Brown, Stephen R HLTH:EX

From: Rongve, Ian HLTH:EX
Sent: November 1, 2019 5:11 PM
To: Brown, Stephen R HLTH:EX; Byres, David W HLTH:EX; Barclay, Corrie A HLTH:EX; Prevost, Jean-Marc GCPE:EX
Cc: Slater, James; Watt, Rebecca HLTH:EX; Pearce, Alison HLTH:EX; Diacu, Mariana HLTH:EX; Perkins, Gary CITZ:EX; Moulton, Holly HLTH:EX
Subject: LifeLabs Issues Note
Attachments: BN Cyber Security Incident Nov 1 Update.pdf

Categories: Printed info

Hi all

Attached is the updated issues note from LL.

Jenn Cudlipp has committed to communicating immediately any significant issues over the weekend, particularly if it looks like BC data is impacted. They are currently working 24/7 on this.

Thanks

Ian Rongve, Ph.D.
Assistant Deputy Minister
Provincial, Hospital & Laboratory Health Services Division
Ministry of Health

LifeLabs®

Briefing Note

November 1, 2019

Cyber Incident Update – November 1

Overview

- Further to the update provided on October 31, LifeLabs is responding to two cyber security incidents that occurred on October 28 and October 31. At this time, we are treating them as separate incidents based on the evidence collected to date.
- In response, LifeLabs' Board and Executive leaders are fully engaged overseeing and managing the response and investigation. We have also engaged third party subject matter experts to provide support conducting the investigation and developing communication materials, if required.
- A summary of each incident is provided below:

Incident 1

- On October 28, shortly before midnight, proactive network surveillance tools detected unauthorized access[s.15]

s.15

- As per standard operating procedure, we quickly isolated the affected systems to eliminate and contain any potential impact of the unauthorized access. We also immediately engaged a top international cyber security firm (CrowdStrike) to conduct a comprehensive forensic review of the situation and further secure other LifeLabs and Excelleris systems.
- Since October 28, we have not detected any activity to suggest that a persistent threat exists and we are confident that our networks are safe, secure and under control. At this time, we do not have evidence to suggest data from the servers was removed from LifeLabs' systems.

s.15

LifeLabs

- We are working with CrowdStrike to continue to investigate s.15 s.15

For more information, contact:

Jennifer Cudlipp, SVP, British Columbia & President, Excelleris
778 668 9475

Brown, Stephen R HLTH:EX

From: CITZ Deputy Minister, CITZ:EX
Sent: November 4, 2019 9:38 AM
To: BCPSA Agency DMC List
Cc: BCPSA Agency DMC Admin & Operational Support
Subject: Information Incident Management Policy
Attachments: 112177 - DM Memo - Information Incident Management Policy - DMC.pdf

Sending on behalf of Jill Kot, Deputy Minister

Ministry of Citizens' Services

BRITISH COLUMBIA

Memorandum

Ref: 112177

Date: November 4, 2019

To: DMC Colleagues

Re: Updated Information Incident Management Policy

Dear Colleagues,

I am writing to let you know of my Ministry's efforts to support you in the appropriate investigation and resolution of information incidents, including privacy breaches. An updated Information Incident Management Policy (the Policy) has been published, and is now in effect.

This Policy modernizes government's information incident response and investigation framework. It focuses on a principles-based approach and key priorities throughout the stages of information incident management, while allowing for flexibility in responding to the unique circumstances of various incidents. The Policy applies to all government employees, with specific responsibilities for supervisors, Ministry Chief Information Officers (MCIOs), and Deputy Ministers. In particular, the Policy more clearly reflects – but doesn't change - Deputy Ministers' ultimate accountability for their organization's response to information incidents.

Under this Policy, the Corporate Information and Records Management Office (CIRMO) remains government's liaison with the Office of the Information and Privacy Commissioner, and in particular the Privacy, Compliance and Training Branch remains government's liaison in relation to information incidents and privacy breaches.

CIRMO has provided briefings on the Policy to MCIOs, as well as Ministry Privacy Officers and Ministry Information Security Officers to ensure they are aware of these changes. Additional information and supporting resources will be published at www.gov.bc.ca/privacy_breaches and communicated via @Work to all employees.

../2

Office of the Deputy Minister
Ministry of Citizens' Services

Mailing Address:
Box 9440 Stn Prov Govt
Victoria BC V8W 9V3

Telephone: 250 387-8852
Facsimile: 250 387-8561
Email: CITZDeputyMinister@gov.bc.ca

If you have any specific questions about the Policy, please feel free to contact me, or Kerry Pridmore, ADM CIRMO.

Kind regards,

Jill Kot
Deputy Minister

Brown, Stephen R HLTH:EX

From: Moulton, Holly HLTH:EX
Sent: November 12, 2019 5:46 PM
To: van Baarsen, Amanda HLTH:EX; Brown, Stephen R HLTH:EX
Subject: Fwd: MOH Lifelabs update November 12
Attachments: Lifelabs update November 12.docx; ATT00001.htm

Update from LL

- Negotiations continuing
- Investigations continuing but scale is not determined yet
- LL in development of communications(including possible call center and credit monitoring) with affected patients
- LL, MOH, CITZ and Ontario engaged in communications planning

See attached for the fulsome update.

LifeLabs Update

- The information security incident with LifeLabs has escalated as LifeLabs has evidence that some BC residents' data has been accessed.
    - So far the data has not involved clinical data and is limited to non clinical appointment data but for prudence we should assume clinical results are included.
    - There is concern about identity theft resulting from the use of data accessed (providers names and addresses, patient names, PHNs, addresses, postal codes, dates of birth, and gender)
- LifeLabs is fully engaged with MOH, CITZ, the OIPC on an investigation and planning on how to respond.
- MOH, CITZ, and LifeLabs are working together to develop a plan for notifying the patients:
    - OIPC was briefed and requested to be updated regularly on the scope of the breach and the timing of the notification to BC citizens
    - LL will consider establishing a contract for credit monitoring services with (with a national organization) e.g. TransUnion.
    - MOH, CITZ and LifeLabs communications teams are fully coordinated.
- MOH has connected with the Ministry of Health in Ontario for the purpose of coordinating communication messages to the public and the timing for the patients' notification of the privacy breach of personal information at LifeLabs in Ontario and British Columbia.
- LL confirmed that Saskatchewan and New Brunswick are potentially impacted in addition to Ontario. LL have confirmed that all Provinces will be made aware of the incident.
- LifeLabs has engaged an internationally recognised firm, Crowdstrike to help them with the technical aspects of the investigation s.15

s.15

- LifeLabs Executive Team and Board are fully involved in the response.
- LifeLabs is currently confident that they have contained the vulnerability and the systems secured. Services to the public have returned to normal.

Chronology

- On October 28, LifeLabs proactive system surveillance identified unauthorized access s.15

s.15

    - LifeLabs immediately isolated the affected systems to eliminate and contain any potential impact of the unauthorized access

s.15

s.15

- LifeLabs has secured services for setting up a call centre for concerned citizens; and, it is working with a credit monitoring agency to provide services that may help protect citizens against identity theft or fraud.

Communications Planning

- GCPE is fully involved and is developing messaging for the incident, actions taken and notification plans.
- GCPE and LifeLabs Communications are monitoring the situation and adjusting the communication messages as necessary based on contingency scenarios (Q&As; mitigation strategies; earl y disclosure)

Brown, Stephen R HLTH:EX

From: Pokorny, Peter HLTH:EX
Sent: December 5, 2019 11:33 AM
To: Brown, Stephen R HLTH:EX
Subject: FW: s.12
s.12
Attachments:

From: Bell, Carolyn P HLTH:EX <Carolyn.Bell@gov.bc.ca>
Sent: October 28, 2019 3:48 PM
To: Pokorny, Peter HLTH:EX <Peter.Pokorny@gov.bc.ca>
Subject: Fwd: s.12

Is this what you are looking for?

Sent from my iPhone

Begin forwarded message:

> **From:** "Bell, Carolyn P HLTH:EX" <Carolyn.Bell@gov.bc.ca>
> **Date:** October 28, 2019 at 3:45:17 PM PDT
> **To:** "'carolyn.bell@gov.bc.ca'" <'carolyn.bell@gov.bc.ca'>
> **Subject: Fwd:** s.12
>
> Sent from my iPhone
>
> Begin forwarded message:
>
> > **From:** "Bell, Carolyn P HLTH:EX" <Carolyn.Bell@gov.bc.ca>
> > **Date:** October 23, 2019 at 9:42:46 AM PDT
> > **To:** "Rongve, Ian HLTH:EX" <Ian.Rongve@gov.bc.ca>
> > **Cc:** "Patterson, Catherine M HLTH:EX" <Catherine.Patterson@gov.bc.ca>
> > **Subject:** s.12
> >
> > Here is the new deck. I will work with Catherine to finalize and send to Bobbi (likely before noon) but after we receive the ADMPR minute from last week and ensure we have answered the minute or that Peter is raising the right topics with Doug Foster and OCG today.

Carolyn Bell, Executive Director/ Precision Medicine and Laboratory Services Transformation Branch/Provincial, Hospital, and Laboratory Health Services Division/BC Ministry of Health/office: 778-698-1755/cell: s.17

Page 11 of 69

Withheld pursuant to/removed as

s.12

Page 12 of 69 to/à Page 13 of 69

Withheld pursuant to/removed as

s.12; s.17

Page 14 of 69

Withheld pursuant to/removed as

s.17; s.12

Page 15 of 69

Withheld pursuant to/removed as

s.12; s.13; s.17

Page 16 of 69 to/à Page 18 of 69

Withheld pursuant to/removed as

s.12

Page 19 of 69 to/à Page 20 of 69

Withheld pursuant to/removed as

s.12; s.13; s.17

Page 21 of 69

Withheld pursuant to/removed as

s.12; s.13

Page 22 of 69

Withheld pursuant to/removed as

s.12; s.17

Page 23 of 69 to/à Page 24 of 69

Withheld pursuant to/removed as

s.12; s.13

Page 25 of 69

Withheld pursuant to/removed as

s.12; s.13; s.17

Page 26 of 69

Withheld pursuant to/removed as

s.12; s.13

Page 27 of 69

Withheld pursuant to/removed as

s.12

Brown, Stephen R HLTH:EX

From: Brown, Stephen R HLTH:EX
Sent: December 5, 2019 11:46 AM
To: Kennedy, Christine PREM:EX
Cc: Moulton, Holly HLTH:EX
Subject: s.12
Attachments:

Hi Christine
Here is an overview deck the program prepared. TB proposal will be developed for early in new calendar year but have not yet been given a time. Steve

Page 29 of 69

Withheld pursuant to/removed as

s.12

Page 30 of 69 to/à Page 32 of 69

Withheld pursuant to/removed as

s.12; s.17

Page 33 of 69

Withheld pursuant to/removed as

s.12; s.13; s.17

Page 34 of 69 to/à Page 36 of 69

Withheld pursuant to/removed as

s.12

Page 37 of 69 to/à Page 38 of 69

Withheld pursuant to/removed as

s.12; s.13; s.17

Page 39 of 69

Withheld pursuant to/removed as

s.12; s.13

Page 40 of 69

Withheld pursuant to/removed as

s.12; s.17

Page 41 of 69

Withheld pursuant to/removed as

s.12; s.13

Page 42 of 69

Withheld pursuant to/removed as

s.13; s.12

Page 43 of 69

Withheld pursuant to/removed as

s.12; s.13; s.17

Page 44 of 69

Withheld pursuant to/removed as

s.12; s.13

Page 45 of 69

Withheld pursuant to/removed as

s.12

Brown, Stephen R HLTH:EX

From: Rongve, Ian HLTH:EX
Sent: December 15, 2019 5:37 PM
To: Brown, Stephen R HLTH:EX; Moulton, Holly HLTH:EX; Prevost, Jean-Marc GCPE:EX
Subject: LL december 16 update v.2
Attachments: LL december 16 update v.2.docx

Hi Steve, Jean-Marc and Holly

Attached is an updated information document on the LL issue. It has been reviewed by MOH and CITZ.

LifeLabs - December 16

Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it comes to the personal information of citizens.
- British Columbians must have the utmost confidence that their information is secure and protected.
- The Ministries of Health and Citizens' Services are working closely with LifeLabs in a consulting role as LifeLabs responds to the incident.
- LifeLabs has hired world-leading cyber security firms to investigate and respond to this incident.
- LifeLabs has notified the Office of the Information and Privacy Commissioner of this incident as well as law enforcement agencies.
- At this time, there is no evidence to indicate that B.C. government systems are affected by this breach.

s.13

- At this time LifeLab's cyber security firms have not seen any further unauthorized use or disclosure of the data.
- Any privacy breach – small or large – is investigated thoroughly, leveraging an established and effective incident management process and by highly trained information incident investigators, to quickly address the breach and mitigate impacts.

Discussion

<u>Detection</u>

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-attack with the LifeLabs booking system.
    - At that time they did not believe that any patient data had been compromised
- LifeLabs confirmed that BC resident data had been compromised on November 7th.
- The Province and Office of the Information and Privacy Commissioner were immediately informed of the incident on November 7th when it was confirmed that B.C. residents' data was involved and has been kept to date on the investigation.
- LifeLabs is a private company and has been leading the investigation but is cooperating with both the Ministry of Health and the Ministry of Citizen Services.

<u>Data</u>

- The data about B.C. residents that has been impacted includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers (BC Services Card/Care Card numbers), gender and dates of birth and some test result information for a small subset of customers.
- LifeLabs has confirmed they were able to secure the data by making a payment.s.15

s.15

- LifeLabs is still investigating the full scope of those who may be affected. There are upwards of four million British Columbians whose information is stored in the LifeLabs repository and who are potentially impacted as a result of the attack.
- LifeLabs has indicated that only a small percentage of the data known to have been impacted includes British Columbia laboratory tests, impacting less than 1 per cent of the population.

Public Notification

- LifeLabs plans on issuing a public notification to all clients at 9:00 AM on December 17, 2019.
    - LifeLabs is working closely with the Ministries of Health and Citizens' Services to develop a plan to notify affected B.C. residents of this incident and to offer protections to mitigate risks associated with the cyber-security incident.
    - LifeLabs is planning on notifying individuals whose test results were affected directly through a letter. If no test results were included for an individual, LifeLabs will be indirectly notifying the person through public announcements, a call centre and a dedicated website
- LifeLabs plans on offering all of their customers cybersecurity protection for one year from TransUnion that includes credit monitoring, credit reporting, dark-web monitoring and identity-theft insurance as a protective measure to those impacted.
- LifeLabs confirmed that they delayed issuing the notification sooner following the discovery of the cyber-attack to ensure their systems were adequately protected to prevent against any subsequent attacks that may occur once the public notification has been issued. Such secondary attacks pose a real risk to the functionality of technical systems as we have seen from other recent cyber-attack around the world. LifeLabs wanted to prevent against any impacts to patient care if their systems were brought offline had the threat actor again been successful in accessing LifeLabs systems.
- LifeLabs also required additional time to ensure all resources are in place to conduct a notification on such a wide scale. This was reviewed and supported by both the Ministry's and the Office of the Information and Privacy Commissioner (OIPC). All parties acknowledge that minimizing any impacts to patient care is a major priority for any incident similar to this.
- The Ministry of Health and the Provincial Health Services Authority are working together to notify the regional health authority Communications, Laboratory Operations, and Information Management executive and to provide key messages that can be used in case they are asked about the incident.
    - At this point, the notification is proposed for shortly before the LifeLabs announcement on December 17.

Information and Privacy Commissioner

- The OIPC has been involved since LifeLabs determined a breach had occurred. They have agreed to the December 17, 2019 release date for when LifeLabs will issue their public notification.
- s.3

s.3

- The OIPC have confirmed that they are conducting a joint investigation with the Privacy Commissioner's office on Ontario. The investigation will result in a public report that will outline the technical findings. The timing of this report is to be determined but will likely be in the spring.
- The OIPC confirmed they will be issuing their own press release on December 17th to direct concerned individuals to contact LifeLab's call center with any questions they have about the incident.

Securing LifeLabs Systems

- LifeLabs and their vendors took immediate action to harden their systems to prevent further attack and they now believe their systems are secure.
- LifeLabs indicated that the investigation and remediation of the incident is complex and requires coordination with various firms that have been engaged in the review.
- LifeLabs' incident response is still underway, and they do not have a timeline for when this work will be completed.
- LifeLabs are currently being supported by CrowdStrike s.15
s.15
- With their support, LifeLabs is putting in place measures to further secure their systems from attacks that may be inspired by the public disclosure on December 17, including:
s.15

Impact on Health Authorities systems

- According to LifeLabs, the databases and systems that were affected are not connected to provincial public systems and so the provincial databases and systems are not affected.
- Health Authorities send lab result information to LifeLabs via the Excelleris lab result distribution service to send to providers and patients via the Excelleris myEhealth portal.
- The connectivity between the Health Authorities and Excelleris are via restricted organization to organization encrypted connections.
- The access does not provide for broad access to Health Authority networks or systems, or direct access to the source Lab Information System within the Health Authority.
- LifeLabs has taken a number of preventive and remedial measures to give the Province confidence that Health Authority networks and systems were not impacted by this cyber attack, including:
    - LifeLabs has indicated that the potential source systems do not contain Health Authority sourced data
    - Impacted LifeLabs systems do not have direct connectivity or data flows to Excelleris, which is used for lab report distribution by the Health Authorities.
    - In scope impacted networks have limited/restricted connectivity to Excelleris data centers

LifeLabs Contract with the Province

- LifeLabs is the largest provider of community (non hospital out-patient) laboratory services in BC.
- In 2018, LifeLabs provided almost 34.6 million tests and had 5.6 million patient visits.
- LifeLabs was paid $234 million in 2018/19 by the Ministry predominantly through modified fee for service and is on track to receive $243 million for fiscal 2019/20.
- LifeLabs is a private operator under the *Laboratory Services Act* providing laboratory services under an agreement.
- LifeLabs is currently in the last year of an agreement with the province to provide community lab services for the province.
- LifeLabs committed in the agreement to maintain the highest standards of privacy, confidentiality and data security of patients and their policies are governed and compliant with the Personal Information Protection Act in the province of British Columbia.
- However, as a signatory of the agreement LifeLabs provides services as a service provider and must comply with the FOIPPA legislative provisions as well as with the obligations and requirements set out in the privacy and security schedules of the agreement.

National impact

- LifeLabs provides services to customers in Ontario, British Columbia, and Saskatchewan.
- LifeLabs' public notification will cover their customers in these three provinces.
- The number of Saskatchewan customers affected by the breach is lower than those in Ontario and British Columbia.
- The Province is working with the Ontario Ministry of Health in sharing information about the public notification and communication process for December 17.

Brown, Stephen R HLTH:EX

From: Brown, Stephen R HLTH:EX
Sent: December 17, 2019 6:14 AM
To: Dix, Adrian HLTH:EX; van Baarsen, Amanda HLTH:EX
Cc: Rongve, Ian HLTH:EX; Moulton, Holly HLTH:EX; Prevost, Jean-Marc GCPE:EX
Subject: 2019-12-17-ipc_oipc-media-statement final Dec 16 2 PM.DOCX
Attachments: 2019-12-17-ipc_oipc-media-statement final Dec 16 2 PM.DOCX

FYI. Here is the draft that the Commissioner has sent to me for their news release today following LIfeLabs. Steve

Page 52 of 69 to/à Page 59 of 69

Withheld pursuant to/removed as

s.3

Brown, Stephen R HLTH:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 17, 2019 1:33 PM
To: Moulton, Holly HLTH:EX
Cc: van Baarsen, Amanda HLTH:EX; Rongve, Ian HLTH:EX; Brown, Stephen R HLTH:EX
Subject: 18/19 data

This is what the Medical Services Commission Blue Book has for 2018/19 (publicly available)

LifeLabs BC LP $240,542,511.93

FY2018/2019	% Claims Volume	Total Fee-For-Service Outpatient Laboratory Testing Claims Volume
% LifeLabs	66%	34.64 M
% Public	29%	14.95 M
% others (Valley, UBC, etc)	5%	2.73 M

Brown, Stephen R HLTH:EX

From: van Baarsen, Amanda HLTH:EX
Sent: December 18, 2019 7:36 PM
To: Dix, Adrian HLTH:EX
Cc: Brown, Stephen R HLTH:EX; Prevost, Jean-Marc GCPE:EX
Subject: LL statement & media tmrw
Attachments: LL Response (004).docx

Ian is confirming the Nov 7th date for accuracy but the rest of the attached (and copied out below) has been fact checked and is accurate if you would like to use this.

We have confirmed that you are able to go on Mike Smyth's show anytime you want, between 10am and 2pm (do you have a preference?) and are still attempting to reach the CBC Early Edition but I am fearful that we have lost our opportunity with that one due to the late hour.

Statement:

s.13

s.13

Amanda van Baarsen
Sr Ministerial Assistant to
Hon. Adrian Dix, Minister of Health
Room 337| Parliament Buildings, Victoria, BC | V8V 1X4
(P) 778-974-5075 (C) 778-678-3454
Pronouns: she/hers

Brown, Stephen R HLTH:EX

From: Rongve, Ian HLTH:EX
Sent: December 19, 2019 3:04 PM
To: Brown, Stephen R HLTH:EX
Subject: Fwd: Data Encryption Response

Sent from my iPhone

Begin forwarded message:

> **From:** "Barclay, Corrie A HLTH:EX" <Corrie.Barclay@gov.bc.ca>
> **Date:** December 19, 2019 at 2:50:41 PM PST
> **To:** "Rongve, Ian HLTH:EX" <Ian.Rongve@gov.bc.ca>
> **Cc:** "Pearce, Alison HLTH:EX" <Alison.Pearce@gov.bc.ca>, "Perkins, Gary CITZ:EX" <Gary.Perkins@gov.bc.ca>, "Carroll, Scott CITZ:EX" <Scott.Carroll@gov.bc.ca>, "XT:Bayne, James HLTH:IN" <James.Bayne@phsa.ca>, "Diacu, Mariana HLTH:EX" <Mariana.Diacu@gov.bc.ca>
> **Subject: Data Encryption Response**
>
> Hi Ian, below are some key messages to answer the questions, what is the standard practice for data encryption and should the province require it from LL. Let me know if you need more or something different. Thank you to Gary for quick turn around.
>
> s.13; s.15

Regards,
Corrie

From: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>
Sent: December 19, 2019 2:09 PM
To: Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; XT:Bayne, James HLTH:IN <James.Bayne@phsa.ca>
Cc: Pearce, Alison HLTH:EX <Alison.Pearce@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: RE: Proposed questions/follow up (please review)

s.13

s.13; s.15

From: Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>
Sent: December 19, 2019 1:58 PM
To: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; XT:Bayne, James HLTH:IN <James.Bayne@phsa.ca>
Cc: Pearce, Alison HLTH:EX <Alison.Pearce@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: RE: Proposed questions/follow up (please review)

Ok, great, thank you. When do you think you will have the ISO or NIST References – wondering if I should send this or wait for a bit

From: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>
Sent: December 19, 2019 1:53 PM
To: Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; XT:Bayne, James HLTH:IN <James.Bayne@phsa.ca>
Cc: Pearce, Alison HLTH:EX <Alison.Pearce@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: RE: Proposed questions/follow up (please review)

Here's my first pass.
I will dig up the ISO or NIST references to encryption.
I like to try and keep it simple.

s.13; s.15

From: Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>
Sent: December 19, 2019 1:01 PM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; XT:Bayne, James HLTH:IN <James.Bayne@phsa.ca>; Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>
Cc: Pearce, Alison HLTH:EX <Alison.Pearce@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: RE: Proposed questions/follow up (please review)

Thank you Scott, I have made a suggested edit to #5 and also have some proposed starting wording to address the question being asked regarding should we require LL to encrypt data:

s.13; s.15

s.13; s.15

Ian needs an answer by end of day on the above, so appreciate review of bullets.

Thank you
Corrie

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: December 19, 2019 12:14 PM
To: XT:Bayne, James HLTH:IN <James.Bayne@phsa.ca>
Cc: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>; Pearce, Alison HLTH:EX <Alison.Pearce@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>
Subject: Re: Proposed questions/follow up (please review)

I can't comment on those as it's not my expertise. I'm open to any edits or feedback there to add clarity as to their intended purpose.

Sent from my iPhone

On Dec 19, 2019, at 12:10 PM, Bayne, James <James.Bayne@phsa.ca> wrote:

> For 4/5 is the intent to just have LL speak to the question?s.13
> s.13
>
> James
>
> > On Dec 19, 2019, at 12:03 PM, Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca> wrote:
> >
> > Questions look good to me except I would take another look at #5.
> >
> > **From:** Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
> > **Sent:** December 19, 2019 11:56 AM
> > **To:** Pearce, Alison HLTH:EX <Alison.Pearce@gov.bc.ca>; Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>; XT:Bayne, James HLTH:IN <James.Bayne@phsa.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>
> > **Subject:** Proposed questions/follow up (please review)
> >
> > I have tried to compile everything for LL based on the feedback. Please have another look below at the questions and send me any additional questions or edits. Please note that recent focus for media has been on whether the data was encrypted, and whether the government would have required for LifeLabs data to

be encrypted. It would be good to know what our requirements would be.

s.13; s.15

Scott Carroll

A/Manager & Senior Investigator

Investigations Unit
Privacy, Compliance and Training Branch, Ministry of Citizens' Services
PO Box 9406, Stn Prov Gov, Victoria BC V8W 9V1
scott.carroll@gov.bc.ca
(250) 356-7349
Cell (250) 216-3784

Brown, Stephen R HLTH:EX

From: Rongve, Ian HLTH:EX
Sent: December 20, 2019 3:47 PM
To: Brown, Stephen R HLTH:EX
Subject: Fwd: LL Audit Report - response for Stephen

Hi Steve. This is an assessment of the security audit report from LL submitted to the lab agency last year.

You had asked if someone who knew what they were doing could review.

Obviously this review is done with hindsight.

Sent from my iPhone

Begin forwarded message:

> **From:** "Barclay, Corrie A HLTH:EX" <Corrie.Barclay@gov.bc.ca>
> **Date:** December 20, 2019 at 3:38:48 PM PST
> **To:** "Rongve, Ian HLTH:EX" <Ian.Rongve@gov.bc.ca>
> **Subject: LL Audit Report - response for Stephen**
>
> Hi Ian, hope this helps -- a summary to help answer your question:
>
> s.13; s.15

s.13

Let me know if you need anything more,
Regards,
Corrie

Murray, Heather HLTH:EX

From: Pokorny, Peter HLTH:EX
Sent: January 28, 2020 10:00 AM
To: Murray, Heather HLTH:EX
Subject: FW: Update
Attachments: image001.jpg; ATT00001.htm; BN Cyber Security Incident Oct 31 Update.pdf; ATT00002.htm

From: Byres, David W HLTH:EX <David.Byres@gov.bc.ca>
Sent: October 31, 2019 1:59 PM
To: Pokorny, Peter HLTH:EX <Peter.Pokorny@gov.bc.ca>
Subject: Fwd: Update

FYI - Citizen Services also notified

Sent from my iPhone

Begin forwarded message:

> **From:** "Rongve, Ian HLTH:EX" <Ian.Rongve@gov.bc.ca>
> **Date:** October 31, 2019 at 1:41:16 PM PDT
> **To:** "Moulton, Holly HLTH:EX" <Holly.Moulton@gov.bc.ca>, "Byres, David W HLTH:EX" <David.Byres@gov.bc.ca>, "Prevost, Jean-Marc GCPE:EX" <Jean-Marc.Prevost@gov.bc.ca>, "Barclay, Corrie A HLTH:EX" <Corrie.Barclay@gov.bc.ca>
> **Subject: FW: Update**
>
> Information note from LL. Not much new info.
>
> **From:** Cudlipp, Jennifer <Jennifer.Cudlipp@lifelabs.com>
> **Sent:** October 31, 2019 1:22 PM
> **To:** Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
> **Subject:** Update
>
> Ian
>
> As discussed, I am attaching the briefing on the incident. We will update you (verbally) as we learn more information and will also follow up with another briefing note as we learn more information.
>
> Jenn
>
> **Jennifer Cudlipp CPA, CGA**
> **SVP, British Columbia & President, Excelleris**
> LifeLabs | 3680 Gilmore Way | Burnaby, BC V5G 4V8
> T 604-507-5187 | C 778-668-9475
> E **Jennifer.Cudlipp@LifeLabs.com**
> **www.LifeLabs.com**

LifeLabs®

Briefing Note

October 31, 2019

Cyber Incident Update - October 31

Overview

- On October 28, 2019, LifeLabs proactive surveillance identified unauthorized access s.15 s.15 that we are currently addressing. s.15 s.15

- As per standard operating procedure, we quickly isolated the affected systems to eliminate and contain any potential impact of the unauthorized access.
- s.15

- Our investigation remains ongoing. We have engaged a top international independent cyber security firm to conduct a comprehensive forensic review of the situation. Although further investigation is needed at this time, it appears that the unauthorized access may have been limited s.15
- As we continue our investigation, we will be in regular touch with the Ministry to provide further updates.

For more information, contact:

Jennifer Cudlipp, SVP, British Columbia & President, Excelleris
778 668 9475

Murray, Heather HLTH:EX

From: Pokorny, Peter HLTH:EX
Sent: January 28, 2020 10:00 AM
To: Murray, Heather HLTH:EX
Subject: FW: LL

-----Original Message-----
From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Sent: November 15, 2019 2:56 PM
To: Brown, Stephen R HLTH:EX <Stephen.Brown@gov.bc.ca>; Pokorny, Peter HLTH:EX <Peter.Pokorny@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: LL

Just heard from jenn cudlipp at LifeLabs. They have the data back. Their technical team is working with it to see exactly what it is.

They will keep us updated as things progress.

Sent from my iPhone

Murray, Heather HLTH:EX

From: Pokorny, Peter HLTH:EX
Sent: January 28, 2020 10:01 AM
To: Murray, Heather HLTH:EX
Subject: FW: 2019-12-17-ipc_oipc-media-statement final Dec 16 2 PM.DOCX
Attachments: 2019-12-17-ipc_oipc-media-statement final Dec 16 2 PM.DOCX

From: Moulton, Holly HLTH:EX <Holly.Moulton@gov.bc.ca>
Sent: December 17, 2019 7:24 AM
To: Pokorny, Peter HLTH:EX <Peter.Pokorny@gov.bc.ca>
Subject: 2019-12-17-ipc_oipc-media-statement final Dec 16 2 PM.DOCX

Draft that the Commissioner has sent for their news release today following LIfeLabs.
HM

Page 5 of 9 to/à Page 6 of 9

Withheld pursuant to/removed as

s.3

Murray, Heather HLTH:EX

From: Pokorny, Peter HLTH:EX
Sent: January 28, 2020 9:59 AM
To: Murray, Heather HLTH:EX
Subject: FW: Commissioners investigating Lifelabs privacy breach affecting millions

From: Duffy, Maija JTT:EX <Maija.Duffy@gov.bc.ca>
Sent: December 17, 2019 4:16 PM
To: Glazer, Brad R HLTH:EX <Brad.Glazer@gov.bc.ca>; Popp, Nathan HLTH:EX <Nathan.Popp@gov.bc.ca>; Shrimpton, Paul HLTH:EX <Paul.Shrimpton@gov.bc.ca>; Bell, Carolyn P HLTH:EX <Carolyn.Bell@gov.bc.ca>; Stylianou, John HLTH:EX <John.Stylianou@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>; Pokorny, Peter HLTH:EX <Peter.Pokorny@gov.bc.ca>; Kingsford, Douglas HLTH:EX <Douglas.Kingsford@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Thain, Leanne P HLTH:EX <Leanne.Thain@gov.bc.ca>
Cc: Chow, David K JTT:EX <David.K.Chow@gov.bc.ca>; Nankivell, Nathan JTT:EX <Nathan.Nankivell@gov.bc.ca>; Brownsey, Silas JTT:EX <Silas.Brownsey@gov.bc.ca>
Subject: FW: Commissioners investigating Lifelabs privacy breach affecting millions

Hi Health Supercluster team

I'm sure you might already be aware of the privacy breach at LifeLabs, but wanted to flag to you as well just in case.

Regards,
Maija

From: Cordeiro, Shantel GCPE:EX <Shantel.Cordeiro@gov.bc.ca>
Sent: Tuesday, December 17, 2019 11:07 AM
To: Duffy, Maija JTT:EX <Maija.Duffy@gov.bc.ca>
Cc: Cascaden, Lori R GCPE:EX <Lori.Cascaden@gov.bc.ca>
Subject: FW: Commissioners investigating Lifelabs privacy breach affecting millions

Hi Maija,

I just wanted to flag the below NR for you to keep in mind as you work with the supercluster on their Cycle 2, My Personal Health Wallet project.

Thanks,
Shantel

From: noreply.newsondemand@gov.bc.ca <noreply.newsondemand@gov.bc.ca>
Sent: December 17, 2019 11:02 AM
To: Cordeiro, Shantel GCPE:EX <Shantel.Cordeiro@gov.bc.ca>
Subject: Commissioners investigating Lifelabs privacy breach affecting millions

For Immediate Release

Dec. 17, 2019

Office of the Information and Privacy Commissioner for British Columbia
Office of the Information and Privacy Commissioner of Ontario

NEWS RELEASE
Commissioners investigating Lifelabs privacy breach affecting millions

VICTORIA - The Office of the Information and Privacy Commissioner of Ontario (IPC) and the Office of the Information and Privacy Commissioner for British Columbia (OIPC) are undertaking a co-ordinated investigation into a cyberattack on the computer systems of Canadian laboratory testing company LifeLabs.

LifeLabs is Canada's largest provider of general diagnostic and specialty laboratory testing services. The company has four core divisions: LifeLabs, LifeLabs Genetics, Rocky Mountain Analytical, and Excelleris.

On Nov. 1, 2019, LifeLabs reported a potential cyberattack on their computer systems to the IPC and the OIPC. Shortly thereafter, they confirmed they were the subject of an attack affecting the personal information of millions of customers, primarily in Ontario and British Columbia. They told us that the affected systems contain information of approximately 15 million LifeLab customers, including name, address, email, customer logins and passwords, health card numbers and lab tests. LifeLabs advised our offices that cyber criminals penetrated the company's systems, extracting data and demanding a ransom. Lifelabs retained outside cybersecurity consultants to investigate and assist with restoring the security of the data.

The co-ordinated IPC/OIPC investigation will, among other things, examine the scope of the breach, the circumstances leading to it and what, if any, measures Lifelabs could have taken to prevent and contain the breach. We will also investigate ways LifeLabs can help ensure the future security of personal information and avoid further attacks.

"An attack of this scale is extremely troubling. I know it will be very distressing to those who may have been affected. This should serve as a reminder to all institutions, large and small, to be vigilant," said Brian Beamish, information and privacy commissioner of Ontario. "Cyberattacks are growing criminal phenomena and perpetrators are becoming increasingly sophisticated. Public institutions and health-care organizations are ultimately responsible for ensuring that any personal information in their custody and control is secure and protected at all times."

Michael McEvoy, information and privacy commissioner for B.C. said, "I am deeply concerned about this matter. The breach of sensitive personal health information can be devastating to those who are affected. Our independent offices are committed to thoroughly investigating this breach. We will publicly report our findings and recommendations once our work is complete."

The IPC and OIPC are reaching out to the information and privacy commissioners of other jurisdictions with affected customers.

LifeLabs has set up a dedicated phone line and information on their website for individuals affected by the breach. To find out more, the public should visit customernotice.lifelabs.com (http://www.customernotice.lifelabs.com/) or contact LifeLabs at 1 888 918-0467.

Note to media: The IPC and OIPC will not discuss the details of the investigation while it is ongoing. The offices will issue a public report once the investigation is complete.

Brian Beamish

Information and Privacy Commissioner of Ontario

Michael McEvoy

Information and Privacy Commissioner of British Columbia

Contacts:

Jane Zatylny
Office of the Information and Privacy Commissioner for British Columbia
jzatylny@oipc.bc.ca
250 415-3283

Jason Papadimos
Office of the Information and Privacy Commissioner of Ontario
media@ipc.on.ca
416 326-3965

Murray, Heather HLTH:EX

From: Byres, David W HLTH:EX
Sent: January 28, 2020 9:29 AM
To: Murray, Heather HLTH:EX
Subject: FW: LifeLabs Security Breach

From: MacKinnon, Mark HLTH:EX <Mark.MacKinnon@gov.bc.ca>
Sent: December 17, 2019 1:47 PM
To: 'registrar@chirobc.com' <registrar@chirobc.com>; 'jlawrence@cdhbc.com' <jlawrence@cdhbc.com>; 'registrar@cdtbc.ca' <registrar@cdtbc.ca>; 'registrarsoffice@cdsbc.org' <registrarsoffice@cdsbc.org>; 'chacker@cdsbc.ca' <chacker@cdsbc.ca>; XT:HLTH REGISTRAR@CD.BC.CA <REGISTRAR@CD.BC.CA>; 'JBouchard@collegeofdietitiansbc.org' <JBouchard@collegeofdietitiansbc.org>; Saville, Amanda HLTH:EX <Amanda.Saville@gov.bc.ca>; 'registrar@cmtbc.ca' <registrar@cmtbc.ca>; 'eric.wredenhagen@cmtbc.ca' <eric.wredenhagen@cmtbc.ca>; 'hoetter@cpsbc.ca' <hoetter@cpsbc.ca>; 'registrar@cmbc.bc.ca' <registrar@cmbc.bc.ca>; 'registrar@cnpbc.bc.ca' <registrar@cnpbc.bc.ca>; XT:HLTH OFFICE@CNPBC.BC.CA <OFFICE@CNPBC.BC.CA>; 'pstanaway@cnpbc.bc.ca' <pstanaway@cnpbc.bc.ca>; 'Cynthia.Johansen@bccnp.ca' <Cynthia.Johansen@bccnp.ca>; XT:HLTH Corbett, Kathy <kcorbett@cotbc.org>; 'lbannerman@cobc.ca' <lbannerman@cobc.ca>; 'college@optometrybc.ca' <college@optometrybc.ca>; 'registrar@optometrybc.ca' <registrar@optometrybc.ca>; 'bob.nakagawa@bcpharmacists.org' <bob.nakagawa@bcpharmacists.org>; 'dmillette@cptbc.org' <dmillette@cptbc.org>; 'registrar@cpodsbc.org' <registrar@cpodsbc.org>; 'registrar@collegeofpsychologists.bc.ca' <registrar@collegeofpsychologists.bc.ca>; 'akowaz@collegeofpsychologists.bc.ca' <akowaz@collegeofpsychologists.bc.ca>; 'cameron.cowper@cshbc.ca' <cameron.cowper@cshbc.ca>; XT:HLTH registrar@ctcma.bc.ca <registrar@ctcma.bc.ca>; 'jonathan@ctcma.bc.ca' <jonathan@ctcma.bc.ca>
Cc: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Armitage, Mark W HLTH:EX <Mark.Armitage@gov.bc.ca>; Byres, David W HLTH:EX <David.Byres@gov.bc.ca>; MacKinnon, Mark HLTH:EX <Mark.MacKinnon@gov.bc.ca>; Smith, Leah M HLTH:EX <Leah.Smith@gov.bc.ca>; Westgate, Brian A HLTH:EX <Brian.Westgate@gov.bc.ca>; Younker, Katherine E HLTH:EX <Katherine.Younker@gov.bc.ca>
Subject: FW: LifeLabs Security Breach

Good afternoon everybody,

Please see below an email fem Mariana Diacu which she has asked me to share with you.

Thanks,

M

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: December 17, 2019 10:36 AM
To: 'mmurray@cpsbc.ca' <mmurray@cpsbc.ca>
Cc: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: LifeLabs Security Breach

Hello,

I would like to give you the heads up about the following breach:

On December 17, 2019, it was announced that LifeLabs, the private company responsible for conducting lab testing services in B.C., experienced a significant data breach stemming from a cyber-security incident. The breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.

At this time LifeLabs investigation has also confirmed some lab test results from Ontario customers were taken during the breach. They will notify those customers directly. LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.

Working in cooperation with the Office of the Information Privacy Commissioner, RCMP and the B.C. Ministries of Health and Citizens' Services, LifeLabs is notifying patients who have used their services while also taking steps to secure their information systems against future attack.

More information at:

https://www.lifelabs.com/

Best wishes,

Mariana Diacu
Executive Director Laboratory and Blood Services Branch
Provincial, Hospital and Laboratory Health Services Division
Tel: 7789 974 4105
Cell: s.17

Murray, Heather HLTH:EX

From: Byres, David W HLTH:EX
Sent: January 28, 2020 9:31 AM
To: Murray, Heather HLTH:EX
Subject: FW: Update
Attachments: BN Cyber Security Incident Oct 31 Update.pdf

From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Sent: October 31, 2019 1:41 PM
To: Moulton, Holly HLTH:EX <Holly.Moulton@gov.bc.ca>; Byres, David W HLTH:EX <David.Byres@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>
Subject: FW: Update

Information note from LL. Not much new info.

From: Cudlipp, Jennifer <Jennifer.Cudlipp@lifelabs.com>
Sent: October 31, 2019 1:22 PM
To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Subject: Update

Ian

As discussed, I am attaching the briefing on the incident. We will update you (verbally) as we learn more information and will also follow up with another briefing note as we learn more information.

Jenn

Jennifer Cudlipp CPA, CGA
SVP, British Columbia & President, Excelleris
LifeLabs | 3680 Gilmore Way | Burnaby, BC V5G 4V8
T 604-507-5187 | C 778-668-9475
E **Jennifer.Cudlipp@LifeLabs.com**
www.LifeLabs.com

LifeLabs®

Briefing Note

October 31, 2019

Cyber Incident Update - October 31

Overview

- On October 28, 2019, LifeLabs proactive surveillance identified unauthorized access s.15 s.15 that we are currently addressing. s.15 s.15
- As per standard operating procedure, we quickly isolated the affected systems to eliminate and contain any potential impact of the unauthorized access.
- s.15
- Our investigation remains ongoing. We have engaged a top international independent cyber security firm to conduct a comprehensive forensic review of the situation. Although further investigation is needed at this time, it appears that the unauthorized access may have been limited s.15
- As we continue our investigation, we will be in regular touch with the Ministry to provide further updates.

For more information, contact:

Jennifer Cudlipp, SVP, British Columbia & President, Excelleris
778 668 9475

Murray, Heather HLTH:EX

From: Byres, David W HLTH:EX
Sent: January 28, 2020 9:31 AM
To: Murray, Heather HLTH:EX
Subject: FW: LifeLabs Issues Note

From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Sent: November 1, 2019 5:15 PM
To: Byres, David W HLTH:EX <David.Byres@gov.bc.ca>
Subject: RE: LifeLabs Issues Note

Good question. I think it is internal but will connect.

From: Byres, David W HLTH:EX <David.Byres@gov.bc.ca>
Sent: November 1, 2019 5:14 PM
To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Subject: Re: LifeLabs Issues Note

We're police notified (given the ransom etc) or is this all managed / investigated internally

Sent from my iPhone

> On Nov 1, 2019, at 5:11 PM, Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca> wrote:
>
> Hi all
>
> Attached is the updated issues note from LL.
>
> Jenn Cudlipp has committed to communicating immediately any significant issues over the weekend, particularly if it looks like BC data is impacted. They are currently working 24/7 on this.
>
> Thanks
>
> Ian Rongve, Ph.D.
> Assistant Deputy Minister
> Provincial, Hospital & Laboratory Health Services Division
> Ministry of Health
>
> <BN Cyber Security Incident Nov 1 Update.pdf>

Dix, Adrian HLTH:EX

From: van Baarsen, Amanda HLTH:EX
Sent: November 12, 2019 5:49 PM
To: Dix, Adrian HLTH:EX
Subject: FW: MOH Lifelabs update November 12
Attachments: Lifelabs update November 12.docx; ATT00001.htm

FYI. Police are not involved.

From: Moulton, Holly HLTH:EX <Holly.Moulton@gov.bc.ca>
Sent: November 12, 2019 5:46 PM
To: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>; Brown, Stephen R HLTH:EX <Stephen.Brown@gov.bc.ca>
Subject: Fwd: MOH Lifelabs update November 12

Update from LL

Negotiations continuing

- Investigations continuing but scale is not determined yet
- LL in development of communications(including possible call center and credit monitoring) with affected patients
- LL, MOH, CITZ and Ontario engaged in communications planning

See attached for the fulsome update.

LifeLabs Update

- The information security incident with LifeLabs has escalated as LifeLabs has evidence that some BC residents' data has been accessed.
    - So far the data has not involved clinical data and is limited to non clinical appointment data but for prudence we should assume clinical results are included.
    - There is concern about identity theft resulting from the use of data accessed (providers names and addresses, patient names, PHNs, addresses, postal codes, dates of birth, and gender)
- LifeLabs is fully engaged with MOH, CITZ, the OIPC on an investigation and planning on how to respond.
- MOH, CITZ, and LifeLabs are working together to develop a plan for notifying the patients:
    - OIPC was briefed and requested to be updated regularly on the scope of the breach and the timing of the notification to BC citizens
    - LL will consider establishing a contract for credit monitoring services with (with a national organization) e.g. TransUnion.
    - MOH, CITZ and LifeLabs communications teams are fully coordinated.
- MOH has connected with the Ministry of Health in Ontario for the purpose of coordinating communication messages to the public and the timing for the patients' notification of the privacy breach of personal information at LifeLabs in Ontario and British Columbia.
- LL confirmed that Saskatchewan and New Brunswick are potentially impacted in addition to Ontario. LL have confirmed that all Provinces will be made aware of the incident.
- LifeLabs has engaged an internationally recognised firm, Crowdstrike to help them with the technical aspects of the investigation s.15

s.15

- LifeLabs Executive Team and Board are fully involved in the response.
- LifeLabs is currently confident that they have contained the vulnerability and the systems secured. Services to the public have returned to normal.

Chronology

- On October 28, LifeLabs proactive system surveillance identified unauthorized access s.15

s.15

    - LifeLabs immediately isolated the affected systems to eliminate and contain any potential impact of the unauthorized access

s.15

s.15

- LifeLabs has secured services for setting up a call centre for concerned citizens; and, it is working with a credit monitoring agency to provide services that may help protect citizens against identity theft or fraud.

Communications Planning

- GCPE is fully involved and is developing messaging for the incident, actions taken and notification plans.
- GCPE and LifeLabs Communications are monitoring the situation and adjusting the communication messages as necessary based on contingency scenarios (Q&As; mitigation strategies; earl y disclosure)

Dix, Adrian HLTH:EX

From: van Baarsen, Amanda HLTH:EX
Sent: December 13, 2019 6:00 PM
To: Dix, Adrian HLTH:EX
Cc: Yeung, Lucinda HLTH:EX
Subject: FW: LL december 12 update
Attachments: LL december 12 update.docx; ATT00001.htm

The latest just came in on LifeLabs to me. Attached.

From: Moulton, Holly HLTH:EX <Holly.Moulton@gov.bc.ca>
Sent: December 13, 2019 5:59 PM
To: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>
Cc: Brown, Stephen R HLTH:EX <Stephen.Brown@gov.bc.ca>
Subject: LL december 12 update

Good afternoon Amanda. Attached is today's update on Lifelabs.

Regards
Holly

LifeLabs - December 12

Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it comes to the personal information of citizens.
- British Columbians must have the utmost confidence that their information is secure and protected.
- The Ministries of Health and Citizens' Services are working closely with LifeLabs in a consulting role as LifeLabs responds to the incident.
- LifeLabs has hired world-leading cyber security firms to investigate and respond to this incident.
- LifeLabs has notified the Office of the Information and Privacy Commissioner of this incident as well as law enforcement agencies.
- At this time, there is no evidence to indicate that B.C. government systems are affected by this breach.
- s.13

- At this time LifeLab's cyber security firms have not seen any further unauthorized use or disclosure of the data.
- Any privacy breach – small or large – is investigated thoroughly, leveraging an established and effective incident management process and by highly trained information incident investigators, to quickly address the breach and mitigate impacts.

Discussion

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a security incident with the LifeLabs booking system.
    - At that time they did not believe that any patient data had been compromised
- LifeLabs confirmed that BC resident data had been compromised on November 7th but the extent was and remains unknown.
- The Office of the Information and Privacy Commissioner was immediately informed of the incident on November 7th when it was confirmed that B.C. residents' data was involved and has been kept to date on the investigation.
- LifeLabs is a private company and has been leading the investigation but is cooperating with both the Ministry of Health and the Ministry of Citizen Services.
- The data about B.C. residents that has been impacted includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers (BC Services Card/Care Card numbers), gender and dates of birth.
- LifeLabs is still investigating the full scope of those who may be affected. There are upwards of four million British Columbians whose information is stored in the LifeLabs repository and who are potentially impacted as a result of the attack.
- However, LifeLabs believes now that the number of British Columbia laboratory tests affected by the breach is relatively small, impacting less than 1 per cent of the population.
- Once the scope is determined, LifeLabs will begin the notification process.

- LifeLabs is working closely with the Ministries of Health and Citizens' Services to develop a plan to notify affected B.C. residents of this incident and to offer protections to mitigate risks associated with the cyber-security incident.

Public notification

- LifeLabs plans on issuing a public notification to all clients on December 17, 2019.
- LifeLabs plans on offering credit monitoring as a protective measure to those impacted.
- LifeLabs has delayed issuing the notification to ensure their systems are adequately protected to prevent against any subsequent attacks that may occur once the public notification has been issued. Such secondary attacks are a real risk and that should the threat actor again be successful that patient care could be impacted if their systems are brought offline.
- LifeLabs also require additional time to ensure all resources are in place to conduct a notification on such a wide scale.

Privacy Commissioner

- The OIPC approved the December 17, 2019 release date for when LifeLabs will issue their public notification.
- s.3

- The OIPC have confirmed that they are conducting a joint investigation with the Commissioner's office on Ontario. The investigation will result in a public report that will outline the technical findings.
- The OIPC confirmed they will be issuing a press release on the 17th to direct concerned individuals to contact LifeLab's call center with any questions they have about the incident.

LifeLabs measures to secure their systems from attacks

- LifeLabs' forensic investigation is ongoing.
- LifeLabs indicated that the investigation and remediation of the incident is complex and requires coordination with various firms that have been engaged in the review.
- LifeLabs' incident response is still underway and they do not have a timeline for when this work will be completed. At this time LifeLabs are still trying to ascertain a full understanding of all the components of the incident.
- LifeLabs are currently being supported by CrowdStrike s.15
s.15
-

- The Province and the Health Authorities recognize that Provincial technical systems are connected to LifeLabs IT infrastructure. Therefore, LifeLabs should complete a review of the connections and provide confirmation of what has been done to date and what will be done to ensure those connections are secure.

Dix, Adrian HLTH:EX

From: van Baarsen, Amanda HLTH:EX
Sent: December 18, 2019 12:12 PM
To: Dix, Adrian HLTH:EX
Subject: Lifelabs Security Improvements
Attachments: Lifelabs work to secure systems_Dec 18_19.docx

Find attached, plain language word doc on what LifeLabs has done to secure the data. Also a pdf of their report to the OIPC.

This is not for distribution or public comment, as highlighted below.

From: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>
Sent: December 18, 2019 11:28 AM
To: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Cc: Shewchuk, Chris GCPE:EX <Chris.Shewchuk@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: RE: HLTH Media Request: Lifelabs breach

My initial feedback on the draft response is that the tone should reflect the reality of the risk – that we recognize it is a risk, technology is always changing, and we are doing everything in our power to protect against it, such as...

WRT our assurances in procurement of contracts with service providers – this needs to reflect that risk. Clearly it didn't work. What have we done to adapt. Etc.

Next steps should be clear, not being worked out, as we have known about this since late October.

From: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Sent: December 18, 2019 10:16 AM
To: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>
Cc: Shewchuk, Chris GCPE:EX <Chris.Shewchuk@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: FW: HLTH Media Request: Lifelabs breach

This is what LL provided to the OIPC – noting the security and confidentiality information – we wouldn't be able to share this with media – but the Minister may feel more comfortable knowing what was provided.

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: December 18, 2019 10:04 AM
To: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>
Cc: Shewchuk, Chris GCPE:EX <Chris.Shewchuk@gov.bc.ca>; Emerson, Kim GCPE:EX <Kim.Emerson@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: RE: HLTH Media Request: Lifelabs breach

I believe this is what you are referring to. It is quite technical. If this is needed in more plain language or if these need to be expanded upon please let me know.

If anyone copied here does not require a copy of this document for their records please delete it.

Thanks,
Scott

From: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Sent: December 18, 2019 9:35 AM
To: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Cc: Shewchuk, Chris GCPE:EX <Chris.Shewchuk@gov.bc.ca>; Emerson, Kim GCPE:EX <Kim.Emerson@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: FW: HLTH Media Request: Lifelabs breach

FYI on the following. Does the following response work?

Reporter
Shawn Benjamin, Producer
CBC
shawn.benjamin@cbc.ca
416-460-5616 c: 416-460-5616

Deadline ASAP

Request
Shawn Benjamin here at the CBC We are doing a follow up story about the lifelabs hack for CBC national TV and Radio News and we have a couple of questions.

1) How does the ministry ensure the protection of the electronic health records of British Columbians?

2) Does the ministry oversee or have security standards for private companies like lifelabs that work with health records?

Background

Recommendation

Government systems have security measures in place to prevent infiltrations, and proactive monitoring tools are in place to detect threats.

B.C. is the only province with a centralized team of highly trained information incident investigators to address any government privacy breaches thoroughly using an established and effective incident management process.

B.C. Government service agreements follow procurement rules that include both privacy protection and security schedules that clearly set out the requirements that contractors must abide by.

Expectations that service providers must meet the terms set out in their agreements are clearly communicated both in the agreement and verbally.

Service providers who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.

If any evidence is received that a service provider is non-compliant with any terms of their agreement, the service provider must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

Next steps for this incident will be determined based on our agreement with LifeLabs.