

Howlett, Tim GCPE:EX

From: Russell, Shannon CITZ:EX
Sent: December 17, 2019 12:54 PM
To: Marriott, Sarah GCPE:EX; Lauvaas, Kirsten GCPE:EX
Cc: Howlett, Tim GCPE:EX; Emerson, Kim GCPE:EX
Subject: RE: HLTH Media Request: LifeLabs Breach

Importance: High

Other than the fact that it needs to be attributed to the Province of BC, not the ministers of Health and CITZ, I'm good with the statement. NOTE that we are still waiting for final sign-off by Jill and Kerry.

Thanks,
Shannon

Shannon Russell
Senior Ministerial Assistant
Ministry of Citizens' Services
Shannon.Russell@gov.bc.ca | 250-387-9699

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Sent: December 17, 2019 12:34 PM
To: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>
Cc: Howlett, Tim GCPE:EX <Tim.Howlett@gov.bc.ca>; Emerson, Kim GCPE:EX <Kim.Emerson@gov.bc.ca>
Subject: RE: HLTH Media Request: LifeLabs Breach

Thank you, you're a star.

From: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Sent: December 17, 2019 12:34 PM
To: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>
Cc: Howlett, Tim GCPE:EX <Tim.Howlett@gov.bc.ca>
Subject: RE: HLTH Media Request: LifeLabs Breach

On it

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Sent: December 17, 2019 12:29 PM
To: Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: Howlett, Tim GCPE:EX <Tim.Howlett@gov.bc.ca>
Subject: FW: HLTH Media Request: LifeLabs Breach
Importance: High

Below is the proposed that is currently with Dix.

Please run it through approvals for release ASAP – ideally in the next 20 min. Many apologies.

With those edits I made below, this is approved by Tim and I.

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 17, 2019 12:25 PM
To: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>
Cc: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Subject: FW: HLTH Media Request: LifeLabs Breach
Importance: High

Rollup of media requests so far are pasted below.

Proposed response:

s.13

Background:

- LifeLabs says there is no evidence British Columbians' lab test results were impacted.
- According to Lifelabs, the breached data in B.C. includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.
- LifeLabs is a private company responsible for conducting approximately 34% of B.C. lab testing services.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Stephen May <Stephen.May@gov.bc.ca>

Sent: December 17, 2019 12:17 PM

To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>

Cc: Emerson, Kim GCPE:EX <Kim.Emerson@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>

Subject: HLTH Media Request: LifeLabs Breach

Reporters

Benjamin Dooley, Producer

CKNW AM 980

benjamin.dooley@corusent.com

604-331-2859 c: 604-331-2838

Bhinder Sajan, Reporter

CTV News (BC)

bhinder.sajan@bellmedia.ca

250-383-2480 c: 250-418-5207

Brett Mineer, Reporter

CHNL Radio (Kamloops) AM 610

bmineer@stingray.ca

250-374-1610 c: 778-789-1664

Jodie Martinson, Producer

CBC - Vancouver

jodie.martinson@cbc.ca

604-662-6463

Deadline ASAP

Request

CBC - Would Minister Dix please join us on CBC Radio The Early Edition at 7:40 AM to talk about the LifeLabs privacy breach?

CTV (Bhinder) - Looking for comment on LifeLabs Breach.

CHNL - Looking for comment from gov't spokesperson or minister.

CKNW - Ben Dooley - Looking for Minister for Lynda Steele show at 4:15 pm re: LifeLabs.

Background

Recommendation

Howlett, Tim GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 17, 2019 10:29 AM
To: Howlett, Tim GCPE:EX
Subject: FW: MORE UPDATES
Attachments: Media Statement Dec 17 2019 10am .docx

Importance: High

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 17, 2019 10:12 AM
To: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>
Subject: MORE UPDATES
Importance: High

I have modified the statement based on our discussions.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Prevost, Jean-Marc GCPE:EX
Sent: December 17, 2019 9:56 AM
To: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>
Subject: UPDATES
Importance: High

Government and OIPC statements attached.

(You may receive these from Holly as well).

Plan was to respond with statements only – **no spokesperson.**

Also I have a new version of the KM doc and Q & A for your review.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>
Sent: December 17, 2019 9:39 AM

To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>

Subject: Re: rundown today

Minister would like to see the privacy commission NR and our statment.

Sent from my iPhone

On Dec 17, 2019, at 9:31 AM, Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca> wrote:

At 10 a.m. at a new conference in Ontario LL will announce they were a victim of a cyber attack
They will confirm they have hired world-leading cyber security firms to assist them in responding
They will confirm they paid money to re-secure breached data

They will announce a website and call-in number for LL customers to get free credit monitoring and fraud-insurance

At 10:10 the BC's privacy commission will issue a news release announcing his investigation into the incident

The governments of Ontario and British Columbia plan to provide statements to media when asked (no plans for proactive statements).

<image001.png>

Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Background:

- LifeLabs says there is no evidence British Columbians' lab test results were impacted.
- The breached data in B.C. includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.
- LifeLabs is a private company responsible for conducting approximately 34% of B.C. lab testing services.

Page 007 of 358 to/à Page 009 of 358

Withheld pursuant to/removed as

s.3

Howlett, Tim GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 16, 2019 10:41 AM
To: Howlett, Tim GCPE:EX
Subject: FW: latest LL products
Attachments: generic LL statement (jmp).docx; draft frontline KMs_LL_sm.docx; LL KM Q A Dec 16.docx

Importance: High

Follow Up Flag: Follow up
Flag Status: Flagged

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 16, 2019 10:40 AM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>
Subject: latest LL products
Importance: High

Media statement
Cutdown Q&A and KM (for sharing with Health Authorities)
Long form Q & A (updates from CITZ as of this morning)

J M P

Desk: 236-478-0302
Cell: 250-886-2154

STATEMENT

For Immediate Release
[release number]
Dec. 17, 2019

Ministry of xx

Minister xx Statement on LifeLabs Cyber Attack

s.13

Media contact: Ministry of xx Communications
250 xxx-xxxx (media line)

Background:

- More than 60% of British Columbian's lab tests happen in hospitals. This breach did not affect any of that data.
- We encourage British Columbians who have had test done at LifeLabs to contact Lifelabs by visiting www.xxx.ca or calling 1-877-xxx-xxxx.

Howlett, Tim GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 10, 2019 1:54 PM
To: Howlett, Tim GCPE:EX
Subject: FW: LL FINAL
Attachments: LL KM Q A Dec 10 FINAL.docx

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 10, 2019 11:55 AM
To: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: RE: LL FINAL

Here it is without tracks.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Sent: December 10, 2019 11:43 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: RE: LL FINAL

Thanks, Jean-Marc.

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 10, 2019 11:41 AM
To: Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Cc: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Subject: LL FINAL

This is approved from Health program area.

Health DM plans to brief Health MO sometime Monday Dec. 16.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Rongve, Ian HLTH:EX
Sent: October 31, 2019 1:41 PM
To: Moulton, Holly HLTH:EX; Byres, David W HLTH:EX; Prevost, Jean-Marc GCPE:EX; Barclay, Corrie A HLTH:EX
Subject: FW: Update
Attachments: BN Cyber Security Incident Oct 31 Update.pdf

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



The information in this e-mail and any attachments is confidential and for the sole use of the intended recipient(s). If you have received this e-mail in error, please: accept our apologies for the inconvenience; note that any use of the information is strictly prohibited; notify the sender as soon as possible; and then delete all copies from your system.

Le contenu de ce message ainsi que du ou des fichiers qui y sont joints est strictement confidentiel et destine exclusivement a son ou sa destinataire. Si vous avez reçu ce courriel par erreur, veuillez en aviser l'expediteur des que possible et supprimer le courriel de votre ordinateur, son utilisation etant strictement interdite. Nous sommes desoles pour tout inconvenient que cette situation aurait pu vous occasionner.

Prevost, Jean-Marc GCPE:EX

From: Rongve, Ian HLTH:EX
Sent: November 5, 2019 4:26 PM
To: Moulton, Holly HLTH:EX; Prevost, Jean-Marc GCPE:EX; Diacu, Mariana HLTH:EX; Bell, Carolyn P HLTH:EX; Pearce, Alison HLTH:EX; Perkins, Gary CITZ:EX
Subject: LifeLabs update November 5
Attachments: LifeLabs update November 5.docx

Update as of today on LL

Prevost, Jean-Marc GCPE:EX

From: Rongve, Ian HLTH:EX
Sent: November 7, 2019 3:02 PM
To: Moulton, Holly HLTH:EX; Prevost, Jean-Marc GCPE:EX; May, Stephen GCPE:EX
Subject: Lifelabs update November 7
Attachments: Lifelabs update November 7.docx

Hi Holly, Jean-Marc and Steve May

Here is the written update on LL. I have also received an updated issues note from LL

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: November 8, 2019 2:44 PM
To: Barclay, Corrie A HLTH:EX; Prevost, Jean-Marc GCPE:EX; May, Stephen GCPE:EX; Jim Slater (james.slater@phsa.ca); Pearce, Alison HLTH:EX; Carroll, Scott CITZ:EX
Cc: Rongve, Ian HLTH:EX
Subject: Lifelabs update November 8
Attachments: Lifelabs update November 8.docx

FYI - Lifelabs update November 8.

Best wishes,

Mariana

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: November 12, 2019 4:23 PM
To: Rongve, Ian HLTH:EX; Barclay, Corrie A HLTH:EX; Pearce, Alison HLTH:EX; May, Stephen GCPE:EX; Perkins, Gary CITZ:EX; Prevost, Jean-Marc GCPE:EX; Carroll, Scott CITZ:EX
Cc: Diacu, Mariana HLTH:EX; Watt, Rebecca HLTH:EX
Subject: MOH Lifelabs update November 12
Attachments: Lifelabs update November 12.docx

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: November 15, 2019 6:19 PM
To: Prevost, Jean-Marc GCPE:EX; LeGuilloux, Marg GCPE:EX
Subject: FOR REVIEW: QA_LL_Nov 14 2018 dr 1
Attachments: QA_LL_Nov 15 2018 draft.docx; ATT00001.htm

Sharing the latest version of the QA, Jean-Marc, as my program area shared with yours. Will continue to update as needed.

Prevost, Jean-Marc GCPE:EX

From: Burton, Meribeth GCPE:EX
Sent: November 18, 2019 9:42 AM
To: Rongve, Ian HLTH:EX; Diacu, Mariana HLTH:EX
Cc: Prevost, Jean-Marc GCPE:EX; May, Stephen GCPE:EX
Subject: QA_LL_Nov 17 dr 1
Attachments: QA_LL_Nov 17 dr 1.docx

Hi Ian and Mariana,

With edits for approval.

Meribeth

Prevost, Jean-Marc GCPE:EX

From: Rongve, Ian HLTH:EX
Sent: November 18, 2019 12:27 PM
To: Prevost, Jean-Marc GCPE:EX; Burton, Meribeth GCPE:EX
Subject: MO has requested a LL update
Attachments: Document1.docx

MO has asked for an update on LL for QP ^{s.13}
attached. It is mostly from the QA document ^{s.13}

. Can you review the

Prevost, Jean-Marc GCPE:EX

From: Moulton, Holly HLTH:EX
Sent: November 18, 2019 1:11 PM
To: Prevost, Jean-Marc GCPE:EX; Rongve, Ian HLTH:EX
Subject: Revised LL KM and Q A.docx
Attachments: Revised LL KM and Q A.docx

Update Jean-Marc with more feedback from Ian.

Holly

Prevost, Jean-Marc GCPE:EX

From: Burton, Meribeth GCPE:EX
Sent: November 18, 2019 1:51 PM
To: Prevost, Jean-Marc GCPE:EX
Cc: May, Stephen GCPE:EX
Subject: FW: FOR HLTH REVIEW: QA on LL
Attachments: QA_LL_Nov 17 dr 1.docx

Importance: High

JMP

Can you revise?

You have edits from Ian.

Mb'

From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Sent: November 18, 2019 1:37 PM
To: Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>
Subject: FW: FOR HLTH REVIEW: QA on LL
Importance: High

Hi Meribeth

This was sent to Steve but doesn't seem to reflect the discussions this morning.

From: Moulton, Holly HLTH:EX <Holly.Moulton@gov.bc.ca>
Sent: November 18, 2019 1:27 PM
To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Subject: FW: FOR HLTH REVIEW: QA on LL
Importance: High

Can you please review.

From: Kot, Jill CITZ:EX <Jill.Kot@gov.bc.ca>
Sent: November 18, 2019 12:25 PM
To: Brown, Stephen R HLTH:EX <Stephen.Brown@gov.bc.ca>
Subject: FW: FOR HLTH REVIEW: QA on LL
Importance: High

Hi Stephen,

Here is the latest version of the Q and As being coordinated through our GCPE shops. ^{s.13}
s.13

Jill

From: Lauvaas, Kirsten GCPE:EX
Sent: November 17, 2019 5:05 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Cc: LeGuilloux, Marg GCPE:EX <Marg.LeGuilloux@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: FOR HLTH REVIEW: QA on LL
Importance: High

Hi Jean-Marc,

The attached Q&A has been through our information and privacy branch. A media statement will follow shortly – just want to ensure our DM sees it.

Please take a look and share this with your program folks. It has not yet been shared with Mariana and Ian.

Also – CIRMO confirms that in other data-breach situations in the past, it's always the ministry responsible/most affected that leads any government response. So in this case, HLTH should lead, with support from CITZ.

Thanks,
Kirsten

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: November 18, 2019 2:10 PM
To: Burton, Meribeth GCPE:EX
Subject: FW: revised as discussed
Attachments: Revised LL KM and Q & A.docx

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Prevost, Jean-Marc GCPE:EX
Sent: November 18, 2019 12:52 PM
To: Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: revised as discussed



Jean-Marc Prevost
COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: November 19, 2019 10:28 AM
To: Diacu, Mariana HLTH:EX; Rongve, Ian HLTH:EX
Cc: Lauvaas, Kirsten GCPE:EX; Burton, Meribeth GCPE:EX; May, Stephen GCPE:EX
Subject: RE: updated LL Q &A
Attachments: QA_LL_Nov 18 8 pm - IAN RONGVE EDITS - November 19.docx

It is here Mariana – I am working to clean up the tracks.

I will send the cleaned up copy to you once I have finished as well

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: November 19, 2019 10:25 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Cc: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Subject: RE: updated LL Q &A

I don't seem to have received a copy – would you be able to re-send? Thank you.

Best wishes,

Mariana

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: November 19, 2019 9:53 AM
To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Cc: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: RE: updated LL Q &A

Can you send me the version you made changes to Ian – the one we reviewed together this morning.

I will clean up as we discussed.

Thanks,

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>

Sent: November 18, 2019 7:46 PM

To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>

Cc: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>

Subject: Re: updated LL Q &A

Thanks Jean-Marc. Will review

Sent from my iPhone

On Nov 18, 2019, at 7:40 PM, Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca> wrote:

Hi Ian and Kirsten,

I have updated this Q & A doc based on discussions we had this morning ... and on new information we got on the call this afternoon (including the RCMP notification).

My changes are tracked. Please review and let me know of any concerns or suggestions at your earliest.

Thanks!

<image001.png>

Jean-Marc Prevost

COMMUNICATIONS DIRECTOR

Desk: 236-478-0302

Cell: 250-886-2154

<QA_LL_Nov 18 8 pm (jmp edits).docx>

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: November 19, 2019 1:27 PM
To: Rongve, Ian HLTH:EX; Carroll, Scott CITZ:EX
Cc: Prevost, Jean-Marc GCPE:EX
Subject: FW: LifeLabs - Ontario

FYI - Please note that Ontario is waiting for LL to discuss their approach with the privacy commissioner.

Best wishes,

Mariana

-----Original Message-----

From: Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Sent: November 19, 2019 12:31 PM
To: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: RE: LifeLabs

Hi Mariana,

We had a conversation with LifeLabs today and are waiting for them to discuss their approach with the privacy commissioner. We are waiting to get confirmation on their planned communications approach before taking action.

Neeta

Prevost, Jean-Marc GCPE:EX

From: Pearce, Alison HLTH:EX
Sent: November 19, 2019 5:42 PM
To: Aitken, Jeff HLTH:EX; XT:Bayne, James HLTH:IN; Carroll, Scott CITZ:EX
Cc: Shrimpton, Paul HLTH:EX; Diacu, Mariana HLTH:EX; Lauvaas, Kirsten GCPE:EX; Prevost, Jean-Marc GCPE:EX
Subject: FW: Cyber Security
Attachments: LL- Cybersecurity v2.docx

Good evening, gentlemen. I have added to and made some edits to Gary's draft cybersecurity note.

Jeff, Corrie has provided the context for you below.

James, go ahead and fill out the HA section.

Scott, just in case you have any other thoughts.

Can you provide your edits back to me and I'll pull it all together for Corrie for tomorrow at 3 pm?

I will cc the same group above with the final.

Thanks,
Alison

From: Corrie Barclay <Corrie.Barclay@gov.bc.ca>
Date: Tuesday, November 19, 2019 at 5:21 PM
To: "Pearce, Alison HLTH:EX" <Alison.Pearce@gov.bc.ca>, "Aitken, Jeff HLTH:EX" <Jeff.Aitken@gov.bc.ca>
Cc: "Lauvaas, Kirsten GCPE:EX" <Kirsten.Lauvaas@gov.bc.ca>, "Shrimpton, Paul HLTH:EX" <Paul.Shrimpton@gov.bc.ca>
Subject: FW: Cyber Security

Hi Alison and Jeff

Alison, can you please brief Jeff on the attached. Please review and add comments, track changes.

For Life Lab section, please add what has been done that you are aware of from PHSA and how this has helped to address the risk and increase confidence.

For the MOH section, can you please add some key messages on how we ensure the protection of our Ministry of health Systems that contain personal health information. Also, can you add an appendix with lists all the health system the Ministry is accountable for that contain personal health information with more detail on how we ensure the security of these systems.

For HA section, please add key messages.

Can you get this to my by tomorrow at 3:00?

Corrie

From: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>
Sent: November 19, 2019 3:53 PM
To: Barclay, Corrie A HLTH:EX <Corrie.Barcly@gov.bc.ca>; Pearce, Alison HLTH:EX <Alison.Pearce@gov.bc.ca>
Cc: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Subject: RE: Cyber Security

Good afternoon,

I went back through all our previous materials for security messaging and brought those bullets forward here.

s.13

Please note I will be on and off the stage from 8 am until 4:30 or later tomorrow.

Regards,

Gary Perkins

Executive Director, Chief Information Security Officer (CISO)
Information Security Branch
Office of the Chief Information Officer
Gary.Perkins@gov.bc.ca
250-387-7590



This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender. Any unauthorized copying, disclosure or distribution of the e-mail or the information it contains, is strictly forbidden.

-----Original Appointment-----

From: Pokorny, Peter HLTH:EX <Peter.Pokorny@gov.bc.ca>
Sent: November 19, 2019 1:23 PM
To: Pokorny, Peter HLTH:EX; Barclay, Corrie A HLTH:EX; Shrimpton, Paul HLTH:EX; Rongve, Ian HLTH:EX; Perkins, Gary CITZ:EX
Subject: Cyber Security
When: November 19, 2019 1:45 PM-2:00 PM (UTC-08:00) Pacific Time (US & Canada).
Where: T/C - Please call Peter Pokorny 250 952-1779
Importance: High

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: November 20, 2019 12:56 PM
To: Prevost, Jean-Marc GCPE:EX
Cc: LeGuilloux, Marg GCPE:EX; Marriott, Sarah GCPE:EX
Subject: FW: Incident Timeline 2019-2248
Attachments: Incident Timeline 2019-2248.docx

Hi All,

Here is the incident timeline (from day LL found out about the breach to today). This is quite detailed, so we may want to simplify or make this more of an infographic for ease of viewing. If you have any questions/comments, please track them in the attached and I'll forward them back to the CITZ team.

Thanks,

Kirsten

From: Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>
Sent: November 19, 2019 6:21 PM
To: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>; Donaldson, Ian R CITZ:EX <Ian.Donaldson@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Avery, Ainslie CITZ:EX <Ainslie.Avery@gov.bc.ca>
Subject: Incident Timeline 2019-2248

Hi all,

There were a few requests for this, so looking to consolidate the communications efforts here. Attached is the timeline of the incident as it has unfolded.

If you have any questions or comments, please reply-all and PCT will make changes. Otherwise, to ensure that we are aligned, can I ask that this go to CJ/Jill/the MO through Kerry only.

Thanks,
-m

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: November 20, 2019 4:59 PM
To: Barclay, Corrie A HLTH:EX
Subject: FW: updated Q & A LL
Attachments: QA_LL_Nov 20 9am (jmp) SC.docx

FYI ... I will be updating this again following this call

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: November 20, 2019 1:56 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: FW: updated Q & A LL

Hello:

I spoke to LL today for a significant amount of time. There were concerns on their end in regards to the areas I flagged with questions. We should discuss these at 2.

Thanks
Scott

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: November 20, 2019 1:27 PM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Subject: RE: updated Q & A LL

Thanks very much Scott – do you think we could get these before 3 pm.?

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: November 20, 2019 10:34 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: RE: updated Q & A LL

I have reviewed and added to this. I will send this to my contacts in my branch now, I should have this back shortly.

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>

Sent: November 20, 2019 9:35 AM

To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>

Cc: Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>

Subject: updated Q & A LL

Hi all,

I have updated this Q & A significantly given the developments we learned yesterday afternoon.

In the tracks you will see I have two outstanding questions ... one for Health one for CITZ.



Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Barclay, Corrie A HLTH:EX
Sent: November 20, 2019 5:16 PM
To: Prevost, Jean-Marc GCPE:EX; Carroll, Scott CITZ:EX
Cc: Rongye, Ian HLTH:EX; Pearce, Alison HLTH:EX
Subject: LL Security Issue - Draft
Attachments: LL Security Issue.docx

Hi there,

Attached is a very quick draft, your feedback and comments are welcome. We are to get something to Peter tonight so your quick feedback is appreciated.

Corrie

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: November 21, 2019 10:30 AM
To: Prevost, Jean-Marc GCPE:EX
Subject: Updates
Attachments: QA_LL_Nov 20 .docx

Hi Jean-Marc,

I have just noticed that my email with suggestions for change didn't leave my inbox. Please note there are a few updates
s.13


Best wishes,

Mariana

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: November 22, 2019 4:57 PM
To: LeGuilloux, Marg GCPE:EX
Subject: Fwd: updated Q & A
Attachments: image001.png; ATT00001.htm; QA_LL_Nov 22 5pm (jmp).docx; ATT00002.htm

Jean-Marc Prevost

 250-886-2154

Begin forwarded message:

From: "Prevost, Jean-Marc GCPE:EX" <Jean-Marc.Prevost@gov.bc.ca>
Date: November 22, 2019 at 4:49:00 PM PST
To: "Rongve, Ian HLTH:EX" <Ian.Rongve@gov.bc.ca>, "Barclay, Corrie A HLTH:EX" <Corrie.Barclay@gov.bc.ca>, "Lauvaas, Kirsten GCPE:EX" <Kirsten.Lauvaas@gov.bc.ca>
Cc: "Carroll, Scott CITZ:EX" <Scott.Carroll@gov.bc.ca>, "Diacu, Mariana HLTH:EX" <Mariana.Diacu@gov.bc.ca>, "Marriott, Sarah GCPE:EX" <Sarah.Marriott@gov.bc.ca>, "Burton, Meribeth GCPE:EX (Meribeth.Burton@gov.bc.ca)" <Meribeth.Burton@gov.bc.ca>, "May, Stephen GCPE:EX" <Stephen.May@gov.bc.ca>
Subject: updated Q & A

These are updated following today's call.

As there are still moving pieces – they are still draft.

I have left Scott's comments on to remind myself of where we are hoping for new data or confirmations to come in.

Please let the group know of concerns or suggestions.

Thanks!

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: November 26, 2019 12:01 PM
To: Carroll, Scott CITZ:EX; Rongve, Ian HLTH:EX; Barclay, Corrie A HLTH:EX; Lauvaas, Kirsten GCPE:EX
Cc: Marriott, Sarah GCPE:EX; Diacu, Mariana HLTH:EX; May, Stephen GCPE:EX; Burton, Meribeth GCPE:EX (Meribeth.Burton@gov.bc.ca)
Subject: Latest Q & A on LifeLabs
Attachments: QA_LL_Nov 26 12pm (jmp).docx

... following our two calls yesterday.



Ministry of
Health

Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: November 26, 2019 2:58 PM
To: May, Stephen GCPE:EX; Burton, Meribeth GCPE:EX (Meribeth.Burton@gov.bc.ca)
Subject: LifeLabs on the LAN
Attachments: QA_LL_Nov 26 12pm (jmp).docx

Hi SM,

Scott Carroll and Ian have both come back to me with no changes (for now).

Could you please find a spot for this to live on the LAN?



Jean-Marc Prevost
COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: November 27, 2019 6:40 AM
To: Carroll, Scott CITZ:EX
Cc: Prevost, Jean-Marc GCPE:EX
Subject: Re: UPDATE - Privacy Incident 2019-2248

Sounds good, Scott. We can have an update call once your other meeting is over. Call my cell if you need to talk before then.

Thanks!

Kirsten Lauvaas
250 213-5572
Sent from my iPhone

On Nov 26, 2019, at 9:42 PM, Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca> wrote:

The call had not been set. Potentially at ten tomorrow. I will be connecting with LL before then to discuss what will be presented. You can reach me on my cell any time after 7 tomorrow. I can always fill you in after the call at ten as well. I don't think it will be too late if we connect after. I imagine the call will just inform the OIPC of the new findings and a date will be set potentially for the notification.

Sent from my iPhone

On Nov 26, 2019, at 9:13 PM, Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca> wrote:

Let's get on a call together in the morning. What time works for you? I am booked through 10am but that may be too late. Can adjust my schedule if needed.

Kirsten Lauvaas
250 213-5572
Sent from my iPhone

On Nov 26, 2019, at 8:38 PM, Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca> wrote:

Below is the update from today. You will note a fairly significant update at the end of the summary that occurred at the very end of the day today, after the regular check in call. Let's connect tomorrow morning (or when you are free) to discuss this.

LifeLabs Incident Update (November 26)

● s.13; s.14

- A copy of governments communication plan (Q&A doc) was sent to LifeLabs for their review to ensure the accuracy of the information. LifeLabs were requested to provide their feedback by the end of the week.
- LifeLabs confirmed that they had no new information or updates to provide at this time. The date for their public notification is still undecided as is their timeline for the completion of their technical review/security fixes.
- LifeLabs were asked when they intend to provide their next briefing to the OIPC. Their initial response was that they intend to contact them in the next 24-48 hours to brief them.
- s.3

•

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

Government confidentiality and privilege requirements apply to this message and any attachments. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use is strictly prohibited. If you are not the intended recipient, please notify the sender immediately, and delete this message and any attachments from both your inbox and deleted items folder. Thank You.

Prevost, Jean-Marc GCPE:EX

From: Marshall, Thomas <Thomas.Marshall@lifelabs.com>
Sent: November 29, 2019 11:54 AM
To: Carroll, Scott CITZ:EX
Cc: Prevost, Jean-Marc GCPE:EX; Lauvaas, Kirsten GCPE:EX; Dent, Ashley; Cudlipp, Jennifer
Subject: [Contents Not Virus Scanned] RE: Communication Material
Attachments: QA_LL_Nov_29_Feedback.DOCX

Hi Scott,

See attached for our feedback.

Sorry for the delay. I got pulled into a meeting.

-Thomas

Thomas Marshall

Director Government Relations

LifeLabs | 3680 Gilmore Way | Burnaby, BC V5G 4V8

T 778-372-2079 | C 604-312-8519

E Thomas.Marshall@LifeLabs.com

www.LifeLabs.com



From: Carroll, Scott CITZ:EX [mailto:Scott.Carroll@gov.bc.ca]
Sent: Friday, November 29, 2019 9:54 AM
To: Marshall, Thomas <Thomas.Marshall@lifelabs.com>
Cc: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Subject: RE: Communication Material

Just email it to me and I will share it out.

Thanks,
Scott

From: Marshall, Thomas <Thomas.Marshall@lifelabs.com>
Sent: November 29, 2019 9:53 AM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Cc: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Subject: RE: Communication Material

It's ready to go. How do you want to receive it?

Thomas Marshall

Director Government Relations

LifeLabs | 3680 Gilmore Way | Burnaby, BC V5G 4V8

T 778-372-2079 | C 604-312-8519

E Thomas.Marshall@LifeLabs.com

www.LifeLabs.com



From: Carroll, Scott CITZ:EX [<mailto:Scott.Carroll@gov.bc.ca>]

Sent: Friday, November 29, 2019 9:51 AM

To: Marshall, Thomas <Thomas.Marshall@lifelabs.com>

Cc: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>

Subject: Communication Material

Hello Thomas:

You mentioned we would have this back this morning. I know several areas are waiting on this, please confirm/send as soon as possible as we will have some work to do that we need to turn around quickly on this.

Thanks,

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

Government confidentiality and privilege requirements apply to this message and any attachments. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use is strictly prohibited. If you are not the intended recipient, please notify the sender immediately, and delete this message and any attachments from both your inbox and deleted items folder. Thank You.

The information in this e-mail and any attachments is confidential and for the sole use of the intended recipient(s). If you have received this e-mail in error, please: accept our apologies for the inconvenience; note that any use of the information is strictly prohibited; notify the sender as soon as possible; and then delete all copies from your system.

Le contenu de ce message ainsi que du ou des fichiers qui y sont joints est strictement confidentiel et destine exclusivement a son ou sa destinataire. Si vous avez reçu ce courriel par erreur, veuillez en aviser l'expediteur des que possible et supprimer le courriel de votre ordinateur, son utilisation etant strictement interdite. Nous sommes desoles pour tout inconvenient que cette situation aurait pu vous occasionner.

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: November 29, 2019 4:09 PM
To: Carroll, Scott CITZ:EX; Lauvaas, Kirsten GCPE:EX
Subject: RE: changes incorporated
Attachments: LL KM Q & A (FINAL) Nov 29 4pm.docx

Good catches.

Corrected in attached

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: November 29, 2019 4:00 PM
To: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: RE: changes incorporated

s.13

- LifeLabs undertakes about 40% of diagnostic testing in B.C. with about three million clients

From: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Sent: November 29, 2019 3:46 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Subject: RE: changes incorporated

I like it. Thanks, Jean-Marc.

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: November 29, 2019 3:44 PM
To: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Subject: changes incorporated

I mostly accepted the changes and cleaned up the formatting.

I also changed three bullets as below.

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs delayed public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.
- We understand that plan includes call centres for clients to contact, where they can receive further information and as well as free identify theft insurance and dark web monitoring services.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: November 29, 2019 4:16 PM
To: May, Stephen GCPE:EX; Burton, Meribeth GCPE:EX (Meribeth.Burton@gov.bc.ca)
Subject: UPDATE: LifeLabs on the LAN
Attachments: LL KM Q & A (FINAL) Nov 29 4pm.docx

This has now been signed off with LL as well.

We can replace what is on the LAN with this version.

Thanks.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Prevost, Jean-Marc GCPE:EX
Sent: November 26, 2019 2:58 PM
To: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Burton, Meribeth GCPE:EX (Meribeth.Burton@gov.bc.ca) <Meribeth.Burton@gov.bc.ca>
Subject: LifeLabs on the LAN

Hi SM,

Scott Carroll and Ian have both come back to me with no changes (for now).

Could you please find a spot for this to live on the LAN?



Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Burton, Meribeth GCPE:EX
Sent: November 29, 2019 4:44 PM
To: Prevost, Jean-Marc GCPE:EX
Subject: LL KM Q A (FINAL) Nov 29 4pm
Attachments: LL KM Q A (FINAL) Nov 29 4pm.docx

Some suggested edits for KMs.

Meribeth

Prevost, Jean-Marc GCPE:EX

From: Reed, Matt CITZ:EX
Sent: November 29, 2019 6:44 PM
To: Prevost, Jean-Marc GCPE:EX; Lauvaas, Kirsten GCPE:EX
Cc: Carroll, Scott CITZ:EX; Avery, Ainslie CITZ:EX
Subject: Incident QA doc
Attachments: LL KM Q A (FINAL) Nov 29 SC.docx

Hi Jean-Marc,

I have had a review of the QA doc that the team has produced, as I understand it, this is meant to route now through you, and then to Ian R.

Can you please include those on this chain in either any changes, or once you are okay with this as is. One of our priorities (aside from getting the right messaging) is to ensure that everyone is aligned – which has been challenging on this file.

If you and Ian are okay with this draft (with the addition of one piece that is missing – but flagged), then Scott can coordinate this draft reaching everyone.

Thanks – and let me know if you have any questions or concerns.

-m

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 3, 2019 4:54 PM
To: james.slater@phsa.ca; XT:Bayne, James HLTH:IN
Subject: FW: LL KM Q&A
Attachments: LL KM Q A Dec 2.docx

As discussed

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Prevost, Jean-Marc GCPE:EX
Sent: December 2, 2019 9:26 AM
To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barclay@gov.bc.ca>
Cc: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Avery, Ainslie CITZ:EX <Ainslie.Avery@gov.bc.ca>; Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Subject: LL KM Q&A

Ian and Corrie,

This has now been through LL, as well as Matt and Avery at CITZ.

Please let us know if you have any concerns or suggestions.

This should be very close to final ...

Thx

J M P

Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 9, 2019 2:53 PM
To: Marriott, Sarah GCPE:EX; Russell, Shannon CITZ:EX
Cc: Lauvaas, Kirsten GCPE:EX
Subject: RE: Updated: LL KM Q A Dec 2
Attachments: LL KM Q A Dec 9.docx

This is the latest – and is clean.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Sent: December 9, 2019 2:31 PM
To: Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>
Cc: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Subject: Fwd: Updated: LL KM Q A Dec 2

Shannon,

Jean-Marc might be able to get you a clean version, but if you delete the below bullet everywhere in the doc, the attached is the most up to date version.

- 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.

Sent from my iPhone

Begin forwarded message:

From: "Lauvaas, Kirsten GCPE:EX" <Kirsten.Lauvaas@gov.bc.ca>
Date: December 3, 2019 at 12:12:46 PM PST
To: "LeGuilloux, Marg GCPE:EX" <Marg.LeGuilloux@gov.bc.ca>, "Marriott, Sarah GCPE:EX" <Sarah.Marriott@gov.bc.ca>
Subject: Updated: LL KM Q A Dec 2

Hi Both,

The attached is nearly final – just needs a couple of pieces added (URL from LL once their site is ready). I will share this version with my MO as well. Jean-Marc has shared with his DM and it sounds like his DM will brief up to his MO.

Still driving towards Dec. 17, but that could change.

Kirsten

Prevost, Jean-Marc GCPE:EX

From: Rongve, Ian HLTH:EX
Sent: December 10, 2019 6:54 AM
To: Prevost, Jean-Marc GCPE:EX
Subject: LL KM Q A Dec 9 (ir)
Attachments: LL KM Q A Dec 9 (ir).docx

My comments. Only two substantive. Clarification on whether LL has an hospital data and a question about identity theft protection.

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 10, 2019 11:46 AM
To: Rongve, Ian HLTH:EX; Barclay, Corrie A HLTH:EX
Subject: RE: Ministers briefing
Attachments: LL KM Q A Dec 10 FINAL.docx

Thanks Ian.

Here is the final Q & A doc back, with you edits saved down.

Shall I share with MO and DMO – or do you prefer to hold all material for this?

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Sent: December 10, 2019 11:17 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barcly@gov.bc.ca>
Subject: Fwd: Ministers briefing

Steve is looking to have a ministers briefing on LL likely on Monday.

Sent from my iPhone

Begin forwarded message:

From: "Schuster, Michelle M HLTH:EX" <Michelle.Schuster@gov.bc.ca>
Date: December 10, 2019 at 1:59:49 PM EST
To: "Rongve, Ian HLTH:EX" <Ian.Rongve@gov.bc.ca>
Subject: RE: Ministers briefing

For sure!

-----Original Message-----

From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Sent: December 10, 2019 10:56 AM
To: Schuster, Michelle M HLTH:EX <Michelle.Schuster@gov.bc.ca>
Subject: Ministers briefing

Can you work with dmo to get a ministers briefing on LL. Probably Monday.

Sent from my iPhone

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 10, 2019 11:50 AM
To: Burton, Meribeth GCPE:EX (Meribeth.Burton@gov.bc.ca); May, Stephen GCPE:EX
Subject: LL on the LAN
Attachments: LL KM Q A Dec 10 FINAL.docx

Stephen could you please create a place on the LAN for this to live?

We are considering it final now.

Note below that DMO is planning to brief MO Monday.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Prevost, Jean-Marc GCPE:EX
Sent: December 10, 2019 11:46 AM
To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barcly@gov.bc.ca>
Subject: RE: Ministers briefing

Thanks Ian.

Here is the final Q & A doc back, with you edits saved down.

Shall I share with MO and DMO – or do you prefer to hold all material for this?

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Sent: December 10, 2019 11:17 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barcly@gov.bc.ca>
Subject: Fwd: Ministers briefing

Steve is looking to have a ministers briefing on LL likely on Monday.

Sent from my iPhone

Begin forwarded message:

From: "Schuster, Michelle M HLTH:EX" <Michelle.Schuster@gov.bc.ca>
Date: December 10, 2019 at 1:59:49 PM EST

To: "Rongve, Ian HLTH:EX" <Ian.Rongve@gov.bc.ca>

Subject: RE: Ministers briefing

For sure!

-----Original Message-----

From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>

Sent: December 10, 2019 10:56 AM

To: Schuster, Michelle M HLTH:EX <Michelle.Schuster@gov.bc.ca>

Subject: Ministers briefing

Can you work with dmo to get a ministers briefing on LL. Probably Monday.

Sent from my iPhone

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 10, 2019 11:55 AM
To: Lauvaas, Kirsten GCPE:EX; Russell, Shannon CITZ:EX; Marriott, Sarah GCPE:EX
Subject: RE: LL FINAL
Attachments: LL KM Q A Dec 10 FINAL.docx

Here it is without tracks.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Sent: December 10, 2019 11:43 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: RE: LL FINAL

Thanks, Jean-Marc.

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 10, 2019 11:41 AM
To: Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Cc: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Subject: LL FINAL

This is approved from Health program area.

Health DM plans to brief Health MO sometime Monday Dec. 16.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 10, 2019 12:02 PM
To: Moulton, Holly HLTH:EX
Cc: Rongve, Ian HLTH:EX
Subject: LL Q&A for review
Attachments: LL KM Q A Dec 10 FINAL.docx

Hi Holly –

Pls see attached for DM's review.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 10, 2019 1:36 PM
To: Diacu, Mariana HLTH:EX
Subject: LL KM Q A Dec 10 FINAL.docx
Attachments: LL KM Q A Dec 10 FINAL.docx; ATT00001.htm

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: December 10, 2019 1:37 PM
To: Prevost, Jean-Marc GCPE:EX
Subject: FW: LL letter

As discussed

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: December 10, 2019 1:09 PM
To: Patterson, Catherine M HLTH:EX <Catherine.Patterson@gov.bc.ca>
Cc: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: LL letter

Hi Catherine,
Here is the letter we discussed - thanks.

s.13

Page 058 of 358

Withheld pursuant to/removed as

s.13

Prevost, Jean-Marc GCPE:EX

From: Barclay, Corrie A HLTH:EX
Sent: December 10, 2019 2:58 PM
To: Prevost, Jean-Marc GCPE:EX; Rongve, Ian HLTH:EX
Cc: Diacu, Mariana HLTH:EX
Subject: RE: Latest LL Q & A

Thank you, looks good to me. I will pass along quickly to my security team and will let you know if there is any required edits.

Corrie

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 9, 2019 3:04 PM
To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Barclay, Corrie A HLTH:EX <Corrie.Barcly@gov.bc.ca>
Cc: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: Latest LL Q & A

Hi Ian and Corrie,

This is the latest version of the Q & A that I have been regularly updating following our daily calls.

CITZ is particularly earnest that it be made final – as their DM wants to use it in briefing their MO.

I have attached my latest draft, and highlighted the only changes I've added since the last time you saw it (in the attachment and below).

Please let me know if you have any concerns or suggestions.

Thanks,



Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

- More than 60% of British Columbian's lab tests happen in hospitals, and that information stays within Health Authorities' systems – which are separate from LifeLabs systems.

The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of lab testing services for British Columbians outside a hospital setting (about 40% of all lab tests in the province).
- For some time, the Province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- This process changed to a service provision agreement with LifeLabs, to help with cost certainty in budgeting for those services.
- 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.

What does the Ministry do to enforce these protections/policies?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor 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 specific incident are still being determined, based on our agreement with LifeLabs.

Prevost, Jean-Marc GCPE:EX

From: Carroll, Scott CITZ:EX
Sent: December 12, 2019 3:19 PM
To: Lauvaas, Kirsten GCPE:EX; Emerson, Kim GCPE:EX; Prevost, Jean-Marc GCPE:EX
Subject: RE: #19902758-v1-PRIVILEGED_AND_CONFIDENTIAL_PEGASUS_-_FAQ_Dec_11 SC

Just so you are aware. This was the feedback from the OIPC^{s.3}
if they will be incorporating this feedback or not.

We will discuss with LL today

s.3

From: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Sent: December 12, 2019 3:06 PM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Emerson, Kim GCPE:EX <Kim.Emerson@gov.bc.ca>
Subject: #19902758-v1-PRIVILEGED_AND_CONFIDENTIAL_PEGASUS_-_FAQ_Dec_11 SC

Hi Scott,

Thanks for this. I've made a few additional edits but this covers our areas of concern/additional Qs as well.

Kirsten

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: December 12, 2019 5:05 PM
To: Prevost, Jean-Marc GCPE:EX; Marriott, Sarah GCPE:EX
Subject: LL Statement Nov 18 dr 1
Attachments: LL Statement Nov 18 dr 1.docx

For discussion – we will work on updating this. Now know LL and OIPC are releasing public statements on Dec. 17th. Suggest Gov put something out – short and sweet – following shortly after LL sends theirs out. Gets us on the record along with the others.

Free for a chat tomorrow morning?

Kirsten

Prevost, Jean-Marc GCPE:EX

From: May, Stephen GCPE:EX
Sent: December 13, 2019 7:58 AM
To: Prevost, Jean-Marc GCPE:EX
Cc: Burton, Meribeth GCPE:EX; Marriott, Sarah GCPE:EX
Subject: RE: frontline messaging
Attachments: draft frontline KMs_LL.docx

Added some messaging around the service agreements.

From: May, Stephen GCPE:EX
Sent: December 13, 2019 7:42 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Cc: Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: RE: frontline messaging

It's solid – high level. The only thing potentially missing (as I could see it being asked) – is concerns around Lifelabs service agreement with Health and whether this would affect it.

Also fixed a misplaced apostrophe.

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 12, 2019 11:24 PM
To: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Cc: Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: frontline messaging

Hi Stephen May,

Some LL developments late this afternoon.

I have made a very rough cut down of messaging we can provide Health Authorities to share with their staff next week.

Pls have a look ... hoping we can discuss tomorrow morning.

Thanks very much.



Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 13, 2019 8:18 AM
To: May, Stephen GCPE:EX
Subject: FYI
Attachments: FW: LL letter; RE: #19902758-v1-PRIVILEGED_AND_CONFIDENTIAL_PEGASUS_-_FAQ_Dec_11 SC



Ministry of
Health

Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 13, 2019 2:31 PM
To: van Baarsen, Amanda HLTH:EX
Subject: LL KM Q A Dec 10 FINAL
Attachments: LL KM Q A Dec 10 FINAL.docx

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: December 13, 2019 4:51 PM
To: Prevost, Jean-Marc GCPE:EX
Subject: Fwd: LL dec 12 update
Attachments: LL december 12 update.docx; ATT00001.htm

This is the update Ian sent to the deputy

Sent from my iPhone

Begin forwarded message:

From: "Diacu, Mariana HLTH:EX" <Mariana.Diacu@gov.bc.ca>
Date: December 12, 2019 at 11:17:37 PM PST
To: "Rongve, Ian HLTH:EX" <Ian.Rongve@gov.bc.ca>
Cc: "Watt, Rebecca HLTH:EX" <Rebecca.Watt@gov.bc.ca>, "Diacu, Mariana HLTH:EX" <Mariana.Diacu@gov.bc.ca>
Subject: LL dec 12 update

Prevost, Jean-Marc GCPE:EX

From: Carroll, Scott CITZ:EX
Sent: December 13, 2019 5:26 PM
To: Marriott, Sarah GCPE:EX; May, Stephen GCPE:EX; Prevost, Jean-Marc GCPE:EX
Cc: Burton, Meribeth GCPE:EX
Subject: RE: frontline messaging
Attachments: Statement_LL Privacy Brach_Dec 13_sm (002).docx

Looks good. One small addition, however, ^{s.13}

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Sent: December 13, 2019 4:22 PM
To: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Cc: Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Subject: RE: frontline messaging

Tim and my edits. Happy to discuss.

Sarah

Sarah Marriott
Issues Manager
250.361.8416

From: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Sent: December 13, 2019 2:10 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Cc: Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Subject: RE: frontline messaging

Looping in Scott as well.

First cut at this.

Stephen May
GCPE-Health
P: 250 952 3401
C: 250 888 9879

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: December 13, 2019 5:59 PM
To: Prevost, Jean-Marc GCPE:EX
Subject: Statement_LL Privacy Brach_Dec 13_sm
Attachments: Statement_LL Privacy Brach_Dec 13_sm.docx

Made a few edits to the attached.

Just for clarity, this came to you from Sarah or from Tim?

Thanks,
Kirsten

Prevost, Jean-Marc GCPE: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.

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 16, 2019 8:53 AM
To: Diacu, Mariana HLTH:EX
Subject: draft frontline KMs_LL
Attachments: draft frontline KMs_LL.docx

J M P

Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: December 16, 2019 8:53 AM
To: Prevost, Jean-Marc GCPE:EX; Marriott, Sarah GCPE:EX
Cc: LeGuilloux, Marg GCPE:EX
Subject: Fwd: LL KM Q A Dec 16
Attachments: LL KM Q A Dec 16.docx; ATT00001.htm

Hi Jean-Marc,

Here is our updated Q&A. We may have a few edits after a 9:30 meeting this morning, but the attached builds out the timeline for the issue and addresses a few items around the Personal Information Protection Act that could come up.

Understand HLTH may be circulating something similar so this will help with alignment.

We will share any updates following our meeting. Would be good to share the Statement with my team as well.

Cheers,

Kirsten Lauvaas
250 213-5572
Sent from my iPhone

Begin forwarded message:

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 16, 2019 12:40 PM
To: Diacu, Mariana HLTH:EX
Subject: RE: 1 pager for internal staff
Attachments: latest LL products

So sorry Mariana

Should have sent this to you an hour ago.

Got tied up

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: December 16, 2019 12:39 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: FW: 1 pager for internal staff

Hi Jean-Mark,

We are all on stand-by for the Q&As for tomorrow – any updates from your end? Thanks.

Best wishes,

Mariana

From: Pearce, Alison HLTH:EX <Alison.Pearce@gov.bc.ca>
Sent: December 16, 2019 9:19 AM
To: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Cc: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; XT:Bayne, James HLTH:IN <James.Bayne@phsa.ca>
Subject: 1 pager for internal staff

Hi Mariana. Do you have an eta on an 1 pager of messaging for internal staff for tomorrow am?

A

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 16, 2019 12:45 PM
To: van Baarsen, Amanda HLTH:EX
Subject: FW: LL december 16 update
Attachments: LL december 16 update v.2.docx

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: December 16, 2019 8:47 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: FW: LL december 16 update

Best wishes,

Mariana

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: December 15, 2019 5:15 PM
To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Cc: Watt, Rebecca HLTH:EX <Rebecca.Watt@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: Re: LL december 16 update

Updated document with Scott's comments. Thomas cannot release the number of impacted patients at this time.

From: Rongve, Ian HLTH:EX
Sent: Sunday, December 15, 2019 2:41 PM
To: Diacu, Mariana HLTH:EX
Cc: Watt, Rebecca HLTH:EX
Subject: Re: LL december 16 update

Thank you.

Sent from my iPhone

On Dec 15, 2019, at 2:24 PM, Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca> wrote:

I sent it to him and he committed to review later today.

From: Rongve, Ian HLTH:EX
Sent: Sunday, December 15, 2019 2:16 PM
To: Diacu, Mariana HLTH:EX
Cc: Watt, Rebecca HLTH:EX
Subject: Re: LL december 16 update

This looks really good Mariana. Has Scott seen it?

Sent from my iPhone

On Dec 15, 2019, at 2:11 PM, Diacu, Mariana HLTH:EX
<Mariana.Diacu@gov.bc.ca> wrote:

Hi Ian,

Sending you an updated version by not final. I am waiting to hear back from Thomas who will provide a one sentence re: number of BC patients impacted by the breach and from Scott who promised to review the whole note later on today.

I thought though, you may want to review and provide feedback before finalizing.

PS: I have not changed the date of the document yet until it is finalized.

Mariana

From: Rongve, Ian HLTH:EX
Sent: Sunday, December 15, 2019 10:13 AM
To: Diacu, Mariana HLTH:EX
Cc: Watt, Rebecca HLTH:EX
Subject: Re: LL december 16 update

Thanks. Build the security into the last bit on the existing contract please.

Sent from my iPhone

On Dec 15, 2019, at 10:10 AM, Diacu, Mariana HLTH:EX
<Mariana.Diacu@gov.bc.ca> wrote:

on it, including the security paragraph.

From: Rongve, Ian HLTH:EX
Sent: Saturday, December 14, 2019 11:17 AM
To: Diacu, Mariana HLTH:EX; Watt, Rebecca HLTH:EX
Subject: LL december 16 update

Hi. I updated the note you produced Thursday mariana. Can you review and edit as appropriate. Once you have had a run I will send to Scott for comments as well

<LL december 16 update.docx>

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: December 16, 2019 1:46 PM
To: Marriott, Sarah GCPE:EX; Prevost, Jean-Marc GCPE:EX
Subject: generic LL statement
Attachments: generic LL statement (jmp)_sm.docx

FYI this version is currently with my ADM and her team for review.

Kirsten

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: December 16, 2019 1:52 PM
To: Prevost, Jean-Marc GCPE:EX; Marriott, Sarah GCPE:EX
Subject: Speaking Points for health authority staff
Attachments: Speaking Points for health authority staff.docx

Hi J-M,

Need me to run this past anyone on my side? I've made some edits in the attached.

K

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: December 16, 2019 2:00 PM
To: Marriott, Sarah GCPE:EX; Prevost, Jean-Marc GCPE:EX; Carroll, Scott CITZ:EX; Lauvaas, Kirsten GCPE:EX
Cc: Rongve, Ian HLTH:EX
Subject: RE: latest LL products
Attachments: Speaking Points for health authority staff.docx

Please see my comments and the suggested language which aligns with the HSIAR data.

Best wishes,

Mariana

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Sent: December 16, 2019 1:51 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: RE: latest LL products

My edits attached. Otherwise works for me, provided it suits others.

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 16, 2019 1:46 PM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: FW: latest LL products

For review

This is what PHSA is suggesting for frontline staff messaging

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Dawkins, Laurie <laurie.dawkins@phsa.ca>
Sent: December 16, 2019 1:44 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: RE: latest LL products

As discussed, for your consideration. I think this is an additional resource the health authorities would appreciate.

From: Prevost, Jean-Marc GCPE:EX [<mailto:Jean-Marc.Prevost@gov.bc.ca>]
Sent: Monday, December 16, 2019 10:42 AM
To: Dawkins, Laurie <laurie.dawkins@phsa.ca>
Subject: FW: latest LL products
Importance: High

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Prevost, Jean-Marc GCPE:EX
Sent: December 16, 2019 10:40 AM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>
Subject: latest LL products
Importance: High

Media statement
Cutdown Q&A and KM (for sharing with Health Authorities)
Long form Q & A (updates from CITZ as of this morning)

J M P

Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: December 16, 2019 2:56 PM
To: Prevost, Jean-Marc GCPE:EX
Subject: FW: LifeLabs

Best wishes,

Mariana

From: Szymczak, Marysia (MOHLTC) <Marysia.Szymczak@ontario.ca>
Sent: December 16, 2019 2:50 PM
To: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Subject: Re: LifeLabs

Hi - we will not be issuing a statement. Comms approach will be reactive.

Please let me know if you have any questions.

Best
Marysia

Get [Outlook for iOS](#)

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: Monday, December 16, 2019 11:46:28 AM
To: Szymczak, Marysia (MOHLTC) <Marysia.Szymczak@ontario.ca>; Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Subject: RE: LifeLabs

CAUTION -- EXTERNAL E-MAIL - Do not click links or open attachments unless you recognize the sender.

Thanks for letting me know.

Best wishes,

Mariana

From: Szymczak, Marysia (MOHLTC) <Marysia.Szymczak@ontario.ca>
Sent: December 16, 2019 4:25 AM
To: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Subject: Re: LifeLabs

Morning - we are still waiting for decisions on direction. Will keep you posted.
Marysia

Get [Outlook for iOS](#)

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: Sunday, December 15, 2019 4:10:11 PM
To: Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Cc: Szymczak, Marysia (MOHLTC) <Marysia.Szymczak@ontario.ca>
Subject: Re: LifeLabs

CAUTION -- EXTERNAL E-MAIL - Do not click links or open attachments unless you recognize the sender.

Thank you, Marysia - looking forward to receiving an update from you.

Mariana

From: Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Sent: Friday, December 13, 2019 6:55 PM
To: Diacu, Mariana HLTH:EX
Cc: Szymczak, Marysia (MOHLTC)
Subject: RE: LifeLabs

Hi Mariana,

Good to hear from you. I'm copying Marysia on this email who is leading our communications plan. We are also in the process of preparing our communications for December 17. Marysia is getting confirmation on the approach and we can keep you posted.

Neeta

-----Original Message-----

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: December 13, 2019 6:15 PM
To: Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Cc: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: RE: LifeLabs

CAUTION -- EXTERNAL E-MAIL - Do not click links or open attachments unless you recognize the sender.

Hi Neeta,

A bit of an update from my end.

s.13

How are you preparing for this event? Are you doing anything differently?

Best wishes,

Mariana
Tel: 250 213 8162

-----Original Message-----

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>

Sent: November 19, 2019 9:49 PM
To: Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Subject: Re: LifeLabs

Thank you for the update, Neeta. We are in contact with LifeLabs, constantly monitoring and adjusting our timelines for communication purposes. Please keep in touch.

Mariana

From: Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Sent: Tuesday, November 19, 2019 12:30 PM
To: Diacu, Mariana HLTH:EX
Subject: RE: LifeLabs

Hi Mariana,

We had a conversation with LifeLabs today and are waiting for them to discuss their approach with the privacy commissioner. We are waiting to get confirmation on their planned communications approach before taking action.

Neeta

-----Original Message-----

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Sent: November 18, 2019 12:03 AM
To: Sarta, Neeta (MOHLTC) <Neeta.Sarta@ontario.ca>
Cc: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>
Subject: LifeLabs

CAUTION -- EXTERNAL E-MAIL - Do not click links or open attachments unless you recognize the sender.

?Hello Neeta,

I want to thank you again for connecting with me last week. We understand that there may be some developments this week and we will proactively develop some communication messages. Do you have an update on what is happening at your end? Thank you!

Best wishes,

Mariana Diacu
Executive Director Laboratory and Blood Services Branch Provincial, Hospital and Laboratory Health Services Division
Tel: 7789 974 4105
Cell: 250 213 8162

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: December 16, 2019 3:19 PM
To: Prevost, Jean-Marc GCPE:EX
Cc: Pearce, Alison HLTH:EX; Diacu, Mariana HLTH:EX; Watt, Rebecca HLTH:EX
Subject: draft frontline KMs_LL_sm
Attachments: draft frontline KMs_LL_sm.docx

Hi Jean-Mark,

The answers provided were accurate, but the question that Alison flagged is confusing. My suggestion is to reframe the question:

1. **The Ministry of Health holds a contract with LifeLabs – what protections are in place when lab data is in the custody of a contractor or service provider?**

Prevost, Jean-Marc GCPE:EX

From: Rongve, Ian HLTH:EX
Sent: December 16, 2019 4:14 PM
To: Slater, James
Cc: XT:Dawkins, Laurie GCPE:IN; Prevost, Jean-Marc GCPE:EX
Subject: Re: LL material

Yes that seems fine. There has been some back and forth on this and I think Jean-Marc is finalizing.

Sent from my iPhone

On Dec 16, 2019, at 4:06 PM, Slater, James <james.slater@phsa.ca> wrote:

Ian, as we discussed earlier, Jean-Marc and I spoke to Laurie Dawkins (PHSA VP Comms) last Friday and today J-M shared some draft materials with Laurie for her feedback. Although these are obviously all still draft, Laurie provided the following for use with the HAs and the front line lab/HA staff:

Speaking Points for health authority staff

Please feel free to share the following information with your staff, including those who may be patient-facing in hospital laboratories. You may also consider using this information in your health authority newsletters and/or on your public-facing websites, as required.

s.13

...we'll need to finalize the messaging for tomorrow morning...☹...jim

Jim Slater

Chief Provincial Diagnostics Officer
Provincial Laboratory Medicine Services (PLMS)
Provincial Health Services Authority (PHSA)

Office: 300 – 1867 West Broadway | Vancouver, BC V6J 4W1
Phone: 604-714-2870 | james.slater@phsa.ca | www.phsa.ca

From: Rongve, Ian HLTH:EX [mailto:ian.Rongve@gov.bc.ca]
Sent: Monday, December 16, 2019 10:01 AM
To: Slater, James <james.slater@phsa.ca>
Subject: LL material

Hi Jim

Two documents attached. One is an update as of yesterday on the incident. It has been shared with our DMO and CITZ

The other is my proposed high level messaging for the public labs. My thought is that it could be sent to the front lines for ease of reference. We will of course provide more info in the call tomorrow but not have it in writing.

Can you give me a call?

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

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: December 16, 2019 4:38 PM
To: Carroll, Scott CITZ:EX; Prevost, Jean-Marc GCPE:EX
Cc: Emerson, Kim GCPE:EX
Subject: RE: Documents for review

Ok – fair enough. ^{s.13}

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: December 16, 2019 4:05 PM
To: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Cc: Emerson, Kim GCPE:EX <Kim.Emerson@gov.bc.ca>
Subject: RE: Documents for review

s.13

From: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Sent: December 16, 2019 3:42 PM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Cc: Emerson, Kim GCPE:EX <Kim.Emerson@gov.bc.ca>
Subject: RE: Documents for review

Ok – ^{s.13}

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: December 16, 2019 3:41 PM
To: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: RE: Documents for review

Not sure that ^{s.13}

From: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Sent: December 16, 2019 3:39 PM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: RE: Documents for review

s.13

K

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: December 16, 2019 3:36 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX

<Kirsten.Lauvaas@gov.bc.ca>

Subject: RE: Documents for review

Hello:

I just spoke to Thomas at LL. ^{s.13}
s.13

I have also attached the OIPC statement just received. Please share with whomever in comms needs this. I will send it to Mariana.

Thanks,
Scott

From: Carroll, Scott CITZ:EX
Sent: December 16, 2019 2:10 PM
To: Marshall, Thomas <Thomas.Marshall@lifelabs.com>
Subject: Documents for review

Hello Thomas:

Thank you for providing your communication material. We have attached ours for your review.

s.13

If additional documents or edits are received I will pass them along.

Thanks,

Scott

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

Government confidentiality and privilege requirements apply to this message and any attachments. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use is strictly prohibited. If you are not the intended recipient, please notify the sender immediately, and delete this message and any attachments from both your inbox and deleted items folder. Thank You.

Prevost, Jean-Marc GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 16, 2019 5:50 PM
To: Prevost, Jean-Marc GCPE:EX
Subject: FW: FINALS: LL materials
Attachments: Media Statement Dec 17 2019.docx

From: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Sent: December 16, 2019 5:11 PM
To: Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>; Fleurant, Kathleen CITZ:EX <Kathleen.Fleurant@gov.bc.ca>; Dycke, Kassandra CITZ:EX <Kassandra.Dycke@gov.bc.ca>
Cc: Emerson, Kim GCPE:EX <Kim.Emerson@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Kot, Jill CITZ:EX <Jill.Kot@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: FINALS: LL materials

Hi All,

Here's where we've landed with the media statement.

As discussed, the statement will be used reactively and pasted into email responses for interested media (not attached as a Word document).

I am eagerly awaiting the final Q&A as well – HLTH GCPE is working through a number of edits and dealing with version control. We're expecting that to come through later this evening, so I'll keep an eye out for it.

Kirsten

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 16, 2019 6:39 PM
To: Rongve, Ian HLTH:EX; Diacu, Mariana HLTH:EX
Subject: UPDATED PRODUCTS
Attachments: LL KM Q A Dec 16 6pm.docx; HA frontline messages 540 p.m..docx

Sarah and I have updated these together following the calls today.

Changes are tracked – and these are the final versions from us.



Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 16, 2019 6:47 PM
To: van Baarsen, Amanda HLTH:EX; Brown, Stephen R HLTH:EX
Subject: UPDATED LL PRODUCTS
Attachments: LL KM Q A Dec 16 6pm.pdf; HA frontline messages.pdf

I have updated these products following the calls today.



Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 17, 2019 7:44 AM
To: May, Stephen GCPE:EX
Subject: FW: Latest materials
Attachments: DOCS-#19918854-LifeLabs_Script_and_FAQs_for Call Centre.docx; DOCS-#19918838-v1-PRIVILEGED_AND_CONFIDENTIAL_PEGASUS_-_FAQ.DOCX; DOCS-#19918243-v2-Customer_Letter.docx

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Sent: December 16, 2019 11:59 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: FW: Latest materials

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: December 16, 2019 11:59 AM
To: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>
Subject: FW: Latest materials

Updated materials received from LL.

From: Marshall, Thomas <Thomas.Marshall@lifelabs.com>
Sent: December 16, 2019 11:28 AM
To: Presley, Trevor OIPC:EX <TPresley@oipc.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Cc: Cudlipp, Jennifer <Jennifer.Cudlipp@lifelabs.com>
Subject: Latest materials

Hi Trevor and Scott,

FYI - See attached for the most recent materials.

Note I suspect there may be some changes throughout the day.

-Thomas

Thomas Marshall
Director Government Relations

LifeLabs | 3680 Gilmore Way | Burnaby, BC V5G 4V8

T 778-372-2079 | C 604-312-8519
E Thomas.Marshall@LifeLabs.com
www.LifeLabs.com



The information in this e-mail and any attachments is confidential and for the sole use of the intended recipient(s). If you have received this e-mail in error, please: accept our apologies for the inconvenience; note that any use of the information is strictly prohibited; notify the sender as soon as possible; and then delete all copies from your system.

Le contenu de ce message ainsi que du ou des fichiers qui y sont joints est strictement confidentiel et destine exclusivement a son ou sa destinataire. Si vous avez reçu ce courriel par erreur, veuillez en aviser l'expediteur des que possible et supprimer le courriel de votre ordinateur, son utilisation etant strictement interdite. Nous sommes desoles pour tout inconvenient que cette situation aurait pu vous occasionner.

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 17, 2019 8:32 AM
To: van Baarsen, Amanda HLTH:EX
Subject: FINALS
Attachments: LL KM Q A Dec 17 FINAL.pdf; LifeLabs speaking points FINAL.pdf



Jean-Marc Prevost
COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Carroll, Scott CITZ:EX
Sent: December 17, 2019 8:37 AM
To: Prevost, Jean-Marc GCPE:EX
Subject: FW: Communication Materials
Attachments: FAQs_December_17.docx; Customer_Letter_December_17.docx

Finals from LL just received.

From: Marshall, Thomas <Thomas.Marshall@lifelabs.com>
Sent: December 17, 2019 8:28 AM
To: Presley, Trevor OIPC:EX <TPresley@oipc.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Cc: Cudlipp, Jennifer <Jennifer.Cudlipp@lifelabs.com>; Dent, Ashley <Ashley.Dent@lifelabs.com>
Subject: Communication Materials

Trevor/Scott

See attached for copies of the communication materials.

-Thomas

Thomas Marshall
Director Government Relations
LifeLabs | 3680 Gilmore Way | Burnaby, BC V5G 4V8
T 778-372-2079 | C 604-312-8519
E Thomas.Marshall@LifeLabs.com
www.LifeLabs.com



The information in this e-mail and any attachments is confidential and for the sole use of the intended recipient(s). If you have received this e-mail in error, please: accept our apologies for the inconvenience; note that any use of the information is strictly prohibited; notify the sender as soon as possible; and then delete all copies from your system.

Le contenu de ce message ainsi que du ou des fichiers qui y sont joints est strictement confidentiel et destine exclusivement a son ou sa destinataire. Si vous avez reçu ce courriel par erreur, veuillez en aviser l'expediteur des que possible et supprimer le courriel de votre ordinateur, son utilisation etant strictement interdite. Nous sommes desoles pour tout inconvenient que cette situation aurait pu vous occasionner.

Prevost, Jean-Marc GCPE:EX

From: Patterson, Catherine M HLTH:EX
Sent: December 17, 2019 8:50 AM
To: Rongve, Ian HLTH:EX; Moulton, Holly HLTH:EX; Prevost, Jean-Marc GCPE:EX
Subject: December 16 Update
Attachments: LL - December 16 2019 Update.docx

As requested.

Catherine



Catherine Patterson
Manager, Divisional Operations
Provincial, Hospital and Laboratory Health Services Division
Ministry of Health
PO Box 9639 Stn Prov Govt, Victoria BC V8W 9P1

Tel: 778 698-1749

Email: Catherine.Patterson@gov.bc.ca

This email communication is intended solely for the person or entity to which it is addressed and may contain confidential and privileged information. Any review, dissemination or other use without the express written consent of the sender is prohibited. If you are not the intended recipient, please notify me at the telephone number above or by return email and delete this communication and any copies immediately. Thank you.

Prevost, Jean-Marc GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 17, 2019 9:13 AM
To: Lauvaas, Kirsten GCPE:EX; Prevost, Jean-Marc GCPE:EX
Subject: Updated KM/QA
Attachments: LL KM Q A Dec 17 9am.docx

Hi Kirsten,

As requested, the cleaned up QA.

JM – I think you can hold off on re-circulating to your folks. We may have other edits today. It's either very minor edits relative to the changes we made last night, or changes to things that Health wouldn't be talking about (the CITZ section).

Sarah Marriott
Issues Manager
250.361.8416

Prevost, Jean-Marc GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 17, 2019 9:16 AM
To: Lauvaas, Kirsten GCPE:EX; Prevost, Jean-Marc GCPE:EX
Subject: CORRECTED: Updated KM/QA
Attachments: LL KM Q A Dec 17 915am.docx

As discussed JM – the KMs now match the statement.

From: Marriott, Sarah GCPE:EX
Sent: December 17, 2019 9:13 AM
To: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: Updated KM/QA

Hi Kirsten,

As requested, the cleaned up QA.

JM – I think you can hold off on re-circulating to your folks. We may have other edits today. It's either very minor edits relative to the changes we made last night, or changes to things that Health wouldn't be talking about (the CITZ section).

Sarah Marriott
Issues Manager
250.361.8416

Prevost, Jean-Marc GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 17, 2019 9:44 AM
To: Prevost, Jean-Marc GCPE:EX
Subject: RE: ASAP -- pls send the LL statement
Attachments: Media Statement Dec 17 2019 930am.docx

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 17, 2019 9:41 AM
To: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: ASAP -- pls send the LL statement
Importance: High



Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: December 17, 2019 9:46 AM
To: Prevost, Jean-Marc GCPE:EX; Marriott, Sarah GCPE:EX
Cc: Emerson, Kim GCPE:EX; Burton, Meribeth GCPE:EX
Subject: LL KM Q A Dec 17 915am
Attachments: LL KM Q A Dec 17 915am.docx

Hi All,

Here are the latest Q&As.

Kirsten

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 17, 2019 10:33 AM
To: LeGuilloux, Marg GCPE:EX
Subject: LifeLabs NR is out

LifeLabs NR is out

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Sent: December 17, 2019 10:29 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Subject: FYI - LL website live w/ open letter

Just FYI – below from CITZ

And online: <https://www.newswire.ca/news-releases/lifelabs-releases-open-letter-to-customers-following-cyber-attack-889534499.html>

From: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>
Sent: December 17, 2019 10:21 AM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Donaldson, Ian R CITZ:EX <Ian.Donaldson@gov.bc.ca>
Cc: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>
Subject: RE: FOR REVIEW: LL KM Q A Dec 16 6pm

Their website is live:
<https://www.customernotice.lifelabs.com>
or
<https://customernotice.lifelabs.com/>

Here's the text:

Copyright

Page 102 of 358

Withheld pursuant to/removed as

Copyright

Prevost, Jean-Marc GCPE:EX

From: Berndt, Eric GCPE:EX
Sent: December 17, 2019 10:37 AM
To: Prevost, Jean-Marc GCPE:EX
Subject: RE: FYI - LL is out

Issue: Life Labs

Background: On Dec 17 it was announced that LifeLabs, the private company responsible for conducting approximately 34% of B.C. lab testing services, experienced a significant data breach stemming from a cyber-security incident.

Key messages:

- It's certainly concerning. The protection of British Columbians' privacy is critical.
- Lifelabs is a private company, I encourage anyone who may have been a client of LifeLabs to contact them.
- I understand they've set up a call centre to assist people.

If pressed:

- The Ministry of Citizen Services is coordinating media on this – they'd be happy to get you further information.

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 17, 2019 10:36 AM
To: Berndt, Eric GCPE:EX <Eric.Berndt@gov.bc.ca>
Subject: FW: FYI - LL is out

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Sent: December 17, 2019 10:29 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Subject: FYI - LL website live w/ open letter

Just FYI – below from CITZ

And online: <https://www.newswire.ca/news-releases/lifelabs-releases-open-letter-to-customers-following-cyber-attack-889534499.html>

From: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>

Sent: December 17, 2019 10:21 AM

To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Donaldson, Ian R CITZ:EX <Ian.Donaldson@gov.bc.ca>

Cc: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>

Subject: RE: FOR REVIEW: LL KM Q A Dec 16 6pm

Their website is live:

<https://www.customernotice.lifelabs.com>

or

<https://customernotice.lifelabs.com/>

Here's the text:

Copyright

Page 105 of 358

Withheld pursuant to/removed as

Copyright

Prevost, Jean-Marc GCPE:EX

From: May, Stephen GCPE:EX
Sent: December 17, 2019 11:01 AM
To: Carroll, Scott CITZ:EX; Diacu, Mariana HLTH:EX; Marriott, Sarah GCPE:EX; Lauvaas, Kirsten GCPE:EX
Cc: Prevost, Jean-Marc GCPE:EX
Subject: RE: Issue with MyTrue Identity

When I called back with this issue – I was asked for my name and phone number (I provided my work line) and am expecting a call back.

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: December 17, 2019 10:53 AM
To: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: RE: Issue with MyTrue Identity

I sent this to LL. Will see what they say.

From: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Sent: December 17, 2019 10:49 AM
To: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Cc: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: Issue with MyTrue Identity

FYI – phoned the number – got the code (there may be concerns as the operator said “zee” as opposed to “zed”, by the way)

However when inputting this information at the My True Identity website – I got the following information

Activation Code Already Used: This code is already



This activation code has already been used in our system and we are unable to provide you access to myTrueIdentit

What to do now:

- Please verify your activation code and try again.
- For assistance, contact any of our customer service representatives Monday through Friday, 8:30 a.m. - 5:00 p.m. E 888-228-4939.



Support

[FAQs](#) [Terms and Conditions](#) [Privacy Policy](#)

From: Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>

Sent: December 16, 2019 1:07 PM

To: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>

Cc: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>

Subject: RE: Latest materials

If you had your blood drawn at your doctor's office/clinic/ in BC it is possible your information was accessed without authorization.

Best wishes,

Mariana

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>

Sent: December 16, 2019 12:56 PM

To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>

Cc: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>

Subject: RE: Latest materials

Hi all,

Just spoke to Scott re the LL materials.

Here is one piece I think we need clarity on (Mariana – Scott tells me you’re likely the person to find it out?):

1. This section from the calling script – currently our materials state that hospital tests are not involved.

Caller: *I had my blood drawn at my doctor’s office/clinic/hospital recently, but I’m not sure if my test went to LifeLabs. Can you confirm if my lab test(s) were included in this breach?*

- **CCC:** Did you have blood collected in either Ontario or BC for testing in the past 10 year?
 - [If customer lives in Ontario, British Columbia] – It is possible your information was accessed without authorization.

s.13

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>

Sent: December 16, 2019 11:59 AM

To: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>

Cc: May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>

Subject: FW: Latest materials

Updated materials received from LL.

From: Marshall, Thomas <Thomas.Marshall@lifelabs.com>

Sent: December 16, 2019 11:28 AM

To: Presley, Trevor OIPC:EX <TPresley@oipc.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>

Cc: Cudlipp, Jennifer <Jennifer.Cudlipp@lifelabs.com>

Subject: Latest materials

Hi Trevor and Scott,

FYI - See attached for the most recent materials.

Note I suspect there may be some changes throughout the day.

-Thomas

Thomas Marshall

Director Government Relations

LifeLabs | 3680 Gilmore Way | Burnaby, BC V5G 4V8

T 778-372-2079 | C 604-312-8519
E Thomas.Marshall@LifeLabs.com
www.LifeLabs.com



The information in this e-mail and any attachments is confidential and for the sole use of the intended recipient(s). If you have received this e-mail in error, please: accept our apologies for the inconvenience; note that any use of the information is strictly prohibited; notify the sender as soon as possible; and then delete all copies from your system.

Le contenu de ce message ainsi que du ou des fichiers qui y sont joints est strictement confidentiel et destine exclusivement a son ou sa destinataire. Si vous avez reçu ce courriel par erreur, veuillez en aviser l'expediteur des que possible et supprimer le courriel de votre ordinateur, son utilisation etant strictement interdite. Nous sommes desoles pour tout inconvenient que cette situation aurait pu vous occasionner.

Prevost, Jean-Marc GCPE:EX

From: van Baarsen, Amanda HLTH:EX
Sent: December 17, 2019 12:02 PM
To: Prevost, Jean-Marc GCPE:EX
Subject: Fwd: LL Backgrounder and Statement

Sent from my iPhone

Begin forwarded message:

From: "Dix, Adrian HLTH:EX" <Adrian.Dix@gov.bc.ca>
Date: December 17, 2019 at 12:00:58 PM PST
To: "van Baarsen, Amanda HLTH:EX" <Amanda.vanBaarsen@gov.bc.ca>
Subject: Re: LL Backgrounder and Statement

s.13

From: van Baarsen, Amanda HLTH:EX
Sent: Tuesday, December 17, 2019 11:39 AM
To: Dix, Adrian HLTH:EX
Subject: RE: LL Backgrounder and Statement

Do you like this?

s.13

Background:

- LifeLabs says there is no evidence British Columbians' lab test results were impacted.
- The breached data in B.C. includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.
- LifeLabs is a private company responsible for conducting approximately 34% of B.C. lab testing services.

From: Dix, Adrian HLTH:EX <Adrian.Dix@gov.bc.ca>
Sent: December 17, 2019 11:25 AM
To: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>
Subject: Re: LL Backgrounder and Statement

Okay. Can the statement be finalized for approval?

On Dec 17, 2019, at 11:04 AM, van Baarsen, Amanda HLTH:EX
<Amanda.vanBaarsen@gov.bc.ca> wrote:

They refused to communicate it with us in advance but we are scouring to find it once posted.

Sent from my iPhone

On Dec 17, 2019, at 10:34 AM, Dix, Adrian HLTH:EX
<Adrian.Dix@gov.bc.ca> wrote:

Do we have a copy of Ontario's statement? ^{s.13}
s.13

Adrian

From: van Baarsen, Amanda HLTH:EX
Sent: Tuesday, December 17, 2019 9:42 AM

To: Dix, Adrian HLTH:EX
Subject: Fwd: LL Backgrounder and Statement

This is what the OIPC will be putting out

Sent from my iPhone

Begin forwarded message:

From: "Moulton, Holly HLTH:EX"
<Holly.Moulton@gov.bc.ca>
Date: December 17, 2019 at 9:41:04 AM PST
To: "van Baarsen, Amanda HLTH:EX"
<Amanda.vanBaarsen@gov.bc.ca>
Subject: LL Backgrounder and Statement

Attached from the Office of the Information and Privacy
Commissioner.

Holly


Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 17, 2019 1:07 PM
To: Moulton, Holly HLTH:EX; Brown, Stephen R HLTH:EX
Subject: LL KM Q A Dec 17 955am.docx
Attachments: LL KM Q A Dec 17 955am.docx; ATT00001.htm

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 17, 2019 1:17 PM
To: Moulton, Holly HLTH:EX
Subject: Fwd: UPDATES
Attachments: 2019-12-17-ipc_oipc-media-statement final Dec 16 2 PM.DOCX; ATT00001.htm; Media Statement Dec 17 2019 930am.docx; ATT00002.htm; LL KM Q A Dec 17 955am.docx; ATT00003.htm

Jean-Marc Prevost

 250-886-2154

Begin forwarded message:

From: "Prevost, Jean-Marc GCPE:EX" <Jean-Marc.Prevost@gov.bc.ca>
Date: December 17, 2019 at 9:55:00 AM PST
To: "van Baarsen, Amanda HLTH:EX" <Amanda.vanBaarsen@gov.bc.ca>
Subject: UPDATES

Government and OIPC statements attached.

(You may receive these from Holly as well).

Plan was to respond with statements only – **no spokesperson.**

Also I have a new version of the KM doc and Q & A for your review.

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: van Baarsen, Amanda HLTH:EX <Amanda.vanBaarsen@gov.bc.ca>
Sent: December 17, 2019 9:39 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: Re: rundown today

Minister would like to see the privacy commission NR and our statment.

Sent from my iPhone

On Dec 17, 2019, at 9:31 AM, Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca> wrote:

At 10 a.m. at a new conference in Ontario LL will announce they were a victim of a cyber attack

They will confirm they have hired world-leading cyber security firms to assist them in responding

They will confirm they paid money to re-secure breached data

They will announce a website and call-in number for LL customers to get free credit monitoring and fraud-insurance

At 10:10 the BC's privacy commission will issue a news release announcing his investigation into the incident

The governments of Ontario and British Columbia plan to provide statements to media when asked (no plans for proactive statements).

<image001.png>

Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Prevost, Jean-Marc GCPE:EX

From: Diacu, Mariana HLTH:EX
Sent: December 17, 2019 1:28 PM
To: Rongve, Ian HLTH:EX
Cc: Watt, Rebecca HLTH:EX; Prevost, Jean-Marc GCPE:EX; Diacu, Mariana HLTH:EX
Subject: LL december 17 update v.1
Attachments: LL december 17 update v.1.docx

Updated version of the document

Prevost, Jean-Marc GCPE:EX

From: Lauvaas, Kirsten GCPE:EX
Sent: December 17, 2019 4:21 PM
To: Prevost, Jean-Marc GCPE:EX
Cc: Emerson, Kim GCPE:EX
Subject: FW: As Requested

Importance: High

Hi Jean-Marc,

For your back pocket. . . .

Thanks for your work and help on all of this. 😊

Have a great holiday season!

Kirsten

From: Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>
Sent: December 17, 2019 1:49 PM
To: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Cc: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Subject: As Requested
Importance: High

Hi Sarah,

As requested, here are the details for the 2pm meeting. Please let me know if you need us to pull further information.

1. How do the *Freedom of Information and Protection of Privacy Act (FOIPPA)* and *Personal Information Protection Act (PIPA)* legislation apply in this case:
 - Government and the rest of the public sector are subject to FOIPPA, whereas private sector organizations are subject to PIPA.
 - Government's contract with LifeLabs, which includes the privacy terms to which LifeLabs must adhere, sets a robust standard for LifeLabs to meet with respect to privacy and security.

s.13

to

2. Number of cyber attacks core government deals with:
 - There are 308 million unauthorized access attempts on B.C. government networks daily – that's 3,565 per second.
 - The number of attempts has increased from 240 million per day since last year – an increase of more than 28%.


Thanks,
Shannon

Shannon Russell

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 18, 2019 10:10 AM
To: May, Stephen GCPE:EX; Shewchuk, Chris GCPE:EX
Subject: Fwd: everything in one place
Attachments: image002.png; ATT00001.htm; 2019-12-17-ipc_oipc-media-statement final Dec 16 2 PM.DOCX; ATT00002.htm; LL KM Q A Dec 17 955am.docx; ATT00003.htm

Jean-Marc Prevost

 [250-886-2154](tel:250-886-2154)

Begin forwarded message:

From: "Prevost, Jean-Marc GCPE:EX" <Jean-Marc.Prevost@gov.bc.ca>
Date: December 17, 2019 at 2:00:00 PM PST
To: "van Baarsen, Amanda HLTH:EX" <Amanda.vanBaarsen@gov.bc.ca>
Subject: **everything in one place**

Attachments:

The latest KM Q&A document (from Ian and me this morning)

The OIPC's statement

LifeLabs 18/19 stats:

Medical Services Commission Blue Book has for 2018/19

LifeLabs BC LP \$240,542,511.93

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

LifeLabs statement below:

TORONTO, Dec. 17, 2019 /CNW/ - LifeLabs is releasing the below open letter to its customers in Canada, following a recent cyber security-attack.

Copyright

Page 122 of 358

Withheld pursuant to/removed as

Copyright

Prevost, Jean-Marc GCPE:EX

From: van Baarsen, Amanda HLTH:EX
Sent: December 18, 2019 5:06 PM
To: Brown, Stephen R HLTH:EX; Prevost, Jean-Marc GCPE:EX
Subject: FW: HLTH Media Request: Lifelabs breach
Attachments: s.3 3Dec19.pdf

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 – s.3 – 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.Barcly@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 9:55 AM
To: Carroll, Scott CITZ:EX <Scott.Carroll@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.Barcly@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

Do we have any details on what LifeLabs is doing s.3 ? This was apparently provided to the OIPC. Minister Dix is asking for it.

From: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>
Sent: December 18, 2019 9:46 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>
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

Looks good to me. No concerns.

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.

Prevost, Jean-Marc GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 20, 2019 8:08 AM
To: van Baarsen, Amanda HLTH:EX
Cc: Shewchuk, Chris GCPE:EX; Prevost, Jean-Marc GCPE:EX
Subject: LL quote for MD

FYI -

Wilkinson: I'm the first one to say that I don't know the answer to that, but it should have been done if it wasn't done. If we're in some way responsible for how the contract got written then we did it wrong. Right now the answer is that there's been a huge blunder and there's been a huge hole driven through the wall of our personal information and they didn't have the courtesy to tell us so we could take protective measures.

Now they say if something goes wrong, they'll think about giving us some insurance if we apply for it. I call BS on all that stuff. Tell us the truth, tell us the truth you knew on day two, not day 42.

Sarah Marriott
Issues Manager
250.361.8416

Wilkinson - LifeLabs privacy breach

CKNW

Thursday, December 19, 2019, 12:36

By CKNW Simi Sara

Copyright

Page 127 of 358 to/à Page 129 of 358

Withheld pursuant to/removed as

Copyright

Prevost, Jean-Marc GCPE:EX

From: Shewchuk, Chris GCPE:EX
Sent: December 20, 2019 10:58 AM
To: XT:Goodwin, Jenn GCPE:IN; XT:Dawkins, Laurie GCPE:IN; May, Stephen GCPE:EX
Cc: Prevost, Jean-Marc GCPE:EX; XT:Conrad, Tim GCPE:IN; XT:HLTH Toews, Erin HLTH:IN
Subject: RE: ContactUs from: ^{s.22}
Attachments: HCP Notification v2.pdf

Hi all, here's an update on what we can say.

We discovered LifeLabs distributed the attached PDF to all clinical partners on Tuesday, they are going to distribute it a second time to encourage the pdf get posted publicly at all clinical locations where samples are collected to help people understand that they may be a LifeLabs client without directly knowing. Will the bullets below work? They are approved on our end.

- Regional health authorities in B.C. contract the analysis of some specimens (tests) to LifeLabs.
- LifeLabs recently sent the attached notification to health care providers to inform its partners throughout Canada of the privacy breach.
- This notification will be posted at any health service provider who partners with LifeLabs, such as private clinics and health authorities to inform patients that they may indirectly be a LifeLabs client.
- B.C. residents who are concerned about the safety of their own personal information related to lab testing should contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.

Chris Shewchuk
Ministry of Health - GCPE
778.698.8234 (office) 778.677.0965 (mobile) chris.shewchuk@gov.bc.ca

-----Original Message-----

From: Goodwin, Jenn <Jenn.Goodwin@interiorhealth.ca>
Sent: December 20, 2019 8:46 AM
To: XT:Dawkins, Laurie GCPE:IN <laurie.dawkins@phsa.ca>; May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Cc: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; XT:Conrad, Tim GCPE:IN <Tim.Conrad@interiorhealth.ca>; Shewchuk, Chris GCPE:EX <Chris.Shewchuk@gov.bc.ca>; XT:HLTH Toews, Erin HLTH:IN <erin.toews@interiorhealth.ca>
Subject: RE: ContactUs from: ^{s.22}

Hi all,

The messaging earlier this week was not specific enough for the questions we are getting. If we remove the piece about the billing system, can we go with below?

> Regional health authorities in B.C. contract the analysis of some specimens (tests) to LifeLabs. However, patient data related to these tests was not impacted by the recent LifeLabs information breach.

>

> The personal information of Interior Health clients who had lab tests conducted at appointments at their local hospital or IH site is not impacted by this breach.

>

> B.C. residents who are concerned about the safety of their own personal information related to lab testing should contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.

>

-----Original Message-----

From: Dawkins, Laurie [mailto:laurie.dawkins@phsa.ca]

Sent: Friday, December 20, 2019 7:37 AM

To: May, Stephen [External Email]

Cc: Goodwin, Jenn; Prevost, Jean-Marc GCPE:EX; Conrad, Tim; Shewchuk, Chris GCPE:EX; Toews, Erin

Subject: Re: ContactUs from: ^{s.22}

s.13

L

Laurie Dawkins, ABC, MC, SCMP
Vice President,
Communications & Stakeholder Engagement
Provincial Health Services Authority

> On Dec 20, 2019, at 7:01 AM, May, Stephen GCPE:EX <Stephen.May@gov.bc.ca> wrote:

>

> I'm running this past program but I don't think it's fully correct ^{s.13}

s.13 I'm also adding in Laurie Dawkins as I believe they developed some messaging for their lab folks on this.

>

> I understand the need for consistent comms material - we're trying to get you information.

>

> Sent from my iPhone

>

> On Dec 19, 2019, at 10:55 PM, Goodwin, Jenn <Jenn.Goodwin@interiorhealth.ca> wrote:

>

>

> Hi Jean Marc,

>

> We really need a clear message to be able to tell patients and staff with respect to the health authorities contracting analysis/testing to Life Labs. Below is one of several emails I received from leaders in IH yesterday asking me for messaging on this specific topic.

>

> Suggest the following – could you please confirm if this is ok for us to share with staff and leaders who are receiving questions, and who will in turn share it with patients who are making inquiries:

>

> Regional health authorities in B.C. contract the analysis of some specimens (tests) to LifeLabs. However, the data related to these tests is not believed to have been impacted by the recent LifeLabs information breach.

>

> The personal information of Interior Health clients who had lab tests conducted at appointments at their local hospital or IH site is not impacted by this breach.

>

> The CEO of LifeLabs has confirmed that the data that was breached included the names, addresses, passwords and email addresses of individuals accessing the LifeLabs online booking system. In addition, test results for 85,000 Ontario residents, prior to 2016, were also compromised.

>

> B.C. residents who are concerned about the safety of their own personal information related to lab testing should contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.

>

> Thanks

> Jenn.

>

>

> From: Isber, Joanne

> Sent: Thursday, December 19, 2019 7:40 PM

> To: Goodwin, Jenn

> Cc: Lowden, Dr. Launny; Braidwood, Mark

> Subject: FW: ContactUs from: ^{s.22}

>

> Hi Jenn

> Any word on a government message regarding public hospitals using Lifelabs?

> The email below is from a community resident emailing our general IH Lab Quality team...I don't want IH to take a bad hit because we aren't being forthcoming on information. Despite providing patients with the message to call Lifelabs directly, they appear to want to understand how their specimens are connected to LL.

>

> Is it an option to create an informative Q&A document for the IH website?

>

> Joanne

>

> Joanne Isber MLT, MLS, EMBA

> Program Director, IH Laboratory Services

> Admin Assistant: ashley.dirks@interiorhealth.ca<<mailto:ashley.dirks@interiorhealth.ca>>

> Office: Community Health and Services Centre

> 505 Doyle Ave, Kelowna, BC V1Y 0C5

> Cell: 250-540-8976

> joanne.isber@interiorhealth.ca<<mailto:joanne.isber@interiorhealth.ca>>

>

>

>

> From: Lowden, Dr. Launny

> Sent: Thursday, December 19, 2019 5:07 PM

> To: IH Lab Quality; Klement, Maria; Isber, Joanne; Anderson, Mark; Bradley, Kelly; Byrne, Hope (Constance)

> Subject: RE: ContactUs from: ^{s.22}

>

> If it's possible to hold off answering, there may be some more communication coming soon regarding this specific issue (i.e. regarding whether patients we have referred for testing are affected or not). Sorry I can't say more than that at this exact moment. Currently the best answer is to say that his question is being looked into and we will get back to him soon, but he can also contact LifeLabs if he is concerned. I hope that helps.

>

> Launny Lowden

>

> Dr. Launny Lowden, FRCPC

> General Pathologist, EKRH

> Department Head, IH Area East
> Interim Medical Director, IH Laboratory Services
> Ph: 250-426-5281 ext 6270
>
> From: IH Lab Quality
> Sent: Thursday, December 19, 2019 5:42 PM
> To: Klement, Maria; Lowden, Dr. Launny; Isber, Joanne; Anderson, Mark; Bradley, Kelly; Byrne, Hope (Constance)
> Subject: FW: ContactUs from: s.22
>
> Good Afternoon,
>
> I am not seeing a lot of transparency around samples collected in IH and sent to LifeLabs in our provided response message. Can you please provide some guidance as to how I should reply to the message below?
>
> Please let me know if you would prefer I sent these messages to the Directors or another contact.
>
> Here is my draft: Interior Health Labs collect samples for testing at LifeLabs and other referral labs such as BC CDC. If you are concerned that you may have had samples that required testing at LifeLabs, I encourage you to contact LifeLabs directly to confirm.
>
> Thank you,
> Katie Monai
> Quality Coordinator
> IH Lab Services
> 250-862-4300 x7396
> Katie.monai@interiorhealth.ca<mailto:Katie.monai@interiorhealth.ca>
>
> From: s.22 [mailto:s.22]
> Sent: Thursday, December 19, 2019 3:35 PM
> To: IH Lab Quality
> Subject: Re: ContactUs from: s.22
>
> CAUTION! This email originated from outside of Interior Health. Do not click links or open attachments unless you recognize the sender, their email address, and know the content is safe. If you suspect this is a phishing or fraudulent email please forward it to spam@interiorhealth.ca.
>
> Thank you. I was wondering if Interior Health Cranbrook uses Life Lab. It seems the answer is yes?
>
>
>
> Sent from Outlook<http://aka.ms/weboutlook>
>
>
> From: IH Lab Quality <ihlabquality@interiorhealth.ca>
> Sent: December 19, 2019 4:23 PM
> To: s.22
> Subject: RE: ContactUs from: s.22
>
> Hi s.22
>
> Thank you for your email. It looks like some of it was cut off, so I hope I can answer your question. If this was not the information you were looking for, please reply and I will try to better answer your question.

>
> If you are concerned about tests with LifeLabs, and the safety of your personal information, contact LifeLabs directly by visiting www.customernotice.lifelabs.com<<http://www.customernotice.lifelabs.com>> or by calling 1-888-918-0467. LifeLabs has committed to providing one free year of protection (dark web monitoring and identity theft insurance) to clients who may have been impacted.
>
> Kind regards,
>
> Katie Monai
> Quality Coordinator
> IH Lab Services
> 250-862-4300 x7396
> ihlabquality@interiorhealth.ca
>
>
>
> -----Original Message-----
> From: ^{s.22}
> Sent: Thursday, December 19, 2019 9:05 AM
> To: IH Lab Quality
> Subject: ContactUs from: ^{s.22}
>
> Contact Name: ^{s.22} ()
> Contact Email: ^{s.22} i
>
>
> rior Health Cranbrook uses Life Lab, but cannot find an answer. Please advise i

Prevost, Jean-Marc GCPE:EX

From: Shewchuk, Chris GCPE:EX
Sent: December 20, 2019 1:38 PM
To: Slater, James
Cc: Barclay, Corrie A HLTH:EX; Prevost, Jean-Marc GCPE:EX; Rongve, Ian HLTH:EX
Subject: RE: For direction ...
Attachments: HCP Notification v2.pdf

Hi Jim,

Here's where we landed to help Interior Health answer the questions they're receiving and I am sharing it with the various Communications VPs as well.

- Regional health authorities in B.C. contract the analysis of some specimens (tests) to LifeLabs.
- LifeLabs recently sent the attached notification to health care providers to inform its partners throughout Canada of the privacy breach.
- This notification will be posted at any health service provider who partners with LifeLabs, such as private clinics and health authorities to inform patients that they may indirectly be a LifeLabs client.
- B.C. residents who are concerned about the safety of their own personal information related to lab testing should contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.

Chris Shewchuk
Ministry of Health - GCPE
778.698.8234 (office) 778.677.0965 (mobile) chris.shewchuk@gov.bc.ca

-----Original Message-----

From: Slater, James <james.slater@phsa.ca>
Sent: December 20, 2019 1:15 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Cc: Barclay, Corrie A HLTH:EX <Corrie.Barcly@gov.bc.ca>; Shewchuk, Chris GCPE:EX <Chris.Shewchuk@gov.bc.ca>
Subject: RE: For direction ...

Sorry I'm coming in to an existing email string and adding an attachment from this issue being escalated to me from PHC...^{s.13}

s.13

Jim Slater
Chief Provincial Diagnostics Officer
Provincial Health Services Authority (PHSA)

Office: 300 – 1867 West Broadway | Vancouver, BC V6J 4W1
Phone: 604-714-2870 | james.slater@phsa.ca | www.phsa.ca

-----Original Message-----

From: Prevost, Jean-Marc GCPE:EX [mailto:Jean-Marc.Prevost@gov.bc.ca]
Sent: Friday, December 20, 2019 12:43 PM
To: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Cc: Corrie.Barclay@gov.bc.ca; Slater, James <james.slater@phsa.ca>; Shewchuk, Chris GCPE:EX <Chris.Shewchuk@gov.bc.ca>
Subject: Re: For direction ...

Yes

Sorry

I jumped into the middle of an email chain

Pls disregard

Jean-Marc Prevost
[mobile-icon] 250-886-2154<tel:250-886-2154>

On Dec 20, 2019, at 2:41 PM, Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca> wrote:

That's not right. We talked through this with Chris.

Sent from my iPhone

On Dec 20, 2019, at 12:15 PM, Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca> wrote:

Jean-Marc Prevost
[mobile-icon] 250-886-2154<tel:250-886-2154>

Begin forwarded message:

From: "Goodwin, Jenn" <Jenn.Goodwin@interiorhealth.ca>
Date: December 20, 2019 at 12:55:17 AM CST

To: "Prevost, Jean-Marc GCPE:EX" <Jean-Marc.Prevost@gov.bc.ca>
Cc: "XT:Conrad, Tim GCPE:IN" <Tim.Conrad@interiorhealth.ca>, "Shewchuk, Chris GCPE:EX" <Chris.Shewchuk@gov.bc.ca>, "May, Stephen GCPE:EX" <Stephen.May@gov.bc.ca>, "XT:HLTH Toews, Erin HLTH:IN" <erin.toews@interiorhealth.ca>
Subject: FW: ContactUs from: s.22

Hi Jean Marc,

We really need a clear message to be able to tell patients and staff with respect to the health authorities contracting analysis/testing to Life Labs. Below is one of several emails I received from leaders in IH yesterday asking me for messaging on this specific topic.

Suggest the following – could you please confirm if this is ok for us to share with staff and leaders who are receiving questions, and who will in turn share it with patients who are making inquiries:

Regional health authorities in B.C. contract the analysis of some specimens (tests) to LifeLabs. s.13

s.13

The CEO of LifeLabs has confirmed that the data that was breached included the names, addresses, passwords and email addresses of individuals accessing the LifeLabs online booking system. In addition, test results for 85,000 Ontario residents, prior to 2016, were also compromised.

B.C. residents who are concerned about the safety of their own personal information related to lab testing should contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.

Thanks
Jenn.

From: Isber, Joanne
Sent: Thursday, December 19, 2019 7:40 PM
To: Goodwin, Jenn
Cc: Lowden, Dr. Launny; Braidwood, Mark
Subject: FW: ContactUs from: s.22

Hi Jenn

Any word on a government message regarding public hospitals using Lifelabs?

The email below is from a community resident emailing our general IH Lab Quality team...I don't want IH to take a bad hit because we aren't being forthcoming on information. Despite providing patients with the message to call Lifelabs directly, they appear to want to understand how their specimens are connected to LL.

Is it an option to create an informative Q&A document for the IH website?

Joanne

Joanne Isber MLT, MLS, EMBA
Program Director, IH Laboratory Services Admin Assistant:
ashley.dirks@interiorhealth.ca<<mailto:ashley.dirks@interiorhealth.ca>>

Office: Community Health and Services Centre
505 Doyle Ave, Kelowna, BC V1Y 0C5
Cell: 250-540-8976
joanne.isber@interiorhealth.ca<mailto:joanne.isber@interiorhealth.ca>

From: Lowden, Dr. Launny
Sent: Thursday, December 19, 2019 5:07 PM
To: IH Lab Quality; Klement, Maria; Isber, Joanne; Anderson, Mark; Bradley, Kelly; Byrne, Hope (Constance)
Subject: RE: ContactUs from: s.22

If it's possible to hold off answering, there may be some more communication coming soon regarding this specific issue (i.e. regarding whether patients we have referred for testing are affected or not). Sorry I can't say more than that at this exact moment. Currently the best answer is to say that his question is being looked into and we will get back to him soon, but he can also contact LifeLabs if he is concerned. I hope that helps.

Launny Lowden

Dr. Launny Lowden, FRCPC
General Pathologist, EKRH
Department Head, IH Area East
Interim Medical Director, IH Laboratory Services
Ph: 250-426-5281 ext 6270

From: IH Lab Quality
Sent: Thursday, December 19, 2019 5:42 PM
To: Klement, Maria; Lowden, Dr. Launny; Isber, Joanne; Anderson, Mark; Bradley, Kelly; Byrne, Hope (Constance)
Subject: FW: ContactUs from: s.22

Good Afternoon,

I am not seeing a lot of transparency around samples collected in IH and sent to LifeLabs in our provided response message. Can you please provide some guidance as to how I should reply to the message below?

Please let me know if you would prefer I sent these messages to the Directors or another contact.

Here is my draft: Interior Health Labs collect samples for testing at LifeLabs and other referral labs such as BC CDC. If you are concerned that you may have had samples that required testing at LifeLabs, I encourage you to contact LifeLabs directly to confirm.

Thank you,
Katie Monai
Quality Coordinator
IH Lab Services
250-862-4300 x7396
Katie.monai@interiorhealth.ca<mailto:Katie.monai@interiorhealth.ca>

From: s.22 [mailto:s.22]
Sent: Thursday, December 19, 2019 3:35 PM
To: IH Lab Quality
Subject: Re: ContactUs from: s.22

CAUTION! This email originated from outside of Interior Health. Do not click links or open attachments unless you recognize the sender, their email address, and know the content is safe. If you suspect this is a phishing or fraudulent email please forward it to spam@interiorhealth.ca.

Thank you. I was wondering if Interior Health Cranbrook uses Life Lab. It seems the answer is yes?

Sent from Outlook<<http://aka.ms/weboutlook>>

From: IH Lab Quality <ihlabquality@interiorhealth.ca>

Sent: December 19, 2019 4:23 PM

To: s.22

Subject: RE: ContactUs from: s.22

Hi s.22

Thank you for your email. It looks like some of it was cut off, so I hope I can answer your question. If this was not the information you were looking for, please reply and I will try to better answer your question.

If you are concerned about tests with LifeLabs, and the safety of your personal information, contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467. LifeLabs has committed to providing one free year of protection (dark web monitoring and identity theft insurance) to clients who may have been impacted.

Kind regards,

Katie Monai
Quality Coordinator
IH Lab Services
250-862-4300 x7396
Ihlabquality@interiorhealth.ca

-----Original Message-----

From: s.22

Sent: Thursday, December 19, 2019 9:05 AM

To: IH Lab Quality

Subject: ContactUs from: s.22

Contact Name: s.22

Contact Email: s.22

rior Health Cranbrook uses Life Lab, but cannot find an answer. Please advisei

Prevost, Jean-Marc GCPE:EX

From: Dawkins, Laurie <laurie.dawkins@phsa.ca>
Sent: December 24, 2019 9:12 AM
To: XT:Chiang, Charlene GCPE:IN; XT:Nuraney, Naseem GCPE:IN; XT:Goodwin, Jenn GCPE:IN; XT:Raper, Steve GCPE:IN; XT:Latimer, Brenna GCPE:IN; XT:Hussain, Shaf GCPE:IN; XT:Braman, Jamie HLTH:IN
Cc: Prevost, Jean-Marc GCPE:EX
Subject: FW: LL Patient Notification Communications
Attachments: BC - Supporting Communications Materials - Dec 24 - Final.docx

Hi guys,

s.13

These materials will be shared with our respective Lab leaders via Jim Slater as well.

Laurie

Laurie Dawkins, ABC, MC, SCMP

Vice President, Communications & Stakeholder Engagement
Provincial Health Services Authority
200 – 1333 W Broadway
Vancouver, British Columbia
V6H 4C1 Canada
604-675-7401 Phone
604-612-8053 Cell
778-867-7472 Media line
www.phsa.ca

Province-wide solutions.
Better health.

Page 141 of 358 to/à Page 144 of 358

Withheld pursuant to/removed as

s.3



LifeLabs Cyber-Attack

Patient Notification Communications Materials

Contents

Community Notice Ad Copy	2
Publications where the ad notice will appear.....	3
Frequently Asked Questions	4
Health Care Providers Letter	6
Patient Flyer	7
Appendix	8
Website News Section Content	8
Social Media Messages	9

Page 146 of 358 to/à Page 154 of 358

Withheld pursuant to/removed as

Copyright

Page 155 of 358 to/à Page 165 of 358

Withheld pursuant to/removed as

s.21

LifeLabs November 18

Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it comes to the personal information of citizens.
- Citizens 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 also notified the Office of the Information and Privacy Commissioner of this incident.
- At this time, there is no evidence to indicate that B.C. government systems are affected by this breach.
- 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 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 still investigating the full scope of those who may be affected.
- Once the scope is determined, LifeLabs will begin the notification process.

On the Question of why Law Enforcement was not notified

- LifeLabs has indicated they will be notifying the RCMP in the near future.
- s.15

- BC's critical priority has always been the safety and security of the information and protecting the privacy of BC citizens
 - LifeLabs and the BC government have been cooperating in the investigation
- LifeLabs has been working with legal counsel and cyber security experts in this matter.
- LifeLabs operates as a private company in BC, Ontario, Saskatchewan and New Brunswick and has to meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

Page 168 of 358 to/à Page 179 of 358

Withheld pursuant to/removed as

Copyright

Page 180 of 358 to/à Page 182 of 358

Withheld pursuant to/removed as

s.21

Page 183 of 358

Withheld pursuant to/removed as

s.13

Speaking Points for health authority staff

Please feel free to share the following information with your staff, including those who may be patient-facing in hospital laboratories. You may also consider using this information in your health authority newsletters and/or on your public-facing websites, as required.

Health authority lab data remains secure

On December 17, 2019, it was announced that LifeLabs, the private company responsible for conducting approximately 34% of B.C. lab testing services, 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.

Should health authority employees be asked about the LifeLabs situation, please feel free to share the following:

- Most of British Columbian's lab tests happen in hospitals and that data is not affected by this breach.
- Government and health authority systems were not impacted. They have security measures in place to prevent infiltrations, and proactive monitoring tools to detect threats.
- LifeLabs is providing all customers access to free identity theft insurance and monitoring services.
- Should patients ask you about the LifeLabs data breach or raise concerns about the safety of their own data, **please encourage them to contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.**

Page 185 of 358 to/à Page 186 of 358

Withheld pursuant to/removed as

Copyright

Incident Timeline 2019-2248

November 19, 2019

October 28, 2019:

- LifeLabs proactive network surveillance tools detected unauthorized access^{s.15}
- Upon detection of the access LifeLabs quickly isolated the affected systems to eliminate and contain any potential impact of the unauthorized access.
- LifeLabs immediately engaged a top international cyber security firm (CrowdStrike) to conduct a comprehensive forensic review and further secure other LifeLabs and Excelleris systems.
- LifeLabs reported the potential incident to the Ministry of Health. At this time there was no confirmation that personal information had been impacted.

s.15

November 1, 2019:

- The incident is reported to CIRMO. No evidence received at this time that BC residents were impacted.

November 5, 2019:

- Confirmation is received that LifeLabs reported the incident to the OIPC without informing government of their intention to report prior to doing so.

November 7, 2019:

s.15

November 8, 2019:

- CIRMO and LifeLabs updated the OIPC that BC resident data has been impacted.
- The OIPC were informed of the scope and information impacted. LifeLabs confirmed they were assessing the new data that had been provided and determining next steps to address this incident.
- Those next steps include efforts to recover the data as well as conducting a notification assessment of the impacted parties.

November 13, 2019:

- The OIPC were informed that the format for the notifications, the notification content and when notifications will occur is still being determined.

November 14, 2019:

- LifeLabs confirmed their call centre will be ready next week. LifeLabs confirmed they plan on offering the impacted individuals one year of credit monitoring at no cost via Trans Union.

November 15, 2019:

- s.15
- LifeLabs also confirmed they will be reporting the incident to law enforcement (RCMP).

November 18, 2019:

- LifeLabs confirmed the incident was reported to law enforcement.

November 19, 2019:

- LifeLabs confirmed that they believe the information was accessed^{s.15}
s.15
- LifeLabs reported that identifying the number of impacted individuals is extremely difficult given the format in which the data was recovered.
- At this time they are still trying to assess the full extent of the impacted parties.^{s.13}
s.13
- To address notification LifeLabs plans on issuing a public notification. The initial plan was for this to be conducted on^{s.13} via a media release, however, the date has since been delayed until^{s.13}
- LifeLabs confirmed that they will share their communications plan with government for review.

LifeLabs Update November, 2019

- LifeLabs is the largest private provider of laboratory medicine services in BC
- In 2018, LifeLabs provided almost 34.6 million tests and had 5.6 million patient visits.
- LifeLabs also distributed laboratory results to most physician offices in BC as well as to facilities in three health authorities utilizing a proprietary IM/IT system.
- LifeLabs was paid \$234 million in 2018/19 by the Ministry predominantly through fee for service and is on track to receive \$243 million for fiscal 2019/20.

What has Happened

October 28, 2019:

- 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
-
-
- LifeLabs immediately engaged CrowdStrike cyber security services^{s.15}
s.15 (Crowd Strike is an international company who is known for their work on Sony's privacy breach in the US).

s.15

● s.13

s.13

s.15

s.15

- The Ontario Privacy Commissioner has been briefed
- The on-line booking system should be available shortly.

Next Steps

● s.15

●

● s.13; s.15

- LifeLabs CEO and Executive VP for BC are personally involved
- MOH, PHSA, and CITZ are collaborating with LifeLabs on this issue.
- MoH/PHSA are monitoring the situation and impacts on patient and provider services; no issues have been identified at this time due to the booking system being down

Update November 4, 2019

- LifeLabs continues to believe there is no BC data involved.
- As yet the police have not been notified.
- s.13

●

- Next update will be November 5, 2019.

Update November 5, 2019

s.15

Page 191 of 358

Withheld pursuant to/removed as

s.15

LifeLabs Update

- The information security incident with LifeLabs has escalated, LifeLabs has proof that some BC 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.
 - Citizen services is concerned about identity theft resulting from the use of data accessed (provider's name and address, patient name, PHN, address, date 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 will be provided with an update later today.
 - 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 patient notification of the privacy breach of personal information at LifeLabs in Ontario and British Columbia.
- LifeLabs has engaged an internationally recognised firm, Crowdstrike to help them with the technical aspects of the investigation, s.15
- LifeLabs Executive Team and Board are fully involved in the response.
- LifeLabs is currently confident that they have contained the vulnerability and services to the public have returned to normal.

Chronology

- On October 28, LifeLabs proactive system surveillance identified unauthorized access^{s.15}
 - LifeLabs immediately isolated the affected systems to eliminate and contain any potential impact of the unauthorized access

s.15

Communications Planning

- GCPE is fully involved and is developing messaging for the incident, actions taken and notification plans.

Ian Rongve
250-516-3411
November 7, 2019

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

s.15

Communications Planning

- GCPE is fully involved and is developing messaging for the incident, actions taken and notification plans.

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

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; early disclosure)

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 BC 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

Detection

- 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.
- On November 7, 2019, LifeLabs confirmed that BC resident data had been compromised.
- On November 7, 2019, the Province and Office of the Information and Privacy Commissioner were immediately informed of the incident when it was confirmed that BC 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.

Data

- The data about BC 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. They did this in collaboration with experts familiar with cyber-attacks and negotiations with cyber criminals.
- 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 percent 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 BC 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 Ministries of Health and Citizens' Services, 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

- The OIPC have confirmed that they are conducting a joint investigation with the Privacy Commissioner's office in 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 17, 2019, 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, therefore, 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, and
 - 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.

Life Labs Data Security Issue

November 18, 2019

LifeLabs Key Messages

- The Province is aware that LifeLabs encountered a data breach involving client information.
- LifeLabs confirmed that they were contacted by an unknown source who confirmed they are in possession of LifeLabs' client personal information.
- Safeguarding customer information and data is an essential part of LifeLab's role as a trusted healthcare partner. LifeLabs is taking this matter very seriously and is committed to the privacy and security of customers' personal information.
- LifeLabs is committed to keeping customers, health care partners and all relevant parties informed as we learn more.
- At this time there is no evidence to indicate that BC Government systems are affected by this breach.

BC Government Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it concerns British Columbians' personal information.
- Citizens must have the utmost confidence that their information is secure and protected whenever they access services or provide information to government and other agencies.
- BC Government has policy and standards related to privacy and security that core government must follow.

s.13

-

- BC Government contracts follow procurement rules and include both a privacy protection and a security schedule that clearly set out the requirements that contractors must abide by.
- Those expectations are clearly communicated, and contractors who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.
- If the Province becomes aware that a contractor is non-compliant with any terms of their contract, the Province follows up with the contractor to conduct an investigation, depending on the circumstances.
- BC government has security measures in place to protect networks, systems, and data and there are proactive monitoring tools in place to detect threats.

s.13; s.15

- Office of the Chief Information Officer (OCIO) Security in BC Government is constantly evaluating potential threats, with systems monitoring 24 hours per day, seven days a week.
- The OCIO and every ministry have dedicated staff to monitor and respond to security issues.
- Individual ministries have responsibility for day-to-day security in their respective areas; the OCIO sets the protocols and standards for IT security across government.
- The OCIO is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.

Ministry of Health (MoH) Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it concerns British Columbians' personal health information.

Page 205 of 358

Withheld pursuant to/removed as

s.13 ; s.15

s.13

-

-

- Over 60% of lab tests actually occur in hospitals. There is no evidence to suggest that lab results from hospitals have been compromised through this breach.

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
-
-

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

Detection

- 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.

Data

- 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. They did this in collaboration with experts familiar with cyber-attacks and negotiations with cyber criminals.

- 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

- 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}
- 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.

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

Detection

- 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.

Data

- 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. They did this in collaboration with experts familiar with cyber-attacks and negotiations with cyber criminals.

- 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.
- While LifeLabs' investigation confirmed some lab test results from Ontario customers were also taken during the breach, they are says their investigation has revealed no evidence British Columbians' lab test results were impacted.

Public Notification

- LifeLabs plans issued a public notification to all clients at 10:00 AM on December 17, 2019.
 - LifeLabs worked 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 plans 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.

-
- 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.
- On December 17, 2019 the OIPC issued a joint news release with the Office of the Information and Privacy Commissioner of Ontario (IPC) on the LifeLabs Privacy Breach, IPC/OIPC investigation, and directed 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 and other third-party vendors to address the incident response and to identify and remediate any vulnerabilities within their systems.
- 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.
- Ontario Ministry of Health confirmed that they will not issue a formal public announcement.

Stakeholder consultation

- On December 17, prior to LifeLabs announcement, the Ministries of Health and Citizen Services, along with PHSA officials, held briefings with Health Authorities communications leads, privacy and security leads, and laboratory leads.
- The Ministry of Health officials informed key stakeholders, including Doctors of BC, BC Association of Laboratory Physicians, the regulatory colleges, Diagnostic Accreditation Program and others about the LifeLabs announcement.

Questions & Answers
LifeLabs Data Security Issue
November 29, 2019

Key Messages

- Protecting the privacy of British Columbians~~'-privacy~~ is critical. ~~Citizens~~ People deserve to know their personal information is secure and protected.
- We understand that there was unauthorized access to LifeLabs systems, resulting in B.C. data being taken.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.

s.13

-

s.13

- ~~At this time LifeLab's cyber security firms have not seen any unauthorized use or disclosure of the data.~~

- We encourage British Columbia clients to contact LifeLabs at {phone number and/or website}.

- Approximately 40% of lab tests in BC are done by LifeLabs. The majority of lab tests – about ~~More than 60% – of British Columbia's lab tests happen in~~ hospitals.

s.13

- The ongoing investigation has uncovered no evidence that lab results from hospitals have been ~~compromised~~ ^{s.13} through this breach.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- 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.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs delayed public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time, they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7th – the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- The Office of the Information and Privacy Commissioner was informed of the incident – as it was confirmed that B.C. residents' data was involved. The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- We understand LifeLabs is consulting with law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, with the assistance of world-leading cyber-security firms, and regularly updating the Ministries of Health and the Ministry of Citizen Services.
- LifeLabs is still investigating the full scope of the incident to determine what data has been impacted.
- On Nov. 19 they indicated the breach could include lab results.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

• s.13

- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C.
- They are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- The notification is expected to be indirect, with LifeLabs issuing a media statement, publishing a dedicated website, and advising clients at their service sites.
- LifeLabs plans to have call centres for clients to contact, where they can receive further information as well as free identity theft insurance and dark web monitoring services.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28st that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing criminal investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data could include lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C. and elsewhere.
- Approximately four million British Columbians may have been affected.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs delayed public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

8. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has the personal information of many British Columbians. Officials from Citizens' Services and Health are working to ensure LifeLabs' investigation and response are thorough and effective.

9. Have any government systems been affected?

- There are no indications that B.C. government systems are affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C. with about three million clients.
- We understand they are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- We understand that plan includes call centres for clients to contact, where they can receive further information as well as free identity theft insurance and dark web monitoring services.

11. When will the call centre be set up?

- We expect the call centre to be fully operational within the next 24 to 48 hours.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- LifeLabs can provide updates as to the status of the call centre.

12. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

13. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they delayed public notification to implement further safeguards.
- They wanted to help prevent secondary attacks, given that a public announcement could create a greater risk of harm.

14. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizen Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

15. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs will connect clients with free identify theft insurance and dark web monitoring services.
- LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

16. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- We continue to monitor their response closely and are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

17. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of diagnostic testing services for British Columbians outside a hospital setting (about 40 per cent of all tests in the province).
- For some time, the Province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- The moved to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- B.C. Government service agreements follow procurement rules that include both privacy protection and a security schedule that clearly set out the requirements that contractors must abide by.

18. What does the Ministry do to enforce these protections/policies?

- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

19. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

20. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

21. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

22. Has government paid ransoms for return of data?

- No.

23. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

24. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

25. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

26. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

27. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, it was determined that the most effective way to alert B.C. residents to this incident was to establish a centralized website to answer key questions and provide access to resources, including call centres and fraud-prevention services.
- That site is located at [URL] plus other info for call centre/TU.

Questions & Answers

LifeLabs Data Security Issue

November 29, 2019

Key Messages

- Protecting British Columbians' privacy is critical. Citizens deserve to know their personal information is secure and protected.
- We understand that there was unauthorized access to LifeLabs systems, resulting in B.C. data being taken.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.

• s.13

- At this time LifeLab's cyber security firms have not seen any unauthorized use or disclosure of the data.
- We encourage British Columbia clients to contact LifeLabs at {phone number and/or website}.
- More than 60% of British Columbian's lab tests happen in hospitals.
- The ongoing investigation has uncovered no evidence that lab results from hospitals have been compromised through this breach.
- 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.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs ^{s.13} public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time, they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7th – the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- The Office of the Information and Privacy Commissioner was informed of the incident – as it was confirmed that B.C. residents’ data was involved. The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- We understand LifeLabs is consulting with law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, with the assistance of world-leading cyber-security firms, and regularly updating the Ministries of Health and the Ministry of Citizen Services.
- LifeLabs is still investigating the full scope of the incident to determine what data has been impacted.
- On Nov. 19 they indicated the breach could include lab results.
- ^{s.13}
- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C.

- They are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- The notification is expected to be indirect, with LifeLabs issuing a media statement, publishing a dedicated website, and advising clients at their service sites.
- LifeLabs plans to have call centres for clients to contact, where they can receive further information as well as free identify theft insurance and dark web monitoring services.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28st that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing criminal investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- They have indicated that impacted data could include lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C, and elsewhere.
- Approximately four million British Columbians may have been affected.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- We understand LifeLabs delayed public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

8. Government – through the Ministry of Health and the Ministry of Citizens’ Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab’s breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has the personal information of many British Columbians. Officials from Citizens’ Services and Health are working to ensure LifeLabs’ investigation and response are thorough and effective.

9. Have any government systems been affected?

- There are no indications that B.C. government systems are affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C. with about three million clients.
- We understand they are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- We understand that plan includes call centres for clients to contact, where they can receive further information as well as free identify theft insurance and dark web monitoring services.

11. When will the call centre be set up?

- We expect the call centre to be fully operational within the next 24 to 48 hours.
- LifeLabs can provide updates as to the status of the call centre.

12. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

13. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they delayed public notification to implement further safeguards.
- They wanted to help prevent secondary attacks, given that a public announcement could create a greater risk of harm.

14. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizen Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

15. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs will connect clients with free identify theft insurance and dark web monitoring services.
- LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

16. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.

- We continue to monitor their response closely and are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

17. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of diagnostic testing services for British Columbians outside a hospital setting (about 40 per cent of all tests in the province).
- For some time, the Province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- The moved to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- B.C. Government service agreements follow procurement rules that include both privacy protection and a security schedule that clearly set out the requirements that contractors must abide by.

18. What does the Ministry do to enforce these protections/policies?

- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

19. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

20. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

21. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

22. Has government paid ransoms for return of data?

- No.

23. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

25. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

26. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

27. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, it was determined that the most effective way to alert B.C. residents to this incident was to establish a centralized website to answer key questions and provide access to resources, including call centres and fraud-prevention services.
- That site is located at [URL] plus other info for call centre/TU.

Questions & Answers
LifeLabs Data Security Issue
November 29, 2019

Key Messages

- Protecting British Columbians' privacy is critical. Citizens deserve to know their personal information is secure and protected.
- We understand that there was unauthorized access to LifeLabs systems, resulting in B.C. data being taken.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.

s.13

- At this time LifeLab's cyber security firms have not seen any further unauthorized use or disclosure of the data.
- We encourage British Columbia clients to contact LifeLabs at {phone number and/or website}.
- More than 60% of British Columbian's lab tests happen in hospitals.
- The ongoing investigation has uncovered no evidence that lab results from hospitals have been compromised through this breach.
- 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.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide^{s.13} public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time, they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7, 2019~~th~~ – the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- The Office of the Information and Privacy Commissioner was informed of the incident – as soon as it was confirmed that B.C. residents' data was involved. The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- We understand LifeLabs is consulting with law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, with the assistance of world-leading cyber-security firms, and regularly updating the Ministries of Health and the Ministry of Citizens' Services.
- LifeLabs is still investigating the full scope of the incident to determine what data has been impacted.
- On Nov. 19 they indicated the breach could include lab results.

s.13

- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- They are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- The notification is expected to be indirect, with LifeLabs issuing a media statement, publishing a dedicated website, and advising clients at their service sites.
- LifeLabs plans to have call centres for clients to contact, where they can receive further information and as well as free identify theft insurance and dark web monitoring services.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing criminal investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data could include lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C. and elsewhere.
- Approximately four million British Columbians may have been affected.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide^{s.13} public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

8. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has the personal information of many British Columbians. Officials from Citizens' Services and Health are working to ensure LifeLabs' investigation and response are thorough and effective.

9. Have any government systems been affected?

- There are no indications that B.C. government systems are affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C.
- We understand they are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- We understand that plan includes call centres for clients to contact, where they can receive further information and as well as free identify theft insurance and dark web monitoring services.

11. When will the call centre be set up?

- We expect the call centre to be fully operational within the next 24 to 48 hours.
- LifeLabs can provide updates as to the status of the call centre. Questions related to this matter should be directed to LifeLabs.

12. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

13. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide delayed public notification until they could implement further safeguards.
- They wanted to help prevent secondary attacks, given that a public announcement could create a greater risk of harm.

14. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizens' Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

15. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- LifeLabs will connect clients with free identify theft insurance and dark web monitoring services.
- LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

16. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- We continue to monitor their response closely and are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

17. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of diagnostic testing services for British Columbians outside a hospital setting (about 40 per cent of all tests in the province).
- For some time, the Province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- The moved to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- B.C. Government service agreements follow procurement rules that include both privacy protection and a security schedule that clearly set out the requirements that contractors must abide by.

s.13

18. What does the Ministry do to enforce these protections/policies?

- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- If any evidence is received that a contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

19. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

20. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

21. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

22. Has government paid ransoms for return of data?

- No.

23. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

25. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

26. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

27. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, it was determined that the most effective way to alert B.C. residents to this incident was to establish a centralized website to answer key questions and provide access to resources, including call centres and fraud-prevention services.
- That site is located at [URL] plus other info for call centre/TU.

Questions & Answers

LifeLabs Data Security Issue

November 29, 2019

Key Messages

- Protecting British Columbians' privacy is critical. Citizens deserve to know their personal information is secure and protected.
- We understand there has been unauthorized access to LifeLabs systems, resulting in B.C. data being taken.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.

s.13

- At this time LifeLab's cyber security firms have not seen any further unauthorized use or disclosure of the data.
- We encourage British Columbia clients to contact LifeLabs at {phone number and/or website}.
- More than 60% of British Columbian's lab tests happen in hospitals.
- The ongoing investigation has uncovered no evidence that lab results from hospitals have been compromised through this breach.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.

- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time, they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7, 2019 – the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- The Office of the Information and Privacy Commissioner was informed of the incident as soon as it was confirmed that B.C. residents' data was involved. The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- We understand LifeLabs is consulting with law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, with the assistance of world-leading cyber-security firms, and regularly updating the Ministries of Health and the Ministry of Citizens' Services.
- LifeLabs is still investigating the full scope of the incident to determine what data has been impacted.
- On Nov. 19 they indicated the breach could include lab results.
- ^{s.13}
- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C.
- They are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.

- The notification is expected to be indirect, with LifeLabs issuing a media statement, publishing a dedicated website, and advising clients at their service sites.
 - LifeLabs plans to have call centres for clients to contact, where they can receive further information and as well as free identify theft insurance and dark web monitoring services.
-

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing criminal investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data could include lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C, and elsewhere.
- Approximately four million British Columbians may have been affected.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

8. Government – through the Ministry of Health and the Ministry of Citizens’ Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab’s breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has the personal information of many British Columbians. Officials from Citizens’ Services and Health are working to ensure LifeLabs’ investigation and response are thorough and effective.

9. Have any government systems been affected?

- There are no indications that B.C. government systems are affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C.
- We understand they are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- We understand that plan includes call centres for clients to contact, where they can receive further information and as well as free identity theft insurance and dark web monitoring services.

11. When will the call centre be set up?

- We expect the call centre to be fully operational within the next 24 to 48 hours.
- LifeLabs can provide updates as to the status of the call centre. Questions related to this matter should be directed to LifeLabs.

12. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.

- Questions related to this matter should be directed to LifeLabs.

13. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide public notification until they could implement further safeguards.
- They wanted to help prevent secondary attacks, given that a public announcement could create a greater risk of harm.

14. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizens' Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

15. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs will connect clients with free identify theft insurance and dark web monitoring services.
- LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

16. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.

- We continue to monitor their response closely and are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
-

Contract Management – LifeLabs & Ministry of Health

17. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of diagnostic testing services for British Columbians outside a hospital setting (about 40 per cent of all tests in the province).
- For some time, the Province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- This process changed to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- 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.

18. What does the Ministry do to enforce these protections/policies?

- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

19. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.

- Questions on this matter should be directed to LifeLabs.

20. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

21. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

22. Has government paid ransoms for return of data?

- No.

23. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

25. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

26. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

27. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, it was determined that the most effective way to alert B.C. residents to this incident was to establish a centralized website to answer key questions and provide access to resources, including call centres and fraud-prevention services.
- That site is located at [URL] plus other info for call centre/TU.

Questions & Answers
LifeLabs Data Security Issue
November 29, 2019

Key Messages

- Protecting British Columbians' privacy is critical. Citizens deserve to know their personal information is secure and protected.
- We understand there has been unauthorized access to LifeLabs systems, resulting in B.C. data being taken.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.

s.13

- At this time LifeLab's cyber security firms have not seen any further unauthorized use or disclosure of the data.
- We encourage British Columbia clients to contact LifeLabs.

- More than 60% of British Columbia's lab tests happen in hospitals. There is no indication that this breach affected any of that data.

s.13

s.13

• ***If pressed:***

- Announcing these types of incidents can attract immediate secondary cyber attacks. We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

s.13

Formatted: List Paragraph,bullet 1,BN 1,Paperitemletter,Dot pt,Liste 1,table bullets,TOC style,lp1,Bullet List - spacing,List Paragraph1,Recommendation,List Paragraph11,L,List Paragraph2,CV text,Table text,F5 List Paragraph,List Paragraph111,列出段落, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

Background

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time, they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7, 2019 – the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- The Office of the Information and Privacy Commissioner was informed of the incident as soon as it was confirmed that B.C. residents' data was involved. The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- We understand LifeLabs is consulting with law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, with the assistance of world-leading cyber-security firms, and regularly updating the Ministries of Health and the Ministry of Citizens' Services.
- LifeLabs is still investigating the full scope of the incident to determine what data has been impacted.
- On Nov. 19 they indicated the breach could include lab results.

s.13

- LifeLabs undertakes about 40% of lab testing in B.C.
- They are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- The notification is expected to be indirect, with LifeLabs issuing a media statement, publishing a dedicated website, and advising clients at their service sites.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- LifeLabs plans to have call centres for clients to contact, where they can receive further information and as well as free identity theft insurance and dark web monitoring services.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing criminal investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data could include lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C. and elsewhere.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- Approximately four million British Columbians may have been affected.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. LifeLabs and government have known about this breach for ~~nearly a month and a half~~ – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

8. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- LifeLabs has the personal information of many British Columbians. Officials from Citizens' Services and Health are working to ensure LifeLabs' investigation and response are thorough and effective.

9. Have any government systems been affected?

- There are no indications that B.C. government or Health Authority systems are affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs undertakes about 40% of lab testing in B.C.
- We understand they are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- We understand that plan includes call centres for clients to contact, where they can receive further information and as well as free identity theft insurance and dark web monitoring services.

11. When will the call centre be set up?

- We expect the call centre to be fully operational within the next 24 to 48 hours.
- LifeLabs can provide updates as to the status of the call centre. Questions related to this matter should be directed to LifeLabs.

12. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

13. Why didn't LifeLabs alert affected clients that their information was breached before now?

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide public notification until they could implement further safeguards.
- They wanted to help prevent secondary attacks, given that a public announcement could create a greater risk of harm.

14. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizens' Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

15. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs will connect clients with free identify theft insurance and dark web monitoring services.
- LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

s.13

16. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- We continue to monitor their response closely and are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
-

Contract Management – LifeLabs & Ministry of Health

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

17. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of lab testing services for British Columbians outside a hospital setting (about 40% of all lab tests in the province).
- For some time, the Province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- This process changed to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- 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.

18. What does the Ministry do to enforce these protections/policies?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor 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 specific incident are still being determined, based on our agreement with LifeLabs.

19. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

20. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

21. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

22. Has government paid ransoms for return of data?

- No.

23. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

25. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

26. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

27. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, it was determined that the most effective way to alert B.C. residents to this incident was to establish a centralized website to answer key questions and provide access to resources, including call centres and fraud-prevention services.

Questions & Answers

LifeLabs Data Security Issue

November 29, 2019

Key Messages

- Protecting British Columbians' privacy is critical. Citizens deserve to know their personal information is secure and protected.
- We understand there has been unauthorized access to LifeLabs systems, resulting in B.C. data being taken.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.

s.13

- At this time LifeLab's cyber security firms have not seen any further unauthorized use or disclosure of the data.
- We encourage British Columbia clients to contact LifeLabs.
- More than 60% of British Columbian's lab tests happen in hospitals. There is no indication that this breach affected any of that data.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks. We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time, they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7, 2019 – the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- The Office of the Information and Privacy Commissioner was informed of the incident as soon as it was confirmed that B.C. residents' data was involved. The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- We understand LifeLabs is consulting with law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, with the assistance of world-leading cyber-security firms, and regularly updating the Ministries of Health and the Ministry of Citizens' Services.
- LifeLabs is still investigating the full scope of the incident to determine what data has been impacted.
- On Nov. 19 they indicated the breach could include lab results.
- ^{s.13}
- LifeLabs undertakes about 40% of lab testing in B.C.
- They are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- The notification is expected to be indirect, with LifeLabs issuing a media statement, publishing a dedicated website, and advising clients at their service sites.
- LifeLabs plans to have call centres for clients to contact, where they can receive further information and as well as free identity theft insurance and dark web monitoring services.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing criminal investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data could include lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C, and elsewhere.
- Approximately four million British Columbians may have been affected.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. LifeLabs and government have known about this breach for a month and a half – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

8. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- LifeLabs has the personal information of many British Columbians. Officials from Citizens' Services and Health are working to ensure LifeLabs' investigation and response are thorough and effective.

9. Have any government systems been affected?

- There are no indications that B.C. government or Health Authority systems are affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs undertakes about 40% of lab testing in B.C.
- We understand they are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- We understand that plan includes call centres for clients to contact, where they can receive further information and as well as free identity theft insurance and dark web monitoring services.

11. When will the call centre be set up?

- We expect the call centre to be fully operational within the next 24 to 48 hours.
- LifeLabs can provide updates as to the status of the call centre. Questions related to this matter should be directed to LifeLabs.

12. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

13. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide public notification until they could implement further safeguards.
- They wanted to help prevent secondary attacks, given that a public announcement could create a greater risk of harm.

14. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizens' Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

15. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs will connect clients with free identity theft protection and dark web monitoring services.
- LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

16. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- We continue to monitor their response closely and are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

17. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of lab testing services for British Columbians outside a hospital setting (about 40% of all lab tests in the province).
- For some time, the Province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- This process changed to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- 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.

18. What does the Ministry do to enforce these protections/policies?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor 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 specific incident are still being determined, based on our agreement with LifeLabs.

19. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

20. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

21. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

22. Has government paid ransoms for return of data?

- No.

23. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

25. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

26. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

27. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, it was determined that the most effective way to alert B.C. residents to this incident was to establish a centralized website to answer key questions and provide access to resources, including call centres and fraud-prevention services.

Questions & Answers

LifeLabs Data Security Issue

December 16, 2019

Key Messages

- This is very concerning. The protection of British Columbians' privacy is critical.
- B.C. is committed to strong privacy and security controls.
- Most of British Columbian's lab tests happen in hospitals and that data is not affected by this breach.
- While LifeLabs is a private company, the Province is closely monitoring and consulting with them as they address this incident.
- The Province understands LifeLabs has hired world-leading cyber security firms to investigate and respond – including implementing additional safeguards to further secure their networks going forward.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.
- The Province will continue to work with LifeLabs to help them ensure that their investigation and response are thorough and effective.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On December 17, 2019, it was announced that LifeLabs, the private company responsible for conducting approximately 34% of B.C. lab testing services, experienced a significant data breach.
- 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 also taken during the breach. LifeLabs 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 the public, while also taking steps to secure their information systems against future attack.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- We understand LifeLabs was able to secure the data taken during the breach by making a payment.
- Questions on this matter should be directed to LifeLabs.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data includes 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 also taken during the breach. LifeLabs will notify those customers directly.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C, and elsewhere.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. Do you feel LifeLab's response has been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with privacy commissioners in several provinces and with B.C.'s Ministries of Health and Citizens' Services to accomplish this notification as efficiently as possible.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.
- The goal was to prevent against any disruptions to service delivery that could negatively impact patient care.

8. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- Officials from Citizens' Services and Health are working to help LifeLabs ensure their investigation and response are thorough and effective.

9. Have any government systems been affected?

- B.C. government and Health Authority systems are not affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs is providing all customers access to free identity theft insurance of up to \$50,000 and monitoring services.
- We encourage anyone who has had testing done at LifeLabs to contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.

11. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

12. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide public notification until they could implement further safeguards against secondary attacks.
- Their goal was to prevent against any disruptions to service delivery that could negatively impact patient care.

13. Does government support LifeLab's approach and timing?

- LifeLabs has been working with privacy commissioners, their legal counsel, external cyber-security experts, and cyber-security and privacy officials at the Ministry of Citizens' Services.
- LifeLabs is a private company operating in B.C., Ontario, Saskatchewan and New Brunswick and must meet multiple legislative notification and disclosure requirements, including the process of engaging law enforcement.

14. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- LifeLabs has paid to secure the breached data.
- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs is providing all customers access to free identity theft insurance up to \$50,000 and monitoring services. LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

15. Does the Province believe LifeLab's mitigation responses for clients are enough?

- LifeLabs is a private company and we continue to monitor their response closely. We are pursuing formal assurances and documentation from LifeLabs that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

16. The Ministry of Health holds a contract with LifeLabs – what protections are in place when data is in the custody of a contractor or service provider?

- 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.

17. What does the Ministry do to enforce these protections/policies?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor 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.

18. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement and privacy commissioners, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

19. How can people have confidence that their health records are secure in B.C.?

- Most of British Columbia's lab tests happen in hospitals and that data is not affected by this breach.
- Government and health authority systems were not impacted. They have security measures in place to prevent infiltrations, and proactive monitoring tools to detect threats.
- Protection of government data and networks is a top priority, especially where it concerns British Columbians' personal information.
- If there are breaches – 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.

- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

20. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

21. Has government paid ransoms for return of data?

- No.

22. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

23. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

25. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

26. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, LifeLabs determined that the most effective way to alert B.C. residents was to establish a centralized website to answer key questions and provide access to resources, including to free identity theft insurance and monitoring services.

27. The Information and Privacy Commissioner has called for changes to the *Personal Information Privacy Act*. Why hasn't the Province acted?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

28. Does government intend on amending the Personal Information Protection Act?

- PIPA applies to over 300,000 private organizations so any changes must be carefully considered to ensure the intended result is achieved.
- We have received recommendations from the Office of the Information and Privacy Commissioner, past Special Committees, advocacy groups and the public.
- This feedback will help inform any future legislative or policy changes to improve the way organizations protect personal information.

Questions & Answers
LifeLabs Data Security Issue
December 16, 2019

Key Messages

- This is very concerning. The protection of British Columbians' privacy is critical.
- B.C. is committed to strong privacy and security controls.
- Most of British Columbian's lab tests happen in hospitals and that data is not affected by this breach.
- While LifeLabs is a private company, the Province is closely monitoring and consulting with them as they address this incident.
- The Province understands LifeLabs has hired world-leading cyber security firms to investigate and respond – including implementing additional safeguards to further secure their networks going forward.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.
- The Province will continue to work with LifeLabs to help them ensure that their investigation and response are thorough and effective.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.
- ~~Protecting British Columbians' privacy is critical.~~
- ~~Citizens deserve to know their personal information is secure and protected.~~
- ~~We understand there has been unauthorized access to LifeLabs systems^{s.13} resulting in B.C. data being taken.~~
- ~~The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.~~

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.

• s.13

- At this time LifeLab's cyber security firms have not seen any further unauthorized use or disclosure of the data.
- We encourage British Columbia clients to contact LifeLabs.
- More than 60% of British Columbia's lab tests happen in hospitals.
- There is no indication that this breach affected any of that data.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

•

Background

• s.13

Formatted: No bullets or numbering

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- LifeLabs confirmed that B.C. resident data had been compromised on November 7, 2019—the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- The Office of the Information and Privacy Commissioner was informed of the incident as soon as it was confirmed that B.C. residents' data was involved. The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- We understand LifeLabs is consulting with law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, with the assistance of world-leading cyber security firms, and regularly updating the Ministries of Health and the Ministry of Citizens' Services.
- LifeLabs is still investigating the full scope of the incident to determine what data has been impacted.
- On November 19th, they indicated the breach could include lab results.
- s.13
- LifeLabs undertakes about 40% of lab testing in B.C.
- They are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- The notification is expected to be indirect, with LifeLabs issuing a media statement, publishing a dedicated website, and advising clients at their service sites.
- The date of public notification has been set for December 17th, so the Province will be ready to address media questions in response to this issue (no proactive release is planned).
- The Office of the Information and Privacy Commissioner (OIPC) has indicated they will issue a statement on December 17th as well.
- s.13

Formatted: Font: (Default) Calibri, Not Bold, Font color: Auto

Formatted: Not Superscript/ Subscript

Formatted: Font: (Default) Calibri, Not Bold, Font color: Auto

Formatted: Font: (Default) Calibri, Not Bold, Font color: Auto

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- On December 17, 2019, it was announced that LifeLabs, the private company responsible for conducting approximately 34% of B.C. lab testing services, experienced a significant data breach.
- 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 also taken during the breach. LifeLabs 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 the public, while also taking steps to secure their information systems against future attack. LifeLabs plans to have call centres for clients to contact, where they can receive further information and as well as free identity theft insurance and dark web monitoring services.

Formatted: Space After: 6 pt, Line spacing: single, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm, Border: Bottom: (No border)

Formatted: Space After: 6 pt, Line spacing: single, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm, Border: Bottom: (No border)

Formatted: Font: (Default) Calibri, 12 pt

Formatted: Space After: 6 pt, Line spacing: single, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm, Border: Bottom: (No border)

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- We understand LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation. was able to secure the data taken during the breach by making a payment.

- Questions on this matter should be directed to LifeLabs.

•

~~If pressed:~~

- ~~Releasing information during an ongoing criminal investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.~~

s.13

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data s.13 includes 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 also taken during the breach. LifeLabs will notify those customers directly.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C. and elsewhere.
- ~~Approximately four million British Columbians may have been affected.~~

s.13

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

7. ~~LifeLabs and government have known about this breach for a month and a half—d~~Do you feel the LifeLab's actions taken to date have response has been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with privacy commissioners in several provinces and with the B.C.'s Ministries of Health and Citizens' Services ~~throughout the process to prepare resources to~~ accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

s.13

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.
- The goal was to prevent against any disruptions to service delivery that could negatively impact patient care.

s.13

8. ~~Government—through the Ministry of Health and the Ministry of Citizens' Services—has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?~~

- LifeLabs is a private company and is leading the investigation and response to the incident.
- ~~LifeLabs has the personal information of many British Columbians.~~ Officials from Citizens' Services and Health are working to help ensure LifeLabs' ensure their investigation and response are thorough and effective.

9. Have any government systems been affected?

- ~~There are no indications that B.C. government or and Health Authority systems are not~~ affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs undertakes about 40% of lab testing in B.C.
- We understand they are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- LifeLabs is providing all customers access to free identity theft insurance of up to \$50,000 and monitoring services.
- We encourage anyone who has had testing done at LifeLabs to contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.
- We understand that plan includes call centres for clients to contact, where they can receive further information and as well as free identify theft insurance and dark web monitoring services.

11. When will the call centre be set up?

- We expect the call centre to be fully operational December 16th.
- LifeLabs can provide updates as to the status of the call centre. Questions related to this matter should be directed to LifeLabs.

s.13

12.11. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

13.12. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide public notification until they could implement further safeguards against secondary attacks.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- Their goal was to prevent against any disruptions to service delivery that could negatively impact patient care.
- They wanted to help prevent secondary attacks, given that a public announcement could create a greater risk of harm.

s.13

14.13. Does government support LifeLab's approach and timing?

- LifeLabs has been working with privacy commissioners, their legal counsel, external cyber-security experts, and cyber-security and privacy officials at the Ministry of Citizens' Services in this matter.
- LifeLabs operates as a private company operating in B.C., Ontario, Saskatchewan and New Brunswick and must meet different multiple legislative notification and disclosure requirements, including the process of engagement with RCMP or other law enforcement.

15.14. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- LifeLabs has paid to secure the breached data.
- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs is providing all customers access to free identity theft insurance up to \$50,000 and monitoring services. LifeLabs will connect clients with free identity theft protection and dark web monitoring services.
- LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

s.13

16.15. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- We continue to monitor their response closely. We and are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Formatted: Space After: 6 pt, Add space between paragraphs of the same style

Contract Management – LifeLabs & Ministry of Health

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

17.16. The Ministry of Health holds a contract with LifeLabs – what protections are in place when when government data is in the custody of a contractor or service provider?

- ~~Lif Labs provides the majority of lab testing services for British Columbians outside a hospital setting (about 40% of all lab tests in the province).~~
- ~~For some time, the Province's Medical Service Plan covered the costs of those tests on a fee-for-service model.~~
- ~~This process changed to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.~~
- 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.

18.17. What does the Ministry do to enforce these protections/policies?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor 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 ~~specific incident are still being~~will be determined, based on our agreement with LifeLabs.

19.18. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement and, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

20.19. How can people have confidence that their health records are secure in B.C.?

- Most of British Columbia's lab tests happen in hospitals and that data is not affected by this breach.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- Government and health authority systems were not impacted. They have security measures in place to prevent infiltrations, and proactive monitoring tools to detect threats.
- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- If there are breaches – 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.
- —
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

21.20. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

22.21. Has government paid ransoms for return of data?

- No.

23.22. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

24.23. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

25.24. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

26.25. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this—

27.26. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, it was LifeLabs determined that the most effective way to alert B.C. residents was to establish a centralized website to answer key questions and provide access to resources, including to free identity theft insurance and monitoring services, call centres and fraud prevention services.

•

Formatted: List Paragraph,bullet 1,BN 1,Paperitemletter,Dot pt,Liste 1,table bullets,TOC style,lp1,Bullet List - spacing,List Paragraph1,Recommendation,List Paragraph11,L,List Paragraph2,CV text,Table text,F5 List Paragraph,List Paragraph111,列出段落

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

28.27. The Information and Privacy Commissioner has called for changes to the *Personal Information Privacy Act*. Why hasn't the Province acted?

Protecting the privacy rights of British Columbians is a top priority.

Formatted: Font: 12 pt, Condensed by 0.15 pt

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.
- It is important that the people of B.C. know that there are rules and guidelines that protect their personal information.
- The Personal Information Protection Act (PIPA) governs the way businesses, non-profits, political parties and other organizations use personal information.
- PIPA helps protect British Columbians' personal information and governs how it's used by these organizations.
- PIPA applies to over 300,000 private organizations so any changes must be carefully considered to ensure the intended result is achieved.

Formatted: Font: 12 pt, Condensed by 0.15 pt

Formatted: Font: 12 pt, Not Italic, Condensed by 0.15 pt

Formatted: Font: 12 pt, Condensed by 0.15 pt

29.28. Does government intend on amending the Personal Information Protection Act?

- PIPA applies to over 300,000 private organizations so any changes must be carefully considered to ensure the intended result is achieved.
- Making meaningful improvements to the way organizations handle and share records is not something we can rush for the sake of a good headline or to score political points.
- We have received recommendations from the Office of the Information and Privacy Commissioner, past Special Committees, advocacy groups and the public.
- This feedback will help inform any future legislative or policy changes to improve the way organizations protect personal information.

Questions & Answers

LifeLabs Data Security Issue

December 16, 2019

Key Messages

- Protecting British Columbians' privacy is critical.
- Citizens deserve to know their personal information is secure and protected.
- We understand there has been unauthorized access to LifeLabs systems, resulting in B.C. data being taken.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.

• s.13

- At this time LifeLab's cyber security firms have not seen any further unauthorized use or disclosure of the data.
- We encourage British Columbia clients to contact LifeLabs.
- More than 60% of British Columbian's lab tests happen in hospitals.
- There is no indication that this breach affected any of that data.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time, they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7, 2019 – the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- The Office of the Information and Privacy Commissioner was informed of the incident as soon as it was confirmed that B.C. residents' data was involved. The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- We understand LifeLabs is consulting with law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, with the assistance of world-leading cyber-security firms, and regularly updating the Ministries of Health and the Ministry of Citizens' Services.
- LifeLabs is still investigating the full scope of the incident to determine what data has been impacted.
- On November 19th, they indicated the breach could include lab results.
- s.13
- LifeLabs undertakes about 40% of lab testing in B.C.
- They are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- The notification is expected to be indirect, with LifeLabs issuing a media statement, publishing a dedicated website, and advising clients at their service sites.
- The date of public notification has been set for December 17th, so the Province will be ready to address media questions in response to this issue (no proactive release is planned).
- The Office of the Information and Privacy Commissioner (OIPC) has indicated they will issue a statement on December 17th as well.

- s.13

-

- LifeLabs plans to have call centres for clients to contact, where they can receive further information and as well as free identity theft insurance and dark web monitoring services.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing criminal investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data could include lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C, and elsewhere.
- Approximately four million British Columbians may have been affected.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. LifeLabs and government have known about this breach for a month and a half – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

8. Government – through the Ministry of Health and the Ministry of Citizens’ Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab’s breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has the personal information of many British Columbians. Officials from Citizens’ Services and Health are working to ensure LifeLabs’ investigation and response are thorough and effective.

9. Have any government systems been affected?

- There are no indications that B.C. government or Health Authority systems are affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs undertakes about 40% of lab testing in B.C.
- We understand they are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- We understand that plan includes call centres for clients to contact, where they can receive further information and as well as free identity theft insurance and dark web monitoring services.

11. When will the call centre be set up?

- We expect the call centre to be fully operational December 16th.
- LifeLabs can provide updates as to the status of the call centre. Questions related to this matter should be directed to LifeLabs.

12. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

13. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide public notification until they could implement further safeguards.
- They wanted to help prevent secondary attacks, given that a public announcement could create a greater risk of harm.

14. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizens' Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

15. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs will connect clients with free identity theft protection and dark web monitoring services.
- LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

16. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- We continue to monitor their response closely and are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

17. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of lab testing services for British Columbians outside a hospital setting (about 40% of all lab tests in the province).
- For some time, the Province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- This process changed to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- 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.

18. What does the Ministry do to enforce these protections/policies?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor 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 specific incident are still being determined, based on our agreement with LifeLabs.

19. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

20. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

21. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

22. Has government paid ransoms for return of data?

- No.

23. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

25. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C related to the notification process in data-breach situations.

26. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

27. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.

- In this situation, it was determined that the most effective way to alert B.C. residents to this incident was to establish a centralized website to answer key questions and provide access to resources, including call centres and fraud-prevention services.

28. The Information and Privacy Commissioner has called for changes to the *Personal Information Privacy Act*. Why hasn't the Province acted?

- Protecting the privacy rights of British Columbians is a top priority.
- It is important that the people of B.C. know that there are rules and guidelines that protect their personal information.
- The *Personal Information Protection Act (PIPA)* governs the way businesses, non-profits, political parties and other organizations use personal information.
- PIPA helps protect British Columbians' personal information and governs how it's used by these organizations.
- PIPA applies to over 300,000 private organizations so any changes must be carefully considered to ensure the intended result is achieved.

29. Does government intend on amending the *Personal Information Protection Act*?

- Making meaningful improvements to the way organizations handle and share records is not something we can rush for the sake of a good headline or to score political points.
- We have received recommendations from the Office of the Information and Privacy Commissioner, past Special Committees, advocacy groups and the public.
- This feedback will help inform any future legislative or policy changes to improve the way organizations protect personal information.

Questions & Answers

LifeLabs Data Security Issue

December 17, 2019

Key Messages

- This is very concerning. The protection of British Columbians' privacy is critical.
- While LifeLabs is a private company, the Province is closely monitoring and consulting with them as they address this incident.
- The Province understands LifeLabs has hired world-leading cyber security firms to investigate and respond – including implementing additional safeguards to further secure their networks going forward.
- B.C. is committed to strong privacy and security controls. Government of B.C. and Health Authority systems were not affected by this breach.
- Most of British Columbians' lab tests happen in hospitals and that data is not affected by this breach.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.
- The Province will continue to work with LifeLabs to help them ensure that their investigation and response are thorough and effective.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On December 17, 2019, it was announced that LifeLabs, the private company responsible for conducting approximately 34% of B.C. lab testing services, experienced a significant data breach.
- 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 also taken during the breach. LifeLabs 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, law enforcement and the B.C. Ministries of Health and Citizens' Services, LifeLabs is notifying the public, while also taking steps to secure their information systems against future attack.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs has told us they were able to secure the data taken during the breach by making a payment.
- They did this in collaboration with experts familiar with cyber-attacks and negotiations.
- Questions on this matter should be directed to LifeLabs.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has reported the incident to law enforcement.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data includes 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 also taken during the breach. LifeLabs will notify those customers directly.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C. and elsewhere.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. Do you feel LifeLab's response has been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been the subject of a privacy breach.
- LifeLabs consulted with privacy commissioners in several provinces and with B.C.'s Ministries of Health and Citizens' Services to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively addressing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.
- The goal was to prevent against any disruptions to service delivery that could negatively impact patient care.

8. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- Officials from Citizens' Services and Health are working to help LifeLabs ensure their investigation and response are thorough and effective.

9. Have any government systems been affected?

- No. B.C. government and Health Authority systems are not affected by this breach.
- Government systems have security measures in place to protect against 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs is providing all customers access to free identity theft insurance of up to \$50,000 and monitoring services.
- We encourage anyone who has had testing done at LifeLabs to contact them directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.

11. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

12. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide public notification until they could implement further safeguards against secondary attacks.
- Their goal was to prevent against any disruptions to service delivery that could negatively impact patient care.

13. Does government support LifeLab's approach and timing?

- LifeLabs has been working with privacy commissioners, their legal counsel, external cyber-security experts, and cyber-security and privacy officials at the Ministry of Citizens' Services.
- LifeLabs is a private company operating in B.C., Ontario, Saskatchewan and New Brunswick and must meet multiple legislative notification and disclosure requirements, including the process of engaging law enforcement.

14. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- LifeLabs tells us they have paid to secure the breached data.
- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs is providing all customers access to free identity theft insurance up to \$50,000 and monitoring services. LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

15. Does the Province believe LifeLab's mitigation responses for clients are enough?

- LifeLabs is a private company and we continue to monitor their response closely. We are pursuing formal assurances and documentation from LifeLabs that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

16. The Ministry of Health holds a contract with LifeLabs – what protections are in place when data is in the custody of a contractor or service provider?

- 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.

17. What does the Ministry do to enforce these protections/policies?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor 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.

18. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement and privacy commissioners, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

19. How can people have confidence that their health records are secure in B.C.?

- Most of British Columbian's lab tests happen in hospitals and that data is not affected by this breach.
- Government and health authority systems were not impacted. They have security measures in place to prevent infiltrations, and proactive monitoring tools to detect threats.
- Protection of government data and networks is a top priority, especially where it concerns British Columbians' personal information.
- If there are breaches – 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.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

20. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

21. Has government paid ransoms for return of data?

- No.

22. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

23. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C related to the notification process in data-breach situations.

25. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

26. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, LifeLabs determined that the most effective way to alert B.C. residents was to establish a centralized website to answer key questions and provide access to resources, including to free identity theft insurance and monitoring services.

27. The Information and Privacy Commissioner has called for changes to the *Personal Information Privacy Act*. Why hasn't the Province acted?

- It is important that the people of B.C. know that there are rules and guidelines that protect their personal information.
- The Personal Information Protection Act (PIPA) governs the way businesses, non-profits, political parties and other organizations use personal information.
- PIPA applies to over 300,000 private organizations so any changes must be carefully considered to ensure the intended result is achieved.

28. Does government intend on amending the Personal Information Protection Act?

- PIPA applies to over 300,000 private organizations, so any changes must be carefully considered to ensure the intended result is achieved.
- We have received recommendations from the Office of the Information and Privacy Commissioner, past Special Committees, advocacy groups and the public.
- This feedback will help inform any future legislative or policy changes to improve the way organizations protect personal information.

Questions & Answers

LifeLabs Data Security Issue

December 17, 2019

Key Messages

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time, they did not believe that any patient data had been compromised.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively addressing it.
- The Province understands LifeLabs has hired world-leading cyber security firms to investigate and respond – including implementing additional safeguards to further secure their networks going forward.
- The Ministries of Health and Citizens' Services required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- On November 7, 2019 LifeLabs confirmed that B.C. resident data had been compromised, and that the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
 - LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C, and elsewhere.
 - Approximately four million British Columbians may have been affected.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- The Office of the Information and Privacy Commissioner was informed of the incident as soon as it was confirmed that B.C. residents' data was involved.
- LifeLabs has also reported the incident to law enforcement.
- The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- This is very concerning. The protection of British Columbians' privacy is critical.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they are taking adequate security measures to prevent this from re-occurring.
- B.C. is committed to strong privacy and security controls. Government of B.C. and Health Authority systems were not affected by this breach.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.
- The Province will continue to work with LifeLabs to help them ensure that their investigation and response are thorough and effective.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On December 17, 2019, LifeLabs announced they had experienced a significant data breach.
- 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 also taken during the breach. LifeLabs 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, law enforcement and the B.C. Ministries of Health and Citizens' Services, LifeLabs is notifying the public, while also taking steps to secure their information systems against future attack.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs has told us they were able to secure the data taken during the breach by making a payment.
- They did this in collaboration with experts familiar with cyber-attacks and negotiations.
- Questions on this matter should be directed to LifeLabs.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has reported the incident to law enforcement.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data includes 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 also taken during the breach. LifeLabs will notify those customers directly.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C. and elsewhere.
- Approximately four million British Columbians may have been affected.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. Do you feel LifeLab's response has been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been the subject of a privacy breach.
- LifeLabs consulted with privacy commissioners in several provinces and with B.C.'s Ministries of Health and Citizens' Services to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively addressing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.
- The goal was to prevent against any disruptions to service delivery that could negatively impact patient care.

8. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- Officials from Citizens' Services and Health are working to help LifeLabs ensure their investigation and response are thorough and effective.

9. Have any government systems been affected?

- No. B.C. government and Health Authority systems are not affected by this breach.
- Government systems have security measures in place to protect against 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs is providing all customers access to free identity theft insurance of up to \$50,000 and monitoring services.
- We encourage anyone who has had testing done at LifeLabs to contact them directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.

11. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

12. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide public notification until they could implement further safeguards against secondary attacks.
- Their goal was to prevent against any disruptions to service delivery that could negatively impact patient care.

13. Does government support LifeLab's approach and timing?

- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively addressing it.
- LifeLabs has been working with privacy commissioners, their legal counsel, external cyber-security experts, and cyber-security and privacy officials at the Ministry of Citizens' Services.
- LifeLabs is a private company operating in B.C., Ontario, Saskatchewan and New Brunswick and must meet multiple legislative notification and disclosure requirements, including the process of engaging law enforcement.

14. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- LifeLabs tells us they have paid to secure the breached data.
- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs is providing all customers access to free identity theft insurance up to \$50,000 and monitoring services. LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

15. Does the Province believe LifeLab's mitigation responses for clients are enough?

- LifeLabs is a private company and we continue to monitor their response closely. We are pursuing formal assurances and documentation from LifeLabs that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

16. The Ministry of Health holds a contract with LifeLabs – what protections are in place when data is in the custody of a contractor or service provider?

- 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.

17. What does the Ministry do to enforce these protections/policies?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor 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.
- We are pursuing formal assurances and documentation from LifeLabs that they have taken adequate security measures to prevent this from re-occurring.
- Next steps for this incident will be determined based on our agreement with LifeLabs.

18. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement and privacy commissioners, and hired world-leading cyber security firms to investigate and respond to this incident.

19. How can people have confidence that their health records are secure in B.C.?

- Most of British Columbia's lab tests happen in hospitals and that data is not affected by this breach.
- Government and health authority systems were not impacted. They have security measures in place to prevent infiltrations, and proactive monitoring tools to detect threats.
- Protection of government data and networks is a top priority, especially where it concerns British Columbians' personal information.
- If there are breaches – 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.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

20. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

21. Has government paid ransoms for return of data?

- No.

22. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

23. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C related to the notification process in data-breach situations.

25. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

26. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, LifeLabs determined that the most effective way to alert B.C. residents was to establish a centralized website to answer key questions and provide access to resources, including to free identity theft insurance and monitoring services.

27. The Information and Privacy Commissioner has called for changes to the *Personal Information Privacy Act*. Why hasn't the Province acted?

- It is important that the people of B.C. know that there are rules and guidelines that protect their personal information.
- The Personal Information Protection Act (PIPA) governs the way businesses, non-profits, political parties and other organizations use personal information.
- PIPA applies to over 300,000 private organizations so any changes must be carefully considered to ensure the intended result is achieved.

28. Does government intend on amending the Personal Information Protection Act?

- PIPA applies to over 300,000 private organizations, so any changes must be carefully considered to ensure the intended result is achieved.
- We have received recommendations from the Office of the Information and Privacy Commissioner, past Special Committees, advocacy groups and the public.
- This feedback will help inform any future legislative or policy changes to improve the way organizations protect personal information.

Questions & Answers
LifeLabs Data Security Issue
December 17, 2019

Key Messages

- This is very concerning. The protection of British Columbians' privacy is critical.
- B.C. is committed to strong privacy and security controls.
- Most of British Columbian's lab tests happen in hospitals and that data is not affected by this breach.
- While LifeLabs is a private company, the Province is closely monitoring and consulting with them as they address this incident.
- The Province understands LifeLabs has hired world-leading cyber security firms to investigate and respond – including implementing additional safeguards to further secure their networks going forward.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.
- The Province will continue to work with LifeLabs to help them ensure that their investigation and response are thorough and effective.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.

Background

- On December 17, 2019, it was announced that LifeLabs, the private company responsible for conducting approximately 34% of B.C. lab testing services, experienced a significant data breach.
- 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 also taken during the breach. LifeLabs 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 the public, while also taking steps to secure their information systems against future attack.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- We understand LifeLabs was able to secure the data taken during the breach by making a payment.
- Questions on this matter should be directed to LifeLabs.

3. When LifeLabs was first detected the breach, did they contact the police?

- LifeLabs has contacted the police and is working with them on their investigation.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What information did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians' client data was breached.
- They have indicated that impacted data includes 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 also taken during the breach. LifeLabs will notify those customers directly.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C, and elsewhere.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens' Services have required LifeLabs to provide senior officials daily updates on their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged world-leading cyber security firms to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. Do you feel LifeLab's response has been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with privacy commissioners in several provinces and with B.C.'s Ministries of Health and Citizens' Services to accomplish this notification as efficiently as possible.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed around the clock to fully ascertain the scope of the attack and to obtain expert recommendations on effectively closing it.
- This work is a critical part of the notification and remediation process.

If pressed:

- Announcing these types of incidents can attract immediate secondary cyber attacks.
- We understand LifeLabs did not provide public notification until the world-class cyber security firms they engaged were able to ensure that LifeLabs networks were effectively secured against further attacks.
- The goal was to prevent against any disruptions to service delivery that could negatively impact patient care.

8. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- Officials from Citizens' Services and Health are working to help LifeLabs ensure their investigation and response are thorough and effective.

9. Have any government systems been affected?

- B.C. government and Health Authority systems are not affected by this breach.
- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs is providing all customers access to free identity theft insurance of up to \$50,000 and monitoring services.
- We encourage anyone who has had testing done at LifeLabs to contact LifeLabs directly by visiting www.customernotice.lifelabs.com or by calling 1-888-918-0467.

11. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

12. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- LifeLabs has engaged world-class cyber security firms to ensure that their networks have been effectively secured against further attacks.
- We understand they did not provide public notification until they could implement further safeguards against secondary attacks.
- Their goal was to prevent against any disruptions to service delivery that could negatively impact patient care.

13. Does government support LifeLab's approach and timing?

- LifeLabs has been working with privacy commissioners, their legal counsel, external cyber-security experts, and cyber-security and privacy officials at the Ministry of Citizens' Services.
- LifeLabs is a private company operating in B.C., Ontario, Saskatchewan and New Brunswick and must meet multiple legislative notification and disclosure requirements, including the process of engaging law enforcement.

14. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- LifeLabs has paid to secure the breached data.
- At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.
- LifeLabs is providing all customers access to free identity theft insurance up to \$50,000 and monitoring services. LifeLabs have assured us that they are taking every precaution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

15. Does the Province believe LifeLab's mitigation responses for clients are enough?

- LifeLabs is a private company and we continue to monitor their response closely. We are pursuing formal assurances and documentation from LifeLabs that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

16. The Ministry of Health holds a contract with LifeLabs – what protections are in place when data is in the custody of a contractor or service provider?

- 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.

17. What does the Ministry do to enforce these protections/policies?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor 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.

18. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand LifeLabs has notified law enforcement and privacy commissioners, and hired world-leading cyber security firms to investigate and respond to this incident.
- Questions on this matter should be directed to LifeLabs.

19. How can people have confidence that their health records are secure in B.C.?

- Most of British Columbia's lab tests happen in hospitals and that data is not affected by this breach.
- Government and health authority systems were not impacted. They have security measures in place to prevent infiltrations, and proactive monitoring tools to detect threats.
- Protection of government data and networks is a top priority, especially where it concerns British Columbians' personal information.
- If there are breaches – 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.

- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

20. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

21. Has government paid ransoms for return of data?

- No.

22. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

23. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

25. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

26. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- In this situation, LifeLabs determined that the most effective way to alert B.C. residents was to establish a centralized website to answer key questions and provide access to resources, including to free identity theft insurance and monitoring services.

27. The Information and Privacy Commissioner has called for changes to the *Personal Information Privacy Act*. Why hasn't the Province acted?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

28. Does government intend on amending the Personal Information Protection Act?

- PIPA applies to over 300,000 private organizations so any changes must be carefully considered to ensure the intended result is achieved.
- We have received recommendations from the Office of the Information and Privacy Commissioner, past Special Committees, advocacy groups and the public.
- This feedback will help inform any future legislative or policy changes to improve the way organizations protect personal information.

**MINISTRY OF HEALTH
INFORMATION BRIEFING NOTE**

Cliff #

PREPARED FOR: Peter Pokorny, Associate Deputy Minister - **FOR INFORMATION**

TITLE: Life Labs Security Issue

PURPOSE: To provide an update on the Life Labs Security Issue and the approach for the Province and the Health Sector in minimizing cyber security risk.

BACKGROUND:

On October 28, 2019, Life Labs (LL) proactive surveillance identified unauthorized access s.15

s.15 As per standard operating procedure, LL quickly isolated the affected systems to eliminate and contain any potential impact of the unauthorized access. LL immediately engaged a top international independent cyber security firm, CrowdStrike, to help them with the technical aspects of the investigation, s.15

s.13; s.15

DISCUSSION:

LL is fully engaged with MOH, CITZ, and the OIPC on an investigation and planning on actions and steps to respond and GCPE is fully involved and is developing messaging for the incident, actions taken and notification plans.

s.13

BC Government approach and key messages to minimizing cyber security risk

- Protecting the privacy and security of British Columbians is a critical priority especially where it concerns British Columbians' personal information.
- Citizens must have the utmost confidence that their information is secure and protected whenever they access services or provide information to government and other agencies.
- BC Government has policy and standards related to privacy and security that core government must follow.
- s.13
- BC Government contracts follow procurement rules and include both a privacy protection and a security schedule that clearly set out the requirements that contractors must abide by.
- Those expectations are clearly communicated, and contractors who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.
- If the Province becomes aware that a contractor is non-compliant with any terms of their contract, the Province follows up with the contractor to conduct an investigation, depending on the circumstances.
- BC government has security measures in place to protect networks, systems, and data and there are proactive monitoring tools in place to detect threats.
- s.13; s.15
- Office of the Chief Information Officer (OCIO) Security in BC Government is constantly evaluating potential threats, with systems monitoring 24 hours per day, seven days a week.
- The OCIO and every ministry have dedicated staff to monitor and respond to security issues.
- Individual ministries have responsibility for day-to-day security in their respective areas; the OCIO sets the protocols and standards for IT security across government.
- The OCIO is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.

Ministry of Health (MoH) approach and key messages to minimizing cyber security risk

- Protecting the privacy and security of British Columbians is a critical priority especially where it concerns British Columbians' personal health information.

s.13

•

s.

•

s.13

•

● s.13; s.15

- The Ministry responsible for managing the security of patient information in its systems.
- Under the LSA, the minister has the power to appoint inspectors to conduct audits and inspections to determine compliance with the legislation.

● s.13; s.15

— s.13

●

- Patient safety is paramount for the Ministry.
- The Ministry is committed to ensuring system users are granted only the minimum access they require to perform their responsibilities, whether they are a staff person, a system support vendor, or a practitioner.

● s.13; s.15

- The Ministry establishes and enforces strong privacy and security standards for organizations connecting to our systems.
- The Ministry reports all potential privacy incidents immediately for assessment and containment.

s.13

- Over 60% of lab tests actually occur in hospitals. There is no evidence to suggest that lab results from hospitals have been compromised through this breach.

ADVICE:

MOH staff are moving forward to develop messaging for the incident, actions taken, and notification plans in coordination with LL, CITZ, OPIC and the Ministry of Health in Ontario.

Commented [DMH3]:

s.13

Formatted: Default, Indent: Left: 0 cm, Hanging: 0.63 cm, Space Before: 0 pt, Line spacing: single, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman

Program ADM/Division: Ian Rongve, ADM, Corrie Barclay, ADM, HSIMT Division
Telephone: 778-698-4753
Program Contact (for content): Alison Pearce
Date: November 20, 2019

Ministry Statement:

British Columbians need to be able to have confidence that their information is secure and protected. LifeLabs reported the data breach to the Office of the Information and Privacy Commissioner as soon as it was confirmed that British Columbians' information was affected. No patient records or medical test results are known to be involved in the incident.

LifeLabs has already implemented additional security controls to further protect their systems and engaged very reputable external resources to help them with the technical aspects of their investigation.

s.13

Background:

- LifeLabs is a private company and is leading the investigation and response. Any questions on the investigation should be directed to LifeLabs.
- No patient records or health test results are known to be involved in the incident.
- People who have been impacted have been contacted by Lifelabs.
- Lifelabs has made a call centre available to support clients and they will be offering credit protection at no cost for a year.
- Privacy and data security experts from the B.C. government are assisting LifeLabs in an advisory capacity.
- Government requires all contractors to adhere to stringent privacy and security requirements in their contracts.
- Government contracts follow procurement rules and include both a privacy protection and a security schedule that clearly set out the legal requirements that the contractor must abide by.
- Those expectations are clearly communicated, and contractors who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.
- If the Province receives evidence that a contractor is non-compliant with any terms of their contract, the contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

Background:

- LifeLabs says there is no evidence British Columbians' lab test results were impacted.
- The breached data in B.C. includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.
- LifeLabs is a private company responsible for conducting approximately 34% of B.C. lab testing services.

Background:

- LifeLabs says there is no evidence British Columbians' lab test results were impacted.
- The breached data in B.C. includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.
- LifeLabs is a private company responsible for conducting approximately 34% of B.C. lab testing services.

Background:

- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.

Prevost, Jean-Marc GCPE:EX

From: Prevost, Jean-Marc GCPE:EX
Sent: December 16, 2019 10:40 AM
To: Carroll, Scott CITZ:EX; Marriott, Sarah GCPE:EX; Lauvaas, Kirsten GCPE:EX
Cc: May, Stephen GCPE:EX; Burton, Meribeth GCPE:EX
Subject: latest LL products
Attachments: generic LL statement (jmp).docx; draft frontline KMs_LL_sm.docx; LL KM Q A Dec 16.docx

Importance: High

Media statement
Cutdown Q&A and KM (for sharing with Health Authorities)
Long form Q & A (updates from CITZ as of this morning)

J M P

Desk: 236-478-0302
Cell: 250-886-2154

Questions & Answers

Life Labs Data Security Issue

November 14, 2019

Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it comes to the personal information of citizens
- Citizens must have the utmost confidence that their information is secure and protected whenever they access services or provide information to government and other agencies.
- The Province is aware that LifeLabs encountered a data breach involving client information.
- LifeLabs confirmed that they were contacted by an unknown source who confirmed they are in possession of LifeLabs' client personal information.
- The Ministries of Health and Citizens' Services are working closely with LifeLabs in a consulting role as they determine the extent and scope of the breach. LifeLabs has also notified the Office of the Information and Privacy Commissioner of this incident.
- At this time there is no evidence to indicate that BC government systems are affected by this breach.
- I can assure you that 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.

Questions & Answers

Issue Specific

1. When did LifeLabs notify the Ministry of the incident?

- LifeLabs notified the Ministry on October ^{s.13}

2. Have any demands for payment been made or indications received as to what will be done with the data?

- Any comments regarding specific details such as this should be directed to LifeLabs as they are leading the investigation. As LifeLabs' infrastructure was impacted by this incident, and as they are a private company, any decisions regarding payment are theirs alone.
- If pressed: Releasing information regarding any negotiations could have potential negative effects on the impacted parties and on LifeLabs and as such we would prefer not to comment on this at this time.

3. When did the Ministry find out that B.C data was impacted?

- When the incident was first reported to the Ministry it was initially unknown if data about B.C residents was impacted.
- However, after further investigation it was confirmed by LifeLabs on November 7, 2019 that data about BC residents was impacted. ^{s.13}
s.13
- The Office of the Information and Privacy Commissioner were immediately informed of the incident on November 7, 2019 when BC residents were confirmed to be involved.

4. How many BC residents are impacted?

- LifeLabs is still investigating the full scope of those who may be impacted.

5. What did the Ministry of Health do following the report by LifeLabs?

- The Ministry has been in daily contact with LifeLabs since the incident was reported and LifeLabs has provided daily updates on the progress made with their investigation.
- Ministry resources such as investigative and technical support have been offered to LifeLabs.
- As LifeLabs is a private company they are leading the investigation and the Ministry is currently participating in an advisory capacity.

6. Have any government systems been impacted?

- At this time there are no indications or evidence to indicate that any government systems have been impacted.
- Government systems have strong security measures in place to prevent infiltrations and proactive monitoring tools are in place to detect threats.

7. What is the Database that was accessed? Where was the information accessed from?

- LifeLabs has confirmed that the information appears to have been accessed from one of their internal databases.

CONFIDENTIAL ADVICE TO MINISTER

- However, they are still in the process of investigating the exact origin of the data.
- LifeLabs have various databases that store personal information such as name, address, date of birth, personal health number (BC Services Card/Care Card number) and gender.

8. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- Government contracts follow procurement rules and include strict requirements for privacy and security.
- Contractors are expected to follow the terms of their contracts related to the protection of personal information.

9. What does the Ministry do to enforce these protections/policies?

- The Ministry requires contractors to adhere to privacy and security requirements in contract.
- Contracts are drafted that include both a privacy protection schedule and a security schedule that sets out the legal requirements that the contractor must abide by. Expectations that they must meet the terms and expectations set out in the contracts are clearly communicated both in the contract and verbally.
- Contractors who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully communicated.
- If any evidence is received that a contractor is non-compliant with any terms of their contract then the matter must be reported to the contract manager, and the contractor must conduct an investigation or cooperate with government's investigation, depending on the circumstances.

1. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats such as malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats with systems monitoring 24 hours per day, 7 days a week.

2. What exactly was the data that was taken (names, test results)?

CONFIDENTIAL ADVICE TO MINISTER

- The data about BC residents that has been impacted includes patient names, addresses, province of residence, postal code, practitioner names, PHN, gender and date of birth. No clinical lab results are known to be impacted for this data set.
- LifeLabs is working closely with the Ministries of Health and Citizens' Services to develop a plan to notify impacted BC residents of this incident and to offer protections to mitigate risks associated with the attack.

3. Are you confident that the threat actors don't have additional data? How can you know for sure that people's personal information is safe?

- LifeLabs is working to confirm whether or not additional data is impacted. Finding the answer to this question is one of the Ministry's top priorities.
- Once new information is received on this it will be communicated accordingly.

4. What steps are you taking to ensure any security gaps are addressed so this doesn't happen again?

- The Ministries of Health and Citizens Services' are receiving daily updates from LifeLabs to ensure government is fully informed as to the progress of LifeLabs' investigation. Any security or privacy issues are being communicated to the appropriate Ministry investigation units for review.
- The Ministry has confirmed that LifeLabs has security controls in place to protect their systems and the information stored within it.
- No organization globally is immune to attack and in this instance, attackers found and exploited a weakness.
- LifeLabs has since taken additional steps to protect their systems as a result and has implemented additional proactive monitoring solutions to detect threats and attacks.
- LifeLabs has confirmed to the Ministry that they have engaged very reputable external resources to help them with the technical aspects of the investigation. The Ministry will be reviewing the information received to ensure security gaps identified in the review are addressed.
- Government regularly upgrades security to protect government users from threats such as malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats with systems monitoring 24 hours per day, 7 days a week.

5. Why did LifeLabs pay/not pay the ransom?

- LifeLabs is a private company and paying the ransom is a decision for the business to make. Questions on this matter should be directed to LifeLabs.

6. Why did government allow/not allow them to pay?

- LifeLabs is a private company and paying the ransom is a decision for the business to make. Questions on this matter should be directed to LifeLabs.

7. What are the potential ramifications of this decision?

- Organizations known to pay ransoms may be further targeted.
- Organizations that do not pay the ransom may have clients' personal information exposed on the internet.

8. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been sufficient? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Ministry recognizes that notifying impacted individuals quickly is crucial when they have been subject to a privacy breach. LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment this was reported to the Ministry all efforts and resources were deployed to fully ascertain the scope of the breach and the data source as this information is critical to the notification and remediation process.

9. When LifeLabs was first contacted by the threat actors, did they contact the police?

LifeLabs is a private company and the decision to engage law enforcement is solely theirs. Questions on this matter should be directed to LifeLabs.

10. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs is contracted through the Ministry of Health, so they are working in partnership to ensure the situation is resolved.
- The Provincial Health Services Authority manages the LifeLabs contract and are also involved.
- Citizens' Services is being consulted to ensure that the investigation follows proper protocols, including incident handling and response, as per government's information incident management policies.

11. Does government have a duty to report breaches to the authorities? Why didn't you?

- Government works with a variety of stakeholders including law enforcement. However, as this incident impacted LifeLabs' infrastructure, and as LifeLabs is a private company, decisions about contacting law enforcement rest solely with LifeLabs. Questions on this matter should be directed to LifeLabs.

Next Steps

12. What is LifeLabs doing to support affected clients?

- LifeLabs will be notifying those impacted by the breach.
- LifeLabs will be setting up a call centre to address any inquiries.
- Clients with questions and concerns about the breach can contact the call centre, which will open to support clients soon
- LifeLabs have also confirmed that the impacted individuals will be offered credit protection at no cost via TransUnion for a 12 month period.

13. When will the call centre be set up?

- Efforts are underway to set up the call centre and this is a priority. We do not have an estimated time of completion presently.

14. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents such as this before notification can be completed. The impacted parties need to be identified, contact information needs to be assessed and verified, communication materials need to be drafted, supports need to be identified and procured and resources need to be obtained to carry this out.
- All of this work was initiated immediately by LifeLabs when the incident was discovered and employees worked around the clock to ensure that as little time as possible elapsed between when it was discovered and when notification was conducted.

15. Does government support LifeLab's approach and timing?

- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process.

- LifeLabs has engaged with government since they became aware and shared information on their approach.
- LifeLabs has taken strong and decisive action in dealing with a difficult situation. As with any incident of this nature, government and LifeLabs will debrief following the conclusion of the incident to identify lessons learned.
- Government has appreciated the open and transparent cooperation that LifeLabs has provided in addressing this issue.

16. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre. Questions related to this matter should be directed to LifeLabs

17. What will LifeLabs – or government – do to help if these clients experience identity theft or fraud as a result of this breach?

- LifeLabs is ensuring credit monitoring for those affected by the breach. Questions related to this matter should be directed to LifeLabs

18. What recourse do clients have if they aren't satisfied with the support they receive through the call centre?

- Citizens may contact the Office of the Information and Privacy Commissioner if they are concerned with the way this incident is being handled.

19. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'. Questions related to this matter should be directed to LifeLabs

Government – Data Security and Privacy Breaches

20. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.
- As each scenario is different government would consider their options on a case by case basis.

21. Has government paid ransoms for return of data?

- No.

22. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators, and will invoke the incident response team in reaction to any incidents that occur and they will lead through the containment of any issues that occur.

23. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats such as malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats with systems monitoring 24 hours per day, 7 days a week.
- Government has an established, effective information incident management policy and a team of trained information incident investigators, and will invoke the incident response team in reaction to any incidents that occur and they will lead through the containment of any issues that occur.

Questions & Answers

Life Labs Data Security Issue

November 16, 2019

Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it comes to the personal information of citizens.
- Citizens 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 also notified the Office of the Information and Privacy Commissioner of this incident.
- At this time, there is no evidence to indicate that B.C. government systems are affected by this breach.
- 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.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October ^{s.13} that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and paying the ransom is their decision to make.
- Any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information regarding any negotiations could have potential negative effects on the impacted parties and on LifeLabs.
- As such, we will not comment further on this.

3. What are the potential ramifications of their decision?

- Organizations that have paid ransoms may be further targeted.
- Organizations that do not pay the ransom may have clients' personal information exposed on the internet or in some other public manner.

4. When LifeLabs was first contacted by the threat actors, did they contact the police?

- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

5. What database did they access? Where was the information accessed from?

- LifeLabs has confirmed that the information appears to have been accessed from one of their internal databases.
- However, they are still in the process of investigating the exact origin of the data.
- LifeLabs has various databases that store personal information, such as names, addresses, dates of birth, personal health numbers (BC Services Card/Care Card numbers) and gender.

6. What exactly was the data that was taken (names, test results)?

- No clinical lab results are known to be included in this data set.
- 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 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.

7. How many B.C. residents are affected?

- LifeLabs is still investigating the full scope of those who may be affected.
- Once the scope is determined, LifeLabs will begin the notification process.

8. Are you confident that the threat actors don't have additional data? How can you know for sure that people's personal information is safe?

- LifeLabs is working to confirm the scope of the incident.

9. What steps are you taking to ensure any security gaps are addressed so this doesn't happen again?

- The Ministries of Health and Citizens Services' are receiving daily updates from LifeLabs to ensure government is fully informed as to the progress of LifeLabs' investigation.
- Any security or privacy issues are being communicated to the appropriate Ministry's investigation unit for review.
- LifeLabs states they now have security controls in place to protect their systems and the information stored within them.
- No organization globally is immune to attack.
- In this instance, attackers found and exploited a weakness.
- LifeLabs has since taken additional steps to protect their systems.
- The company has implemented additional proactive monitoring solutions to detect further threats and attacks.
- LifeLabs has engaged very reputable external resources to help them with the technical aspects of their investigation.

Issue Specific – B.C. Government

10. When did the B.C. Government find out that B.C. data was impacted?

- When the incident was first reported to the Province, it was initially unknown if data about B.C residents was affected.
- However, after further investigation, LifeLabs confirmed on November 7th that data about B.C. residents was included in the breach.
- 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.

11. What did the B.C. government do following the report by LifeLabs?

- As LifeLabs is a private company, they are leading the investigation.
- They have already implemented additional security controls to further protect their systems.
- They have also engaged reputable external resources, including an internationally recognized cyber-security company, to help them with the technical aspects of their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity.
- This includes providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken to address what has occurred.
- The ministries have been in daily contact with LifeLabs since the incident was reported, and LifeLabs has provided daily updates on the progress made with their investigation.

12. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been sufficient? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed to fully ascertain the scope of the breach, as well as the data source, as this information is a critical part of the notification and remediation process.

13. Have any government systems been affected?

- Government systems have strong security measures in place to prevent infiltrations, and proactive monitoring tools are in place to detect threats.
- At this time, there are no indications that B.C. government systems are affected by this breach.

14. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs is contracted through the Ministry of Health, so they are working in partnership to ensure the situation is resolved.
- The Provincial Health Services Authority manages the LifeLabs contract and is also involved.
- Citizens' Services is being consulted to ensure that the investigation follows proper protocols, including incident handling and response, as per government's information incident management policies.

Next Steps

15. What is LifeLabs doing to support affected clients?

- Once LifeLabs determines the full scope of affected data, they will begin notifying those who have been affected by the breach.
- Lifelabs is in the process of setting up a call centre to address any inquiries.
- Clients with questions and concerns about the breach can contact the call centre, which will open to support clients soon.
- LifeLabs has also confirmed that the affected individuals will be offered credit protection at no cost via TransUnion for a 12-month period.

16. When will the call centre be set up?

- LifeLabs is working to set up the call centre and this is a priority.
- We do not have an estimated time of completion presently.
- LifeLabs can provide updates as to the status of the call centre.

17. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

18. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- The affected parties need to be identified, contact information needs to be assessed and verified, communication materials need to be drafted, supports need to be identified and procured, and resources need to be obtained to carry out notifications and remediation.
- LifeLabs initiated of this work immediately when the incident was discovered.
- Employees have worked around the clock to ensure that as little time as possible elapsed between when the breach was discovered and when notification began.

19. Does government support LifeLab's approach and timing?

- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process.
- LifeLabs has worked with government since they became aware and shared information on their approach.
- They have taken strong and decisive action in dealing with a difficult situation.
- As with any incident of this nature, government and LifeLabs will debrief following the conclusion of the incident to identify lessons learned.
- Government has appreciated the open and transparent cooperation that LifeLabs has provided in addressing this issue.

20. What will LifeLabs – or government – do to help if these clients experience identity theft or fraud as a result of this breach?

- LifeLabs is ensuring credit monitoring for those affected by the breach.
- Questions related to this matter should be directed to LifeLabs.

If pressed:

- Credit-monitoring services are provided by third-party companies, to alert an individual when changes affecting their credit scores occur, so that they may respond quickly to an identity-theft risk.
- They are a common remediation response to breaches that have the potential for identity theft or fraud.

21. What recourse do clients have if they aren't satisfied with the support they receive through the call centre?

- Citizens may contact the Office of the Information and Privacy Commissioner if they are concerned with the way this incident is being handled.

22. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- Questions related to this matter should be directed to them.

Contract Management – LifeLabs & Ministry of Health

23. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- Government contracts follow procurement rules and include strict requirements for privacy and security.
- Contractors are expected to follow the terms of their contracts related to the protection of personal information.

24. What does the Ministry do to enforce these protections/policies?

- The Ministry requires contractors to adhere to privacy and security requirements in contract.
- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

25. Does government have a duty to report breaches to the authorities? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- Questions on this matter should be directed to LifeLabs.

26. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.

Government – Data Security and Privacy Breaches (General)

27. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

28. Has government paid ransoms for return of data?

- No.

29. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

30. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

31. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

32. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.
- However, best practice is to address all issues in as little time as possible to mitigate harm.

33. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- While B.C. and Ontario assess the same factors when considering whether to notify individuals impacted by privacy breaches, B.C. is the only province with a centralized team to conduct these assessments and support the delivery of notifications.

Questions & Answers
Life Labs Data Security Issue
November 16, 2019

Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it comes to the personal information of citizens.
- Citizens 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 also notified the Office of the Information and Privacy Commissioner of this incident.
- At this time, there is no evidence to indicate that B.C. government systems are affected by this breach.
- 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.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October^{s.13} that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and paying the ransom is their decision to make.
- Any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- ~~LifeLabs are leading the investigation and you would need to speak to them about specific matters. Releasing information regarding any negotiations could have potential negative effects on the impacted parties and on LifeLabs.~~
- ~~As such, we will not comment further on this.~~
- ~~_____~~

3. ~~What are the potential ramifications of their decision?~~

- ~~Organizations that have paid ransoms may be further targeted.~~
- ~~Organizations that do not pay the ransom may have clients' personal information exposed on the internet or in some other public manner.~~

4.3. When LifeLabs was first contacted by the threat actors, did they contact the police?

- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

5.4. What database did they access? Where was the information accessed from?

- LifeLabs has confirmed that the information appears to have been accessed from one of their internal databases.
- However, they are still in the process of investigating the exact origin of the data.
- LifeLabs has various databases that store personal information, such as names, addresses, dates of birth, personal health numbers (BC Services Card/Care Card numbers) and gender.

Formatted: List Paragraph,bullet 1,BN 1,Paperitemletter,Dot pt,Liste 1,table bullets,TOC style,lp1,Bullet List - spacing,List Paragraph1,Recommendation,List Paragraph11,L,List Paragraph2,CV text,Table text,F5 List Paragraph,List Paragraph111,列出段落, Space After: 6 pt, Bulleted + Level: 1 + Aligned at: 0.63 cm + Tab after: 1.27 cm + Indent at: 1.27 cm

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

6.5. What exactly was the data that was taken (names, test results)?

- No clinical lab results are known to be included in this data set.
- 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 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.

7.6. How many B.C. residents are affected?

- LifeLabs is still investigating the full scope of those who may be affected.
- Once the scope is determined, LifeLabs will begin the notification process.

8.7. Are you confident that the threat actors don't have additional data? How can you know for sure that people's personal information is safe?

- LifeLabs is working to confirm the scope of the incident.

9.8. What steps are you taking to ensure any security gaps are addressed so this doesn't happen again?

- The Ministries of Health and Citizens Services' are receiving daily updates from LifeLabs to ensure government is fully informed as to the progress of LifeLabs' investigation.
- Any security or privacy issues are being communicated to the appropriate Ministry's investigation unit for review.
- LifeLabs states they now have security controls in place to protect their systems and the information stored within them.
- No organization globally is immune to attack.
- In this instance, attackers found and exploited a weakness.
- LifeLabs has since taken additional steps to protect their systems.
- The company has implemented additional proactive monitoring solutions to detect further threats and attacks.
- LifeLabs has engaged very reputable external resources to help them with the technical aspects of their investigation.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

Issue Specific – B.C. Government

10.9. When did the B.C. Government find out that B.C. data was impacted?

- When the incident was first reported to the Province, it was initially unknown if data about B.C residents was affected.
- However, after further investigation, LifeLabs confirmed on November 7th that data about B.C. residents was included in the breach.
- 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.

11.10. What did the B.C. government do following the report by LifeLabs?

- As LifeLabs is a private company, they are leading the investigation.
- They have already implemented additional security controls to further protect their systems.
- They have also engaged reputable external resources, including an internationally recognized cyber-security company, to help them with the technical aspects of their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity.
- This includes providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken to address what has occurred.
- The ministries have been in daily contact with LifeLabs since the incident was reported, and LifeLabs has provided daily updates on the progress made with their investigation.

12.11. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been sufficient? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed to fully ascertain the scope of the breach, as well as the data source, as this information is a critical part of the notification and remediation process.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

13.12. Have any government systems been affected?

- Government systems have strong security measures in place to prevent infiltrations, and proactive monitoring tools are in place to detect threats.
- At this time, there are no indications that B.C. government systems are affected by this breach.

14.13. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs is contracted through the Ministry of Health, so they are working in partnership to ensure the situation is resolved.
- The Provincial Health Services Authority manages the LifeLabs contract and is also involved.
- Citizens' Services is being consulted to ensure that the investigation follows proper protocols, including incident handling and response, as per government's information incident management policies.

Next Steps

15.14. What is LifeLabs doing to support affected clients?

- Once LifeLabs determines the full scope of affected data, they will begin notifying those who have been affected by the breach.
- LifeLabs is in the process of setting up a call centre to address any inquiries.
- Clients with questions and concerns about the breach can contact the call centre, which will open to support clients soon.
- LifeLabs has also confirmed that the affected individuals will be offered credit protection at no cost via TransUnion for a 12-month period.

16.15. When will the call centre be set up?

- LifeLabs is working to set up the call centre and this is a priority.
- We do not have an estimated time of completion presently.
- LifeLabs can provide updates as to the status of the call centre.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

17.16. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

18.17. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- The affected parties need to be identified, contact information needs to be assessed and verified, communication materials need to be drafted, supports need to be identified and procured, and resources need to be obtained to carry out notifications and remediation.
- LifeLabs initiated of this work immediately when the incident was discovered.
- Employees have worked around the clock to ensure that as little time as possible elapsed between when the breach was discovered and when notification began.

19.18. Does government support LifeLab's approach and timing?

- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process.
- LifeLabs has worked with government since they became aware and shared information on their approach.
- They have taken strong and decisive action in dealing with a difficult situation.
- As with any incident of this nature, government and LifeLabs will debrief following the conclusion of the incident to identify lessons learned.
- Government has appreciated the open and transparent cooperation that LifeLabs has provided in addressing this issue.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

20.19. What will LifeLabs – or government – do to help if these clients experience identity theft or fraud as a result of this breach?

- LifeLabs is ensuring credit monitoring for those affected by the breach.
- Questions related to this matter should be directed to LifeLabs.

If pressed:

- Credit-monitoring services are provided by third-party companies, to alert an individual when changes affecting their credit scores occur, so that they may respond quickly to an identity-theft risk.
- They are a common remediation response to breaches that have the potential for identity theft or fraud.

21.20. What recourse do clients have if they aren't satisfied with the support they receive through the call centre?

- Citizens may contact the Office of the Information and Privacy Commissioner if they are concerned with the way this incident is being handled.

22.21. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- Questions related to this matter should be directed to them.

Contract Management – LifeLabs & Ministry of Health

23.22. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- Government contracts follow procurement rules and include strict requirements for privacy and security.
- Contractors are expected to follow the terms of their contracts related to the protection of personal information.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

24,23. What does the Ministry do to enforce these protections/policies?

- The Ministry requires contractors to adhere to privacy and security requirements in contract.
- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

25,24. Does government have a duty to report breaches to the authorities? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- Questions on this matter should be directed to LifeLabs.

26,25. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

Government – Data Security and Privacy Breaches (General)

27. Does government pay ransoms?

- ~~To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.~~

28. Has government paid ransoms for return of data?

- ~~No.~~

~~29,26.~~ What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

~~30,27.~~ What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

31,28. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

32,29. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.
- However, best practice is to address all issues in as little time as possible to mitigate harm.

33,30. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- While B.C. and Ontario assess the same factors when considering whether to notify individuals impacted by privacy breaches, B.C. is the only province with a centralized team to conduct these assessments and support the delivery of notifications.

Questions & Answers
Life Labs Data Security Issue
November 16, 2019

Key Messages

- ~~Protecting the privacy and security of British Columbians' privacy is a critical priority especially where it comes to the personal information of citizens.~~
- ~~_____~~
- Citizens ~~must have the utmost confidence that~~ deserve to know their personal information is secure and protected.
- The Ministries of Health and Citizens' Services are ~~working closely with~~ monitoring and consulting with LifeLabs in a consulting role as LifeLabs as it responds to the is incident.
- LifeLabs has also notified the Office of the Information and Privacy Commissioner of this incident.
- At this time, there is no evidence to indicate that B.C. government systems are affected by this breach.
- ~~s.13~~
- ~~Any government privacy breaches — small or large — is investigated thoroughly, leveraging using 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 cyber-security incident with their booking system. At that time they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7th – the data includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth. The number of affected residents 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.
- We understand LifeLabs have also contacted law enforcement about this incident.
- 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.
- 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 still investigating the full scope of those who may be affected.
- Once the scope is determined, LifeLabs will begin the notification process.

Formatted: Font: (Default) Calibri, 14 pt, English (Canada), Not Expanded by / Condensed by

Formatted: Space After: 6 pt, Line spacing: single, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

Formatted: Font: (Default) Calibri, 14 pt, English (Canada), Not Expanded by / Condensed by

Formatted: Font: (Default) Calibri, 14 pt, English (Canada), Not Expanded by / Condensed by

Formatted: Font: (Default) Calibri, 14 pt, English (Canada), Not Expanded by / Condensed by

Formatted: Font: (Default) Calibri, 14 pt, English (Canada), Not Expanded by / Condensed by

Formatted: Font: (Default) Calibri, 14 pt, English (Canada), Not Expanded by / Condensed by

Formatted: Space After: 6 pt, Line spacing: single, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

Formatted: Font: (Default) Calibri, 14 pt, English (Canada), Not Expanded by / Condensed by

s.13

Commented [RIH2R1]:

Formatted: Font: (Default) Calibri, 14 pt, Not Bold, Font color: Auto

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28^{s.13} that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and paying the ransom is their decision to make.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- Any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- ~~Releasing information regarding during an ongoing investigation y negotiations could have potential negative effects on the impacted parties and we will on LifeLabs.~~
- ~~As such, we will not comment further on this wait until the investigation has progressed further before providing any additional information.~~

~~3. What are the potential ramifications of their decision?~~

- ~~Organizations that have paid ransoms may be further targeted.~~
- ~~Organizations that do not pay the ransom may have clients' personal information exposed on the internet or in some other public manner.~~

~~4.3. When LifeLabs was first contacted by the threat actors, did they contact the police?~~

- We understand LifeLabs have contacted the police.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

~~5.4. What database did they access? Where was the information accessed from?~~

- LifeLabs has confirmed that the information appears to have been accessed from one of their internal databases.
- However, they are still in the process of investigating the exact origin of the data.
- LifeLabs has various databases that store personal information, such as names, addresses, dates of birth, personal health numbers (BC Services Card/Care Card numbers) and gender.

~~6.5. What exactly was the data that was taken (names, test results)?~~

- No clinical lab results are known to be included in this data set.
- 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 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.

s.13

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

7.6. How many B.C. residents are affected?

- LifeLabs is still investigating the full scope of those who may be affected.
- Once the scope is determined, LifeLabs will begin the notification process.

8.7. Are you confident that the threat actors don't have additional data? How can you know for sure that people's personal information is safe?

- LifeLabs is working to confirm the scope of the incident.

9.8. What steps are you taking to ensure any security gaps are addressed so this doesn't happen again?

- The Ministries of Health and Citizens Services' are receiving daily updates from LifeLabs to ensure government is fully informed as to the progress of LifeLabs' investigation.
- Any security or privacy issues are being communicated to the appropriate Ministry's investigation unit for review.
- LifeLabs states they now have security controls in place to protect their systems and the information stored within them.
- No organization globally is immune to attack.
- In this instance, attackers found and exploited a weakness.
- LifeLabs has since taken additional steps to protect their systems.
- The company has implemented additional proactive monitoring solutions to detect further threats and attacks.
- LifeLabs has engaged very reputable external resources to help them with the technical aspects of their investigation.

Issue Specific – B.C. Government

10.9. When did the B.C. Government find out that B.C. data was impacted?

- When the incident was first reported to the Province, it was initially unknown if data about B.C. residents was affected.
- However, after further investigation, LifeLabs confirmed on November 7th that data about B.C. residents was included in the breach.
- 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.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

11.10. What did the B.C. government do following the report by LifeLabs?

- As LifeLabs is a private company, they are leading the investigation.
- They have already implemented additional security controls to further protect their systems.
- They have also engaged reputable external resources, including an internationally recognized cyber-security company, to help them with the technical aspects of their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity.
- This includes, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken to address what has occurred.
- The ministries have been in daily contact with LifeLabs since the incident was reported, and LifeLabs has provided daily updates on the progress made with their investigation.

12.11. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been sufficient enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed to fully ascertain the scope of the breach, as well as the data source, as this information is a critical part of the notification and remediation process.
- LifeLabs is still investigating the full scope of those who may be affected.
- Once the scope is determined, LifeLabs will begin the notification process.
-

s.13

13.1. Have any government systems been affected?

- Government systems have strong security measures in place to prevent infiltrations, and proactive monitoring tools are in place to detect threats.
- At this time, there are no indications that B.C. government systems are affected by this breach.

Formatted: Not Highlight

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

14.12. Government – through the Ministry of Health and the Ministry of Citizens’ Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab’s breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has is contracted through with the Ministry of Health, so they are working in partnership to ensure the situation is resolved.
- The Provincial Health Services Authority manages the LifeLabs contract and is also involved.
- Citizens’ Services is being consulted to ensure that the investigation follows proper protocols, including incident handling and response, as per government’s information incident management policies.

13. Have any government systems been affected?

- Government systems have strong security measures in place to prevent infiltrations, and proactive monitoring tools are in place to detect threats.
- At this time, there are no indications that B.C. government systems are affected by this breach.

Next Steps

15.14. What is LifeLabs doing to support affected clients?

- Once LifeLabs determines the full scope of affected data, they will begin notifying those who have been affected by the breach.
- Lifelabs is in the process of setting up a call centre to address any inquiries.
- Clients with questions and concerns about the breach can contact the call centre, which will open to support clients soon.
- LifeLabs has also confirmed that the affected individuals will be offered credit protection at no cost via TransUnion for a 12-month period.

16.15. When will the call centre be set up?

- LifeLabs is working to set up the call centre and this is a priority.
- We do not have an estimated time of completion presently.
- LifeLabs can provide updates as to the status of the call centre.

Formatted: Font: 12 pt, Condensed by 0.15 pt

Formatted: Normal, No bullets or numbering

s.13

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

17,16. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

18,17. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- The affected parties need to be identified, contact information needs to be assessed and verified, communication materials need to be drafted, supports need to be identified and procured, and resources need to be obtained to carry out notifications and remediation.
- LifeLabs initiated this work immediately when the incident was discovered.
- Employees have worked around the clock to ensure that as little time as possible elapsed between when the breach was discovered and when notification began.

19,18. Does government support LifeLab's approach and timing?

- ~~LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process.~~
- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizen Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.
- ~~LifeLabs has worked with government since they became aware and shared information on their approach.~~
- ~~They have taken strong and decisive action in dealing with a difficult situation.~~
- ~~As with any incident of this nature, government and LifeLabs will debrief following the conclusion of the incident to identify lessons learned.~~
- ~~Government has appreciated the open and transparent cooperation that LifeLabs has provided in addressing this issue.~~

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

20.19. What will LifeLabs – or government – do to help if these clients experience identity theft or fraud as a result of this breach?

- LifeLabs is ensuring credit monitoring for those affected by the breach.
- Questions related to this matter should be directed to LifeLabs.

If pressed:

- Credit-monitoring services are provided by third-party companies, to alert an individual when changes affecting their credit scores occur, so that they may respond quickly to an identity-theft risk.
- They are a common remediation response to breaches that have the potential for identity theft or fraud.

21.20. What recourse do clients have if they aren't satisfied with the support they receive through the call centre?

- Citizens may contact the Office of the Information and Privacy Commissioner if they are concerned with the way this incident is being handled.

22.21. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- Questions related to this matter should be directed to them.

Contract Management – LifeLabs & Ministry of Health

23.22. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- Government contracts follow procurement rules and include strict requirements for privacy and security.
- Contractors are expected to follow the terms of their contracts related to the protection of personal information.

s.13

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

24.23. What does the Ministry do to enforce these protections/policies?

- The Ministry requires contractors to adhere to privacy and security requirements in contract.
- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

25.24. Does government have a duty to report breaches to the authorities? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- Questions on this matter should be directed to LifeLabs.

26.25. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

Government – Data Security and Privacy Breaches (General)

27.26. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

28.27. Has government paid ransoms for return of data?

- No.

29.28. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

30.29. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

31.30. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

32.31. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.
- However, best practice is to address all issues in as little time as possible to mitigate harm.

33.32. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- While B.C. and Ontario assess the same factors when considering whether to notify individuals impacted by privacy breaches, B.C. is the only province with a centralized team to conduct these assessments and support the delivery of notifications.

Questions & Answers
Life Labs Data Security Issue
November 16, 2019

Key Messages

- Protecting British Columbians' privacy is critical.
- Citizens deserve to know their personal information is secure and protected.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement and the Office of the Information and Privacy Commissioner of this incident. They also hired a world-leading cyber security firm investigate and respond to this incident.
- More than 60% of British Columbian's lab tests happen in hospitals. There is no evidence to suggest that lab results from hospitals have been compromised through this breach.
- There is also no evidence to indicate that B.C. government systems are affected by this breach.
- Highly trained information incident investigators address any government privacy breaches thoroughly using an established and effective incident management process to quickly address the breach and mitigate impacts.

Discussion

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7th – the data includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth. The number of affected residents 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.
- We understand LifeLabs have also contacted law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, consulting with the Ministries of Health and the Ministry of Citizen Services.
- LifeLabs is still investigating the full scope of ^{s.13} the breach to determine what data has been impacted. On Nov. 19 they indicated the breach ^{s.13} could include lab results, ^{s.13}
^{s.13}
- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C. (how many British Columbians would this represent?). They are working closely with the Ministries of Health and Citizens' Services to develop a plan to notify affected B.C. residents and to offer protections to mitigate risks associated with the breach.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28st that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

s.13

3. When LifeLabs was first detected the breach, did they contact the police?

- We understand LifeLabs have contacted the police.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What database did they access? Where was the information accessed from?

- LifeLabs initially confirmed that the information appeared to have been accessed from one of their internal databases, s.13

s.13

5. What exactly was the data that was taken (names, test results)?

- s.13 lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- 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.

6. How many B.C. residents are affected?

- s.13

- How many British Columbians is this?

s.13

7. What did the B.C. government do following the report by LifeLabs?

- LifeLabs is providing daily updates on their investigation to the Ministries of Health and Citizens Services.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- LifeLabs has engaged a world-leading cyber security firm to help them with the technical aspects of their investigation.
- The company has implemented additional proactive monitoring solutions to detect further threats and attacks.

s. 13

Issue Specific – B.C. Government

8. When did the B.C. Government find out that B.C. data was impacted?

- When the incident was first reported to the Province on October 28th, it was initially unknown if data about B.C residents was affected.
- However, after further investigation, LifeLabs confirmed on November 7th that data about B.C. residents data was included in the breach.
- 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.

s. 13

Formatted: Superscript

s. 13

- LifeLabs has engaged a world-leading cyber security firm to help them with the technical aspects of their investigation.
- The company has implemented additional proactive monitoring solutions to detect further threats and attacks.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs.
- The ministries have been in daily contact with LifeLabs since the incident was reported, and LifeLabs has provided daily updates on the progress made with their investigation.

s. 13

9. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed to fully ascertain the scope of the breach, as well as the data source, as this information is a critical part of the notification and remediation process.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

10. Government – through the Ministry of Health and the Ministry of Citizens’ Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab’s breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has the personal information of many British Columbians. Officials from Citizens’ Services and Health are working to ensure LifeLabs’ investigation and response are thorough and effective.

11. Have any government systems been affected?

- Government systems have strong security measures in place to prevent infiltrations, and proactive monitoring tools are in place to detect threats.
- At this time, there are no indications that B.C. government systems are affected by this breach.

Next Steps

12. What is LifeLabs doing to support affected clients?

- LifeLabs is preparing their notification process – ^{s.13}
s.13
- Their notification process will include a call centre to address any inquiries.
- Clients with questions and concerns about the breach can contact the call centre, which will open to support clients soon.
- LifeLabs has also confirmed that the affected individuals will be offered some form of credit protection or monitoring. ^{s.13}

13. When will the call centre be set up?

- LifeLabs is working to set up the call centre and this is a priority.
- We do not have an estimated time of completion presently.
- LifeLabs can provide updates as to the status of the call centre.

14. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

15. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- The affected parties need to be identified, ~~contact information needs to be assessed and verified,~~ communication materials need to be drafted, supports need to be identified and procured, and resources need to be obtained to carry out notifications and remediation.
- LifeLabs initiated all of this work immediately when the incident was discovered.
- Employees have worked around the clock to ensure that as little time as possible elapsed between when the breach was discovered and when notification began.

s.13

16. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizen Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

17. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- LifeLabs is ensuring credit monitoring is provided for those affected by the breach.
- ~~Questions related to this matter should be directed to LifeLabs.~~

s.13

s.13

18. What recourse do clients have if they aren't satisfied with the support they receive through the call centre?

- Citizens may contact the Office of the Information and Privacy Commissioner if they ~~are concerned with the way this incident is being handled.~~

s.13

Formatted: Space After: 0 pt

Formatted: Font: 12 pt, Bold

Formatted: Indent: Left: 0.63 cm

19. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- Questions related to this matter should be directed to ~~them~~ LifeLabs.

Contract Management – LifeLabs & Ministry of Health

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

20. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of diagnostic testing services for British Columbians outside a hospital setting (about 40 per cent of all tests in the province).
- For some time the province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- The moved to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- BC Government contracts follow procurement rules and include both a privacy protection and a security schedule that clearly set out the requirements that contractors must abide by.
- Those expectations are clearly communicated, and contractors who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.
- If the Province becomes aware that a contractor is non-compliant with any terms of their contract, the Province follows up with the contractor to conduct an investigation, depending on the circumstances.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

21. What does the Ministry do to enforce these protections/policies?

- The Ministry requires contractors to adhere to privacy and security requirements in contract.
- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

22. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand they have contacted law enforcement.
- Questions on this matter should be directed to LifeLabs.

23. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.

Government – Data Security and Privacy Breaches (General)

24. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

25. Has government paid ransoms for return of data?

- No.

26. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

27. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

28. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

29. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

30. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- While B.C. and Ontario assess the same factors when considering whether to notify individuals impacted by privacy breaches, B.C. is the only province with a centralized team to conduct these assessments and support the delivery of notifications.

s.13

Questions & Answers
Life Labs Data Security Issue
November 16, 2019

Key Messages

- Protecting British Columbians' privacy is critical.
- Citizens deserve to know their personal information is secure and protected.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement and the Office of the Information and Privacy Commissioner of this incident. They also hired a world-leading cyber security firm investigate and respond to this incident.
- More than 60% of British Columbian's lab tests happen in hospitals. There is no evidence to suggest that lab results from hospitals have been compromised through this breach.
- There is also no evidence to indicate that B.C. government systems are affected by this breach.
- Highly trained information incident investigators address any government privacy breaches thoroughly using an established and effective incident management process to quickly address the breach and mitigate impacts.

Discussion

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7th – the data includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth. The number of affected residents 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.
- We understand LifeLabs have also contacted law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, consulting with the Ministries of Health and the Ministry of Citizen Services.
- LifeLabs is still investigating the full scope of s.13 breach. On Nov. 19 they indicated the breach s.13 could include lab results, s.13 s.13
- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C. (how many British Columbians would this represent?). They are working closely with the Ministries of Health and Citizens' Services to develop a plan to notify affected B.C. residents and to offer protections to mitigate risks associated with the breach.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28th that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

3. When LifeLabs was first detected the breach, did they contact the police?

- We understand LifeLabs have contacted the police.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What database did they access? Where was the information accessed from?

- LifeLabs initially confirmed that the information appeared to have been accessed from one of their internal databases, on Nov 19 they indicated ^{s.13}

5. What exactly was the data that was taken (names, test results)?

- ^{s.13} lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- 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.

6. How many B.C. residents are affected?

^{s.13}

7. What did the B.C. government do following the report by LifeLabs?

- LifeLabs is providing daily updates on their investigation to the Ministries of Health and Citizens Services.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- LifeLabs has engaged a world-leading cyber security firm to help them with the technical aspects of their investigation.
- The company has implemented additional proactive monitoring solutions to detect further threats and attacks.

Issue Specific – B.C. Government

8. When did the B.C. Government find out that B.C. data was impacted?

- When the incident was first reported to the Province, it was initially unknown if data about B.C residents was affected.
- However, after further investigation, LifeLabs confirmed on November 7th that data about B.C. residents was included in the breach.
- 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.
- s.13

- LifeLabs has engaged a world-leading cyber security firm to help them with the technical aspects of their investigation.
- The company has implemented additional proactive monitoring solutions to detect further threats and attacks.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs.
- The ministries have been in daily contact with LifeLabs since the incident was reported, and LifeLabs has provided daily updates on the progress made with their investigation.

9. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed to fully ascertain the scope of the breach, as well as the data source, as this information is a critical part of the notification and remediation process.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

10. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has the personal information of many British Columbians. Officials from Citizens' Services and Health are working to ensure LifeLabs' investigation and response are thorough and effective.

11. Have any government systems been affected?

- Government systems have strong security measures in place to prevent infiltrations, and proactive monitoring tools are in place to detect threats.
- At this time, there are no indications that B.C. government systems are affected by this breach.

Next Steps

12. What is LifeLabs doing to support affected clients?

- LifeLabs is preparing their notification process –^{s.13}
s.13
- Their notification process will include a call centre to address any inquiries.
- Clients with questions and concerns about the breach can contact the call centre, which will open to support clients soon.
- LifeLabs has also confirmed that the affected individuals will be offered some form of credit protection or monitoring.

13. When will the call centre be set up?

- LifeLabs is working to set up the call centre and this is a priority.
- We do not have an estimated time of completion presently.
- LifeLabs can provide updates as to the status of the call centre.

14. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

15. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- The affected parties need to be identified, contact information needs to be assessed and verified, communication materials need to be drafted, supports need to be identified and procured, and resources need to be obtained to carry out notifications and remediation.
- LifeLabs initiated of this work immediately when the incident was discovered.
- Employees have worked around the clock to ensure that as little time as possible elapsed between when the breach was discovered and when notification began.

16. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizen Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan, and New Brunswick^{s.13} and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

17. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- LifeLabs is ensuring credit monitoring for those affected by the breach.

• s.13

•

- Questions related to this matter should be directed to LifeLabs.

18. What recourse do clients have if they aren't satisfied with the support they receive through the call centre?

- Citizens may contact the Office of the Information and Privacy Commissioner if they are concerned with the way this incident is being handled.

19. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- Questions related to this matter should be directed to them.

s.13

Formatted: Font: (Default) +Body (Calibri), English (United Kingdom), Condensed by 0.15 pt, Highlight

Contract Management – LifeLabs & Ministry of Health

20. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of diagnostic testing services for British Columbians outside a hospital setting (about 40 per cent of all tests in the province).
- For some time the province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- After the Laboratory Services Act was implemented, the Ministry The moved to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- BC Government contracts follow procurement rules and include both a privacy protection and a security schedule that clearly set out the requirements that contractors must abide by.
- Those expectations are clearly communicated, and contractors who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.
- If the Province becomes aware that a contractor is non-compliant with any terms of their contract, the Province follows up with the contractor to conduct an investigation, depending on the circumstances.
- s.13

Formatted: Font: (Default) +Body (Calibri), 12 pt,
English (United Kingdom), Condensed by 0.15 pt

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

21. What does the Ministry do to enforce these protections/policies?

- The Ministry requires contractors to adhere to privacy and security requirements in contract.
- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

s.13

22. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand they have contacted law enforcement.
- Questions on this matter should be directed to LifeLabs.

23. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.

Government – Data Security and Privacy Breaches (General)

24. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

25. Has government paid ransoms for return of data?

- No.

26. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

27. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

28. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C related to the notification process in data-breach situations.

29. What is the Office of the Information and Privacy Commissioner’s suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

30. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- While B.C. and Ontario assess the same factors when considering whether to notify individuals impacted by privacy breaches, B.C. is the only province with a centralized team to conduct these assessments and support the delivery of notifications.

s. 13

Questions & Answers
Life Labs Data Security Issue
November 16, 2019

Key Messages

- Protecting British Columbians' privacy is critical.
 - Citizens deserve to know their personal information is secure and protected.
 - The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
 - We understand LifeLabs has notified law enforcement and the Office of the Information and Privacy Commissioner and hired a world-leading cyber security firm investigate and respond to this incident.
- s.13
- More than 60% of British Columbian's lab tests happen in hospitals. There is no evidence to suggest that lab results from hospitals have been compromised through this breach.
 - There is also no evidence to indicate that B.C. government systems are affected by this breach.
 - 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 to quickly address the breach and mitigate impacts.

Background

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cybersecurity incident with their booking system. At that time they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7th – the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- 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.
- We understand LifeLabs have also contacted law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, consulting with the Ministries of Health and the Ministry of Citizen Services.
- LifeLabs is still investigating the full scope of the breach to determine what data has been impacted. On Nov. 19 they indicated^{s.13}

s.13

- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C. with about three million clients. They are working closely with the Ministries of Health and Citizens' Services to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.

s.13

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28st that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

s.13

3. When LifeLabs was first detected the breach, did they contact the police?

- We understand LifeLabs have contacted the police.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What database did they access? Where was the information accessed from?

LifeLabs initially confirmed that the information appeared to have been accessed from one of their internal databases, s.13

s.13

5. What exactly was the data that was taken (names, test results)?

- Impacted data s.13 lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- 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.

6. How many B.C. residents are affected?

s.13

s.13

7. What did the B.C. government do following the report by LifeLabs?

- LifeLabs is providing daily updates on their investigation to the Ministries of Health and Citizens Services.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged a world-leading cyber security firm to help them with the technical aspects of their investigation.

We are seeking formal assurances and documentation from LL to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

8. When did the B.C. Government find out that B.C. data was impacted?

- When the incident was first reported to the Province on October 28th, it was initially unknown if data about B.C residents was affected.
- However, after further investigation, LifeLabs confirmed on November 7th that B.C. residents' data was included in the breach.
- s.13

- LifeLabs has engaged a world-leading cyber security firm to help them with the technical aspects of their investigation.
- The company has implemented additional proactive monitoring solutions to detect further threats and attacks.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs.
- The ministries have been in daily contact with LifeLabs since the incident was reported, and LifeLabs has provided daily updates on the progress made with their investigation.

9. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed to fully ascertain the scope of the breach, as well as the data source, as this information is a critical part of the notification and remediation process.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

10. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has the personal information of many British Columbians. Officials from Citizens' Services and Health are working to ensure LifeLabs' investigation and response are thorough and effective.

11. Have any government systems been affected?

- Government systems have security measures in place to prevent infiltrations, and proactive monitoring tools are in place to detect threats.
- At this time, there are no indications that B.C. government systems are affected by this breach.

Next Steps

12. What is LifeLabs doing to support affected clients?

- LifeLabs is preparing their notification process – s.13
s.13
- Their notification process will include a call centre to address any inquiries.
- Clients with questions and concerns about the breach can contact the call centre, which will open to support clients soon.
- LifeLabs has also confirmed that the affected individuals will be offered some form of credit protection or monitoring.

s.13

13. When will the call centre be set up?

- LifeLabs is working to set up the call centre and this is a priority.
- We do not have an estimated time of completion presently.
- LifeLabs can provide updates as to the status of the call centre.

14. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

15. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- The affected parties need to be identified, communication materials need to be drafted, supports need to be identified and procured, and resources need to be obtained to carry out notifications and remediation.
- LifeLabs initiated all of this work immediately when the incident was discovered.
- Employees have worked around the clock to ensure that as little time as possible elapsed between when the breach was discovered and when notification began.

s.13

16. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizen Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

17. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- LifeLabs is ensuring some form of credit monitoring/protection is provided for those affected by the breach.
- LifeLabs have assured us that they are taking every pre-caution necessary to contain the breach and prevent further dissemination of the information. Questions related to this matter should be directed to LifeLabs.

18. What recourse do clients have if they aren't satisfied with the support they receive through the call centre?

- Citizens may contact the Office of the Information and Privacy Commissioner if they would like to file a complaint about government's response to this incident.

19. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- Questions related to this matter should be directed to LifeLabs.

Contract Management – LifeLabs & Ministry of Health

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

20. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of diagnostic testing services for British Columbians outside a hospital setting (about 40 per cent of all tests in the province).
- For some time the province's Medical Service Plan covered the costs of those tests on a fee-for-service model.
- The moved to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- BC Government contracts follow procurement rules and include both a privacy protection and a security schedule that clearly set out the requirements that contractors must abide by.
- Those expectations are clearly communicated, and contractors who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.
- If the Province becomes aware that a contractor is non-compliant with any terms of their contract, the Province follows up with the contractor to conduct an investigation, depending on the circumstances.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

21. What does the Ministry do to enforce these protections/policies?

- The Ministry requires contractors to adhere to privacy and security requirements in contract.
- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

22. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand they have contacted law enforcement.
- Questions on this matter should be directed to LifeLabs.

23. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.

Government – Data Security and Privacy Breaches (General)

24. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

25. Has government paid ransoms for return of data?

- No.

26. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

27. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

28. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

29. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

30. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- While B.C. and Ontario assess the same factors when considering whether to notify individuals impacted by privacy breaches, B.C. is the only province with a centralized team to conduct these assessments and support the delivery of notifications.

Questions & Answers

Life Labs Data Security Issue

November 16, 2019

Key Messages

- Protecting British Columbians' privacy is critical. Citizens deserve to know their personal information is secure and protected.
- We understand that British Columbians' client data was breached in a cyber attack at LifeLabs.
- The Ministries of Health and Citizens' Services are closely monitoring and consulting with LifeLabs as it responds to this incident.
- We understand LifeLabs has notified law enforcement, the Office of the Information and Privacy Commissioner, and hired a world-leading cyber security firm to investigate and respond to this incident.

s.13

- More than 60% of British Columbian's lab tests happen in hospitals. There is no evidence to suggest that lab results from hospitals have been compromised through this breach.
- 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.

If pressed:

s.13

Background

- On October 28, 2019 LifeLabs made the Ministry of Health aware of a cyber-security incident with their booking system. At that time they did not believe that any patient data had been compromised.
- LifeLabs confirmed that B.C. resident data had been compromised on November 7th – the breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- The Office of the Information and Privacy Commissioner was informed of the incident – as it was confirmed that B.C. residents' data was involved. The Office of the Information and Privacy Commissioner is being kept up to date on the investigation.
- We understand LifeLabs have also contacted law enforcement about this incident.
- LifeLabs is a private company and has been leading the investigation, consulting with the Ministries of Health and the Ministry of Citizen Services.
- LifeLabs is still investigating the full scope of the breach to determine what data has been impacted. On Nov. 19 they indicated^{s.13}
^{s.13} and could impact their entire clientele including clients in B.C. and elsewhere.
- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C. with about three million clients. They are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- The notification is expected to be indirect, with LifeLabs issuing a media statement and purchasing advertising indicating that a breach could have affected all their clients.
- LifeLabs plans to have call centres for clients to contact, where they can receive further information and be connected to a free credit monitoring service for a year.

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October 28st that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information during an ongoing investigation could have potential negative effects on the impacted parties and we will wait until the investigation has progressed further before providing any additional information.

3. When LifeLabs was first detected the breach, did they contact the police?

- We understand LifeLabs have contacted the police.
- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

4. What database did they access? Where was the information accessed from?

- LifeLabs knows that British Columbians client data was breached.
- They have indicated that impacted data could include lab results in addition to patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.

5. How many B.C. residents are affected?

- LifeLabs believes data from all their clients could have been included in the breach, including clients in B.C, and else where.
- Approximately three million British Columbians have had tests done at LifeLabs.

6. What did the B.C. government do following the report by LifeLabs?

- The Ministries of Health and Citizens Services have required LifeLabs provide seniors daily updates on their investigation.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity, including providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken.
- LifeLabs has engaged a world-leading cyber security firm to help them with the technical aspects of their investigation.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Issue Specific – B.C. Government

7. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been enough? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed to fully ascertain the scope of the breach, as well as the data source, as this information is a critical part of the notification and remediation process.

If pressed:

- s.13

8. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs has the personal information of many British Columbians. Officials from Citizens' Services and Health are working to ensure LifeLabs' investigation and response are thorough and effective.

9. Have any government systems been affected?

- There are no indications that B.C. government systems are affected by this breach.

- 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.

Next Steps

10. What is LifeLabs doing to support affected clients?

- LifeLabs undertakes about 40 per cent of diagnostic testing in B.C. with about three million clients.
- We understand they are working to develop a plan to notify affected B.C. residents that they could have been impacted and to offer protections to mitigate risks associated with the breach.
- We understand that plan includes call centres for clients to contact, where they can receive further information and be connected to a free credit monitoring service for a year.

11. When will the call centre be set up?

- We do not have an estimated time of completion presently.
- LifeLabs can provide updates as to the status of the call centre.

12. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

13. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.

- s.13

14. Does government support LifeLab's approach and timing?

- LifeLabs has been working with their legal counsel, external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizen Services in this matter.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and must meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

15. What will LifeLabs – or government – do to help if these clients experience identity theft, fraud or other privacy violations as a result of this breach?

- We understand LifeLabs will connect clients to a free credit monitoring service for a year.
- LifeLabs have assured us that they are taking every pre-caution necessary to contain the breach and prevent further dissemination of the information.
- We are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.
- Further questions related to this matter should be directed to LifeLabs.

16. Does the Province believe LifeLab’s mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs’.
- We continue to monitor their response closely and are pursuing formal assurances and documentation from LifeLabs to ensure that they have taken adequate security measures to prevent this from re-occurring.

Contract Management – LifeLabs & Ministry of Health

17. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- LifeLabs provides the majority of diagnostic testing services for British Columbians outside a hospital setting (about 40 per cent of all tests in the province).
- For some time the province’s Medical Service Plan covered the costs of those tests on a fee-for-service model.
- The moved to a service provision agreement with LifeLabs to help with cost certainty in budgeting for those services.
- B.C. Government service agreements follow procurement rules that include both privacy protection and a security schedule that clearly set out the requirements that contractors must abide by.

18. What does the Ministry do to enforce these protections/policies?

- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.

CONFIDENTIAL ADVICE TO MINISTER

DRAFT – NOT FOR DISTRIBUTION

- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

19. Does government have a duty to report breaches to law enforcement? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- We understand they have contacted law enforcement.
- Questions on this matter should be directed to LifeLabs.

20. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.

Government – Data Security and Privacy Breaches (General)

21. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

22. Has government paid ransoms for return of data?

- No.

23. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- 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.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

24. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, seven days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

25. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C related to the notification process in data-breach situations.

26. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.

27. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.

LifeLabs November 18

Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it comes to the personal information of citizens.
- ~~Citizens must~~ 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 also notified the Office of the Information and Privacy Commissioner of this incident.
- At this time, there is no evidence to indicate that B.C. government systems are affected by this breach.
- 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 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 still investigating the full scope of those who may be affected.
- Once the scope is determined, LifeLabs will begin the notification process.

On the Question of why Law Enforcement was not notified

- LifeLabs has indicated they ~~will be~~ were going to be notifying the RCMP ~~in the near future.~~
- s.13; s.15

BC's critical priority has always been the safety and security of the information and protecting the privacy of ~~BC citizens~~ British Columbians.

⊖ LifeLabs and the BC government have been cooperating in the investigation

- LifeLabs has been working with their legal counsel, and external cyber-security experts, and cyber security and privacy officials at the Ministry of Citizen Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and has to meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

s.13

•

Formatted: Indent: Left: 1.27 cm, No bullets or numbering

Formatted: Indent: Left: 1.27 cm, No bullets or numbering

Formatted: Normal, No bullets or numbering

LifeLabs November 18

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 also notified the Office of the Information and Privacy Commissioner of this incident.
- At this time, there is no evidence to indicate that B.C. government systems are affected by this breach.
- 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 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 still investigating the full scope of those who may be affected.
- Once the scope is determined, LifeLabs will begin the notification process.

On the Question of why Law Enforcement was not notified

- LifeLabs indicated they are going to be notifying the RCMP shortly.
- s.15
- Government's critical priority has always been the safety and security of the information and protecting the privacy of British Columbians and so our efforts have focused on that.
- LifeLabs has been working with their legal counsel, external cyber-security experts, and with cyber security and privacy officials at the Ministry of Citizen Services in this matter.
- LifeLabs operates as a private company in B.C., Ontario, Saskatchewan and New Brunswick and has to meet different legislative notification and disclosure requirements, including the engagement with RCMP or other law enforcement.

s.13

Speaking Points for health authority staff

Please feel free to share the following information with your staff, including those who may be patient-facing in hospital laboratories. You may also consider using this information in your health authority newsletters and/or on your public-facing websites, as required.

s.13

s.13

s.13

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

Speaking Points for health authority staff

Please feel free to share the following information with your staff, including those who may be patient-facing in hospital laboratories. You may also consider using this information in your health authority newsletters and/or on your public-facing websites, as required.

s.13

s.13

Formatted: Font: Bold

s.13

Formatted: Font: Bold

Formatted: Comment Text, Space After: 0 pt, No bullets or numbering

STATEMENT

For Immediate Release
[release number]
[date]

Ministry of Health

s.13

Media contact: Ministry of Health Communications
250 952-1887 (media line)

Background:

- More than 60% of British Columbian's lab tests happen in hospitals. This breach did not affect any of that data.
- We encourage British Columbians who have had test done at LifeLabs to contact Lifelabs by visiting www.xxx.ca or calling 1-877-xxx-xxxx.

STATEMENT

For Immediate Release

[release number]

[date] Dec. 17, 2019

Ministry of Health

s.13

s.13

Media contact: Ministry of Health Communications
250 952-1887 (media line)

Background:

- More than 60% of British Columbian's lab tests happen in hospitals. This breach did not affect any of that data.
- We encourage British Columbians who have had test done at LifeLabs to contact Lifelabs by visiting www.xxx.ca or calling 1-877-xxx-xxxx.

Marriott, Sarah GCPE:EX

Subject: Daily Call: LL
Location: Dial in: s.15; s.17 Participant^{s.15; s.17} Moderator: Ian Rongve

Start: Mon 2019-12-02 4:30 PM
End: Mon 2019-12-02 5:00 PM
Show Time As: Tentative

Recurrence: Daily
Recurrence Pattern: every weekday from 4:30 PM to 5:00 PM

Meeting Status: Not yet responded

Organizer: Rongve, Ian HLTH:EX

Required Attendees Barclay, Corrie A HLTH:EX; Diacu, Mariana HLTH:EX; Watt, Rebecca HLTH:EX; Slater, James; Prevost, Jean-Marc GCPE:EX; Pearce, Alison HLTH:EX (Alison.Pearce@gov.bc.ca); May, Stephen GCPE:EX; Lauvaas, Kirsten GCPE:EX; Carroll, Scott CITZ:EX; Russell, Shannon CITZ:EX; XT:Bayne, James HLTH:IN; Marriott, Sarah GCPE:EX; Perkins, Gary CITZ:EX

Daily called scheduled December 2 to 20

From: [Lauvaas, Kirsten GCPE:EX](#)
To: [Prevost, Jean-Marc GCPE:EX](#)
Cc: [Marriott, Sarah GCPE:EX](#); [Burton, Meribeth GCPE:EX](#); [May, Stephen GCPE:EX](#)
Subject: RE: updated Q & A
Date: November 22, 2019 4:58:28 PM

Thanks, Jean-Marc. I am definitely around tomorrow; Sunday is a bit busier, but reach out if you need to. Looks like we're more likely to get traction with these early next week.

From: Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Sent: November 22, 2019 4:54 PM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Cc: Barclay, Corrie A HLTH:EX <Corrie.Barcly@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Diacu, Mariana HLTH:EX <Mariana.Diacu@gov.bc.ca>; Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Burton, Meribeth GCPE:EX <Meribeth.Burton@gov.bc.ca>; May, Stephen GCPE:EX <Stephen.May@gov.bc.ca>
Subject: Re: updated Q & A

Thank you.

Sent from my iPhone

On Nov 22, 2019, at 4:49 PM, Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca> wrote:

These are updated following today's call.

As there are still moving pieces – they are still draft.

I have left Scott's comments on to remind myself of where we are hoping for new data or confirmations to come in.

Please let the group know of concerns or suggestions.

Thanks!

<image001.png>

Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

<QA_LL_Nov 22 5pm (jmp).docx>

Marriott, Sarah GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 16, 2019 1:47 PM
To: Lauvaas, Kirsten GCPE:EX; Prevost, Jean-Marc GCPE:EX
Subject: RE: generic LL statement

That's great. Thanks Kirsten.

From: Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>
Sent: December 16, 2019 1:46 PM
To: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Subject: generic LL statement

FYI this version is currently with my ADM and her team for review.

Kirsten

Marriott, Sarah GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 16, 2019 12:20 PM
To: LeGuilloux, Marg GCPE:EX
Subject: FW: Statement
Attachments: BC - LL statement.docx

From: Marriott, Sarah GCPE:EX
Sent: December 16, 2019 12:15 PM
To: Russell, Shannon CITZ:EX <Shannon.Russell@gov.bc.ca>
Subject: Statement

Here's the statement – it's formatted as if it's proactive, but it will be REACTIVE-ONLY in response to media requests.

Sarah

Sarah Marriott
Issues Manager
250.361.8416

Page 05 of 35

Withheld pursuant to/removed as

s.13

Marriott, Sarah GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 17, 2019 8:47 AM
To: Berndt, Eric GCPE:EX
Subject: KMs
Attachments: LL - MJD.docx

Attached

Sarah Marriott
Issues Manager
250.361.8416

LifeLabs

Background:

- On Dec 17 it was announced that LifeLabs, the private company responsible for conducting approximately 34% of B.C. lab testing services, experienced a significant data breach stemming from a cyber-security incident.
- Government and health authority systems were not impacted. Most of British Columbia's lab tests happen in hospitals and that data is not affected by this breach.
- LifeLabs says their investigation has revealed NO evidence British Columbians' lab test results were impacted (not the case in Ontario).
- The breached data in BC included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- LifeLabs has hired world-leading cyber security firms to investigate and respond – including implementing additional safeguards to further secure their networks going forward.
- The Province will continue to work with LifeLabs to help them ensure that their investigation and response are thorough and effective.
- LifeLabs is providing all customers access to free identity theft insurance and monitoring services. People should contact LifeLabs directly.

Key messages:

- It's certainly concerning. The protection of British Columbians' privacy is critical.
- Lifelabs is a private company, I encourage anyone who may have been a client of LifeLabs to contact them.
- I understand they've set up a call centre to assist people.

If pressed:

- The Ministry of Citizen Services is coordinating media on this – they'd be happy to get you further information.

Marriott, Sarah GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 17, 2019 9:44 AM
To: Prevost, Jean-Marc GCPE:EX
Subject: RE: ASAP -- pls send the LL statement
Attachments: Media Statement Dec 17 2019 930am.docx

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 17, 2019 9:41 AM
To: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Subject: ASAP -- pls send the LL statement
Importance: High



Ministry of
Health

Jean-Marc Prevost

COMMUNICATIONS DIRECTOR
Desk: 236-478-0302
Cell: 250-886-2154

Background:

- LifeLabs says there is no evidence British Columbians' lab test results were impacted.
- The breached data in B.C. includes patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- British Columbians who have had tests done at LifeLabs are encouraged to contact LifeLabs by visiting www.customernotice.lifelabs.com or calling 1-888-918-0467.
- LifeLabs is a private company responsible for conducting approximately 34% of B.C. lab testing services.

Marriott, Sarah GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 17, 2019 10:29 AM
To: Prevost, Jean-Marc GCPE:EX; Rongve, Ian HLTH:EX
Subject: FYI - LL website live w/ open letter

Just FYI – below from CITZ

And online: <https://www.newswire.ca/news-releases/lifelabs-releases-open-letter-to-customers-following-cyber-attack-889534499.html>

From: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>
Sent: December 17, 2019 10:21 AM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Donaldson, Ian R CITZ:EX <Ian.Donaldson@gov.bc.ca>
Cc: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>
Subject: RE: FOR REVIEW: LL KM Q A Dec 16 6pm

Their website is live:
<https://www.customernotice.lifelabs.com>
or
<https://customernotice.lifelabs.com/>

Here's the text:

Copyright

Page 11 of 35

Withheld pursuant to/removed as

Copyright

Marriott, Sarah GCPE:EX

Subject: 4:45 - Daily Call: LL

Location: Dial in: ^{s.15; s.17} Participant ^{s.15; s.17} Moderator: Ian Rongve

Start: Mon 2019-12-16 4:45 PM

End: Mon 2019-12-16 5:15 PM

Show Time As: Tentative

Recurrence: Weekly

Recurrence Pattern: Occurs every weekday from 4:30 PM to 5:00 PM effective 02/12/2019 until 20/12/2019. (UTC-08:00)
Pacific Time (US & Canada)

Meeting Status: Not yet responded

Organizer: Rongve, Ian HLTH:EX

Required Attendees: Prevost, Jean-Marc GCPE:EX; XT:Bayne, James HLTH:IN; Slater, James; Perkins, Gary CITZ:EX; Marriott, Sarah GCPE:EX; Barclay, Corrie A HLTH:EX; Diacu, Mariana HLTH:EX; Watt, Rebecca HLTH:EX; Russell, Shannon CITZ:EX; Lauvaas, Kirsten GCPE:EX; Pearce, Alison HLTH:EX (Alison.Pearce@gov.bc.ca); May, Stephen GCPE:EX; Carroll, Scott CITZ:EX

Optional Attendees: Emerson, Kim GCPE:EX

Importance: High

Per Ian Rongve's request, start time for today's meeting pushed back by 15 minutes. **New start time of 4:45 p.m.**

Marriott, Sarah GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 20, 2019 8:08 AM
To: van Baarsen, Amanda HLTH:EX
Cc: Shewchuk, Chris GCPE:EX; Prevost, Jean-Marc GCPE:EX
Subject: LL quote for MD

FYI -

Wilkinson: I'm the first one to say that I don't know the answer to that, but it should have been done if it wasn't done. If we're in some way responsible for how the contract got written then we did it wrong. Right now the answer is that there's been a huge blunder and there's been a huge hole driven through the wall of our personal information and they didn't have the courtesy to tell us so we could take protective measures.

Now they say if something goes wrong, they'll think about giving us some insurance if we apply for it. I call BS on all that stuff. Tell us the truth, tell us the truth you knew on day two, not day 42.

Sarah Marriott
Issues Manager
250.361.8416

Wilkinson - LifeLabs privacy breach

CKNW

Thursday, December 19, 2019, 12:36

By CKNW Simi Sara

Copyright

Andrew Wilkinson: Personal information, health information is the property of the patient -- that's you and me -- it does not belong to the government, it does not belong to the lab, it does not belong to the doctor. This information got stolen six weeks ago from the vast majority of our population and they didn't have the courtesy to tell us. For six weeks they spent their time covering their rear ends and the Ministry of Health was apparently fretting about it.

Page 14 of 35 to/à Page 16 of 35

Withheld pursuant to/removed as

Copyright

Marriott, Sarah GCPE:EX

From: Marriott, Sarah GCPE:EX
Sent: December 18, 2019 2:48 PM
To: van Baarsen, Amanda HLTH:EX; Prevost, Jean-Marc GCPE:EX; Shewchuk, Chris GCPE:EX
Subject: FW: CBC Online: Proposed class-action lawsuit launched against LifeLabs in BC Supreme Court

Just FYI

From: tno@gov.bc.ca <tno@gov.bc.ca>
Sent: December 18, 2019 2:43 PM
Subject: CBC Online: Proposed class-action lawsuit launched against LifeLabs in BC Supreme Court

CBC Online

18-Dec-2019 14:40

Copyright

TNO...

<https://www.cbc.ca/news/canada/british-columbia/proposed-class-action-lawsuit-launched-against-lifelabs-in-b-c-supreme-court-1.5401477>

This e-mail is a service provided by Government Communications and Public Engagement and is only intended for the original addressee. All content is the copyrighted property of a third party creator of the material. Copying, retransmitting, redistributing, selling, licensing, or emailing the material to any third party or any employee of the Province who is not authorized to access the material is prohibited.

Marriott, Sarah GCPE: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

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

Page 21 of 35 to/à Page 22 of 35

Withheld pursuant to/removed as

s.13

LifeLabs

Background:

- On December 17, it was announced that LifeLabs experienced a significant data breach stemming from a cyber-security incident.
- Lifelabs is a private company that provides medical laboratory services under a long-standing service provision agreement with the Province.
- Lifelabs has said the breach affects 15 million Canadian customers, mostly in B.C. and Ontario. Last year, LifeLabs performed 34 million publicly funded tests in BC alone.
- The breached data in B.C. included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- LifeLabs has told the Province their investigation has revealed NO evidence British Columbians' lab test results were impacted (lab test results from 85,000 Ontario customers were taken).
- LifeLabs says they have paid to secure the breached data. At this time, the cyber-security firms that are working with LifeLabs have not seen any further unauthorized use or disclosure of data.

Key messages:

- It's something that the province takes really seriously. Millions of people rely on Lifelabs – they're a significant part of healthcare in B.C.
- Lifelabs have been working with world-class cyber security experts to take steps to secure the information and further secure their networks going forward.
- s.13
- Lifelabs is encouraging anyone who has been a client or who is concerned to contact them at 1-888-918-0467 or <https://customernotice.lifelabs.com/>. They're offering free identity theft and cyber security protection services.
- Security experts from the Province have also been working with them. It's our expectation that they'll cooperate with the privacy commissioner's investigation and continue to work closely with us to fulfil their obligations to protect people's information.

Advice to Minister

s.13

Ministry Statement:

s.13

LifeLabs has already implemented additional security controls to further protect their systems, and engaged very reputable external resources to help them with the technical aspects of their investigation.

Background:

- LifeLabs is a private company and is leading the investigation and response. Any questions on the investigation should be directed to LifeLabs.

s.13

- Privacy and data security experts from the B.C. government are assisting LifeLabs in an advisory capacity.
- Government requires all contractors to adhere to stringent privacy and security requirements in their contracts.
- Government contracts follow procurement rules and include both a privacy protection and a security schedule that clearly set out the legal requirements that the contractor must abide by.
- Those expectations are clearly communicated, and contractors who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.
- If the Province receives evidence that a contractor is non-compliant with any terms of their contract, the contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

s.13

Questions & Answers
Life Labs Data Security Issue
November 16, 2019

Key Messages

- Protecting the privacy and security of British Columbians is a critical priority especially where it comes to the personal information of citizens.
- Citizens must have the utmost confidence that their information is secure and protected.
- The Province is aware that LifeLabs encountered a data breach involving client information.
- The Ministries of Health and Citizens' Services are working closely with LifeLabs in a consulting role as LifeLabs responds to the incident.
- LifeLabs has also notified the Office of the Information and Privacy Commissioner of this incident.
- s.13
At this time, there is no evidence to indicate that B.C. government systems are affected by this breach.
- 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.

s.13

s.13

Questions & Answers

Issue Specific – LifeLabs

1. When did LifeLabs notify the B.C. government about the incident?

- LifeLabs initially notified the B.C. government on October^{s.13} that there had been an incident and confirmed that British Columbians' data was affected on November 7th.

2. Have any demands for payment been made or indications received as to what will be done with the data?

- LifeLabs is a private company, and paying the ransom is their decision to make.
- Any comments regarding specific details should be directed to LifeLabs, as they are leading the investigation.

If pressed:

- Releasing information regarding any negotiations could have potential negative effects on the impacted parties and on LifeLabs.
- As such, we will not comment further on this.

3. What are the potential ramifications of s.13 -a decision to pay ransom?

- Organizations that have paid ransoms may be further targeted.
- Organizations that do not pay the ransom may have clients' personal information exposed on the internet or in some other public manner.

4. When LifeLabs was first contacted by the threat actors, did they contact the police?

- LifeLabs is a private company and the decision to engage law enforcement is solely theirs.
- Questions on this matter should be directed to LifeLabs.

5. What database did they access? Where was the information accessed from?

- LifeLabs has confirmed that the information appears to have been accessed from one of their internal databases.
- However, they are still in the process of investigating the exact origin of the data.
- LifeLabs has various databases that store personal information, such as names, addresses, dates of birth, personal health numbers (BC Services Card/Care Card numbers) and gender.

s.13

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

6. What exactly was the data that was taken (names, test results)?

- No clinical lab results are known to be included in this data set.
- 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 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.

7. How many B.C. residents are affected?

- LifeLabs is still investigating the full scope of those who may be affected.
- Once the scope is determined, LifeLabs will begin the notification process.

8. Are you confident that the threat actors don't have additional data? How can you know for sure that people's personal information is safe?

- LifeLabs is working to confirm the scope of the incident.

9. What steps are you taking to ensure any security gaps are addressed so this doesn't happen again?

- The Ministries of Health and Citizens Services' are receiving daily updates from LifeLabs to ensure government is fully informed as to the progress of LifeLabs' investigation.
- Any security or privacy issues are being communicated to the appropriate Ministry's investigation unit for review.
- LifeLabs states they now have security controls in place to protect their systems and the information stored within them.
- No organization globally is immune to attack.
- In this instance, attackers found and exploited a weakness.
- LifeLabs has since taken additional steps to protect their systems.
- The company has implemented additional proactive monitoring solutions to detect further threats and attacks.
- LifeLabs has engaged very reputable external resources to help them with the technical aspects of their investigation.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

Issue Specific – B.C. Government

10. When did the B.C. Government find out that B.C. data was impacted?

- When the incident was first reported to the Province, it was initially unknown if data about B.C. residents was affected.
- However, after further investigation, LifeLabs confirmed on November 7th that data about B.C. residents was included in the breach.
- 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.

11. What did the B.C. government do following the report by LifeLabs?

- As LifeLabs is a private company, they are leading the investigation.
- They have already implemented additional security controls to further protect their systems.
- They have also engaged reputable external resources, including an internationally recognized cyber-security company, to help them with the technical aspects of their investigation.
- Privacy and data-security experts from the B.C. Government have been supporting their efforts in an advisory capacity.
- This includes providing assistance and oversight to LifeLabs to ensure that appropriate incident-response measures are taken to address what has occurred.
- The ministries have been in daily contact with LifeLabs since the incident was reported, and LifeLabs has provided daily updates on the progress made with their investigation.

12. LifeLabs and government have known about this breach for nearly a month – do you feel the actions taken to date have been sufficient? Don't you think clients have a right to know sooner if their personal information is potentially at risk?

- The Province recognizes that notifying affected individuals quickly is crucial when they have been subject to a privacy breach.
- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process to prepare resources to accomplish this notification as efficiently as possible.
- From the moment LifeLabs reported this incident to government, all efforts and resources were deployed to fully ascertain the scope of the breach, as well as the data source, as this information is a critical part of the notification and remediation process.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

13. Have any government systems been affected?

- Government systems have strong security measures in place to prevent infiltrations, and proactive monitoring tools are in place to detect threats.
- At this time, there are no indications that B.C. government systems are affected by this breach.

14. Government – through the Ministry of Health and the Ministry of Citizens' Services – has been acting as consultants with LifeLabs throughout this process. This is LifeLab's breach, so why are you involved?

- LifeLabs is a private company and is leading the investigation and response to the incident.
- LifeLabs is contracted through the Ministry of Health, so they are working in partnership to ensure the situation is resolved.
- The Provincial Health Services Authority manages the LifeLabs contract and is also involved.
- Citizens' Services is being consulted to ensure that the investigation follows proper protocols, including incident handling and response, as per government's information incident management policies.

Next Steps

15. What is LifeLabs doing to support affected clients?

- Once LifeLabs determines the full scope of affected data, they will begin notifying those who have been affected by the breach.
- Lifelabs is in the process of setting up a call centre to address any inquiries.
- Clients with questions and concerns about the breach can contact the call centre, which will open to support clients soon.
- LifeLabs has also confirmed that the affected individuals will be offered credit protection at no cost via TransUnion for a 12-month period.

16. When will the call centre be set up?

- LifeLabs is working to set up the call centre and this is a priority.
- We do not have an estimated time of completion presently.
- LifeLabs can provide updates as to the status of the call centre.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

17. Who will manage the call centre and where is the budget coming from? How much will this cost?

- LifeLabs will oversee and fund the call centre.
- Questions related to this matter should be directed to LifeLabs.

18. Why didn't LifeLabs alert affected clients that their information was breached before now?

- There is significant work required for incidents like this before notification can be conducted.
- The affected parties need to be identified, contact information needs to be assessed and verified, communication materials need to be drafted, supports need to be identified and procured, and resources need to be obtained to carry out notifications and remediation.
- LifeLabs initiated of this work immediately when the incident was discovered.
- Employees have worked around the clock to ensure that as little time as possible elapsed between when the breach was discovered and when notification began.

19. Does government support LifeLab's approach and timing?

- LifeLabs has consulted with the Ministries of Health and Citizens' Services throughout the process.
- LifeLabs has worked with government since they became aware and shared information on their approach.
- They have taken strong and decisive action in dealing with a difficult situation.
- As with any incident of this nature, government and LifeLabs will debrief following the conclusion of the incident to identify lessons learned.
- Government has appreciated the open and transparent cooperation that LifeLabs has provided in addressing this issue.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

20. What will LifeLabs – or government – do to help if these clients experience identity theft or fraud as a result of this breach?

- LifeLabs is ensuring credit monitoring for those affected by the breach.
- Questions related to this matter should be directed to LifeLabs.

If pressed:

- Credit-monitoring services are provided by third-party companies, to alert an individual when changes affecting their credit scores occur, so that they may respond quickly to an identity-theft risk.
- They are a common remediation response to breaches that have the potential for identity theft or fraud.

21. What recourse do clients have if they aren't satisfied with the support they receive through the call centre?

- Citizens may contact the Office of the Information and Privacy Commissioner if they are concerned with the way this incident is being handled.

22. Does the Province believe LifeLab's mitigation responses (call centre, credit monitoring) for clients are enough?

- LifeLabs is a private company and decisions on these issues are solely LifeLabs'.
- Questions related to this matter should be directed to them.

Contract Management – LifeLabs & Ministry of Health

23. The Ministry of Health holds a contract with LifeLabs – what protections are in place when government data is in the custody of a contractor or service provider?

- Government contracts follow procurement rules and include strict requirements for privacy and security.
- Contractors are expected to follow the terms of their contracts related to the protection of personal information.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

24. What does the Ministry do to enforce these protections/policies?

- The Ministry requires contractors to adhere to privacy and security requirements in contract.
- Contracts are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that contractors must meet the terms set out in their contracts are clearly communicated both in the contract and verbally.
- Contractors 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 contractor is non-compliant with any terms of their contract, the matter must be reported to the contract manager.
- The contractor must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.

25. Does government have a duty to report breaches to the authorities? Why didn't you?

- As this incident impacted LifeLabs' infrastructure, and they are a private company, decisions about contacting law enforcement rest solely with them.
- Questions on this matter should be directed to LifeLabs.

26. How can people have confidence that their health records are secure in B.C.?

- Protection of government data and networks is a top priority for this government, especially where it concerns British Columbians' personal information.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing awareness of best practices for information technology overall.
- Government is constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.

Government – Data Security and Privacy Breaches (General)

27. Does government pay ransoms?

- To date, the Province has not had a situation where we have had to consider paying a ransom for the return (or destruction) of data – personal or otherwise.

28. Has government paid ransoms for return of data?

- No.

29. What specific actions does government take when they are aware of a real – or potential – breach of data, especially personal data from British Columbians?

- Government has security controls to protect networks, systems and data.
- Government has an established, effective information incident management policy and a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

30. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- Government is committed to strong privacy and security controls and to increasing overall awareness of best practices for information technology.
- We are constantly evaluating threats, with systems monitoring 24 hours per day, 7 days a week.
- Government has an established, effective information incident management policy.
- We also have a team of trained information incident investigators.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

CONFIDENTIAL ADVICE TO MINISTER
DRAFT – NOT FOR DISTRIBUTION

31. Is there a specific law in B.C. related to the notification process in data breach situations?

- There are no specific laws in B.C. related to the notification process in data-breach situations.

32. What is the Office of the Information and Privacy Commissioner's suggested timeframe for responding to breaches of personal information?

- There is no specific timeframe identified for responding to all matters involved in a breach such as this.
- However, best practice is to address all issues in as little time as possible to mitigate harm.

33. Is there an established best practice for notifying individuals that their personal information has been compromised? Is this different in B.C. than it is in Ontario?

- Best practices are to notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.
- While B.C. and Ontario assess the same factors when considering whether to notify individuals impacted by privacy breaches, B.C. is the only province with a centralized team to conduct these assessments and support the delivery of notifications.