144] After indicating that it took five months to complete its investigation, LifeLabs has refused to provide a detailed report to my office.

[145] Moreover, LifeLabs has not provided enough details about the safeguards in place at the time of the breach, the causes of the breach and the measures it has taken to prevent future breaches to satisfy the expectations of my office.

[146] The piecemeal information that followed LifeLabs' initial response in January 2020 has not provided my office with a satisfactory sense of what occurred.

[147] I am unable to conclude that LifeLabs has produced a comprehensive investigation report. It certainly has not provided one to my office.

[148] The SHA has provided me with an investigation report, but because it did not require full cooperation from LifeLabs, the SHA's investigation report is not complete.

Overall assessment of the response to the breach

[149] My role as Commissioner during privacy breach investigations is to assess the response of a trustee/IMSP to a privacy breach and then report to the public whether I have concluded the trustee/IMSP has responded reasonably and adequately.

[150] In this case, seven months after the discovery of the breach, I have concluded that LifeLabs' has not done enough to properly notify affected individuals, investigate the breach, prevent future breaches or create a comprehensive investigation report. I have also identified several ways in which LifeLabs' was not in compliance with HIPA at the time of the cyberattack. I have had to make these conclusions based on the limited information provided by LifeLabs.

[151] Overall, I am disappointed with the lack of information about the breach provided by LifeLabs, the delay in notifying my office and affected individuals and its assessment of the risk to affected individuals.

[152] LifeLabs has missed its opportunity to demonstrate to my office that it has responded adequately to this breach. I leave it to the SHA to enforce contracts with LifeLabs. I also leave it to the Ministry to review licences granted to LifeLabs. Both the SHA and the Ministry have the ability and the responsibility to ensure that LifeLabs has enough safeguards in place to adequately protect personal health information in the future.

[153] The SHA Agreement provides the SHA with the following ability to audit privacy related records and facilities of LifeLabs. Appendix E of the SHA Agreement provides:

> 8. Audit
>
> [LifeLabs] will provide (a) [the SHA]'s internal auditors; and/or (b) a nationally recognized Canadian audit firm appointed by [the SHA] upon fifteen (15) days prior written notice, with reasonable access to relevant books, records and facilities related to the Agreement in order to conduct appropriate audits. examinations and inspections to ensure [LifeLabs]'s compliance with this Appendix.
>
> …
>
> [LifeLabs] will provide access to information and facilities reasonably required by [the SHA]'s auditors to perform such audits during the normal business hours for the Services in question and upon reasonable prior written notice to the Contract, such written notice to be not less than fifteen (15) days.
>
> …
>
> [LifeLabs] agrees to respond in writing to any observations made by any audit within ninety(90) days of receipt of such observations. If any audit or inspection by [the SHA] or its representative reveals that [LifeLabs] is non-compliant with this Schedule,

> [LifeLabs] shall promptly bring itself into compliance. In addition, if [LifeLabs] is found to be materially non-compliant with this Schedule, [LifeLabs] shall pay the reasonable costs associated with the audit. Further, in such case, [the SHA] shall be entitled to conduct such further audits as are reasonably necessary to ensure that [LifeLabs] has, in fact, brought itself into compliance.

[154] I recommend that the SHA undertake, pursuant to Appendix E, an audit of LifeLabs' systems and responses to this breach to ensure that the breach has been fully addressed and that LifeLabs is in compliance with HIPA and the SHA Agreement. I further note that the SHA Agreement provides the following:

> 15. Breach of Privacy.
> …
>
> b) If [LifeLabs] is found to have breached any term or condition contained in this Appendix and/or more specifically failed to conduct their operation in alignment with applicable privacy legislation, [LifeLabs] shall immediately notify [the SHA] in writing, and [LifeLabs] shall immediately take steps to remedy the breach.
>
> c) If [LifeLabs] has breached any term or condition contained in this Appendix, [the SHA] may by notice in writing to [LifeLabs], require [LifeLabs] to contain the breach as quickly as possible and where possible, using best efforts, remedy the breach within a specified period of time, but in no event less than thirty (30) days.
>
> d) If [LifeLabs] does not remedy the breach to the satisfaction of [the SHA] within the time prescribed in such written notice, which time period [the SHA] confirms will be reasonable given the nature of the breach, [the SHA] may, by notice in writing, terminate this Agreement.
>
> e) All of the confidentiality, protection and security provisions in this Agreement survive the termination of the Agreement.

[155] If LifeLabs is uncooperative with the SHA's attempts to audit LifeLabs' response to the privacy breach, or if the SHA finds it has insufficient safeguards and no feasible plans to prevent future breaches, I recommend that the SHA consider terminating its agreement with LifeLabs.

[156] I recommend that the SHA provide regular updates to my office about its progress in implementing these recommendations.

[157] Further, the Ministry has authority over LifeLabs because it grants licences through the Licencing Act.

[158] Section 11 of the Licencing Act describes when a licence should be suspended or cancelled as follows:

> **11**(1) The director may amend, suspend or cancel a licence where, in the opinion of the director, the licensee:
>
> (a) has failed to comply with:
>
> (i) a provision of this Act or the regulations; or
>
> (ii) a term or condition contained in the licence;
>
> (b) has failed to take part in the accreditation program; or
>
> (c) is operating the medical laboratory in a manner that is contrary to the public interest.
>
> (2) For the purposes of section 4, a licence that is suspended pursuant to this section is, for the period of the suspension, deemed to have not been granted.

[159] I note that the Licencing Act predates HIPA and therefore it is not explicit in either the Licencing Act or *The Medical Laboratory Licensing Regulations, 1995* (the Licencing Regulations) that laboratories must comply with HIPA. I view HIPA as applying to medical laboratories because they are trustees. HIPA also applies to IMSPs providing services on a trustee's behalf. For clarity, I recommend that the Ministry study an amendment to either the Licencing Act or the Licencing Regulations to require that laboratories comply with HIPA as a condition of having a licence.

[160] While it is not explicitly a requirement of the Licencing Act that laboratories comply with HIPA or protect privacy, it is in the public interest to do so.

[161] The Ministry has the power to amend licences and to impose conditions. I recommend the Ministry amend LifeLabs' licences to include a condition that they, in all respects, comply with HIPA.

[162] Part of the Ministry's ability to manage these licences is the ability to inspect or investigate what the Ministry considers necessary. Section 14 of the Licencing Act provides:

> **14**(1) For the purposes of administering this Act and the regulations, the director or any person designated by the director for the purpose may make any inspection, investigation or inquiry that the director or that person considers necessary.
>
> (2) Every licensee shall:
>
> > (a) cause the medical laboratory for which the licence is granted to be open for inspection by the director or a person designated pursuant to subsection (1) at all reasonable times during the hours of operation of the medical laboratory; and
> >
> > (b) cause all books, documents, records, specimens and equipment pertaining to the operation of the medical laboratory to be available for inspection by the director or a person designated pursuant to subsection (1) during the times described in clause (a).
>
> (3) The director or a person appointed pursuant to subsection (1) shall not enter a private dwelling without a warrant issued pursuant to section 15 unless the occupant of the dwelling consents to the entry.

[163] I recommend that the Ministry inspect LifeLabs' documents, records, and equipment to ensure it is adequately protecting personal health information in the public interest. If after an inspection by the Ministry, it is determined that LifeLabs' is not adequately protecting personal health information, I recommend that the Ministry consider suspending or cancelling LifeLabs' licences.

III FINDINGS

[164] I find that the SHA has control of the personal health information in question.

[165] I find that the disclosure of personal health information to the cyberattacker constitutes both a breach of HIPA and of the SHA Agreement.

[166] I find that LifeLabs made an adequate effort to contain the breach.

[167] I find that LifeLabs has not protected the integrity or accuracy of the personal health information in question in accordance with subsection 16(a) of HIPA.

[168] I find that LifeLabs and the SHA have not adequately notified affected individuals.

[169] As LifeLabs did not have written security policies in place, I find that LifeLabs was not in compliance with subsection 16(c) of HIPA. I find that it also breached the SHA Agreement.

[170] I find that LifeLabs has not demonstrated that it had reasonable safeguards in place at the time of the breach in accordance with subsection 16(b) of HIPA.

[171] I find that LifeLabs and the SHA have not demonstrated that it has properly investigated this breach.

[172] I find that LifeLabs has not done enough to demonstrate it will prevent similar breaches from occurring in the future.

[173] I find that the SHA has not done enough to ensure the personal health information in its control is protected from future breaches.

[174] I find that LifeLabs and the SHA did not produce an adequate investigation report.

IV RECOMMENDATIONS

[175] I recommend that the SHA and LifeLabs specifically address the issue of custody and control of personal health information in the patient wait time system in the SHA agreement and communicate it clearly to the citizens of Saskatchewan.

[176] I recommend that LifeLabs update its patient wait time system so that it is able to authenticate the identity of individuals.

[177] I recommend that LifeLabs and the SHA provide cyber security protection to affected individuals from Saskatchewan for a minimum of five years.

[178] I recommend that the SHA request the list of preventative measures from LifeLabs as well as quarterly updates on its progress of implementation of the prevention measures identified.

[179] I recommend that LifeLabs make developing, formalizing and updating its written security policies a priority and obtain the approval of the SHA.

[180] I recommend that the SHA undertake, under the terms of Appendix E, an audit of LifeLabs' systems and response to this breach, or another meaningful arrangement to ensure the breach has been fully addressed and that LifeLabs is in compliance with HIPA and the SHA Agreement.

[181] I recommend that the SHA provide quarterly updates to my office about its progress in implementing these recommendations.

[182] If LifeLabs is uncooperative with the SHA's attempts to audit LifeLabs' response to the privacy breach, or if the SHA finds it has insufficient safeguards and no feasible plans to prevent future breaches, I recommend that the SHA consider terminating its agreement with LifeLabs.

Dated at Regina, in the Province of Saskatchewan, this 9th day of June, 2020.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy
Commissioner