HANSARD

NOVA SCOTIA HOUSE OF ASSEMBLY

COMMITTEE

ON

PUBLIC ACCOUNTS

Wednesday, October 14, 2020

Legislative Chamber

Cybersecurity and Fraud Risks -
October 2019 Report of the Auditor General, Financial

Printed and Published by Nova Scotia Hansard Reporting Services

Public Accounts Committee

Keith Bain (Chair)
Suzanne Lohnes-Croft (Vice-Chair)
Brendan Maguire
Hon. Margaret Miller
Ben Jessome
Rafah DiCostanzo
Tim Halman
Lisa Roberts
Susan Leblanc

[Brendan Maguire was replaced by Bill Horne.]

In Attendance:

Kim Langille
Legislative Committee Clerk

Gordon Hebb
Chief Legislative Counsel

Mike MacPhee
Acting Deputy Auditor General

Janet White
Audit Principal

Kirk Robinson
Audit Manager

WITNESSES

Nova Scotia Health Authority

Dr. Brendan Carr -
Acting Deputy Auditor General

Derek Spinney -
Vice President, Corporate Services, Infrastructure & Chief Financial Officer

Andrew Nemirovsky -
Senior Director, IM/IT & CIO

Karen Hornberger -
Director of Privacy

House of Assembly
Nova Scotia

HALIFAX, WEDNESDAY, OCTOBER 14, 2020

STANDING COMMITTEE ON PUBLIC ACCOUNTS

9:00 A.M.

CHAIR
Keith Bain

VICE-CHAIR
Suzanne Lohnes-Croft

THE CHAIR: Order please. We'll call the Standing Committee on Public Accounts to order.

Before we begin, I just want to remind everybody in the audience to turn your phones to silent or vibrate, please.

We'll begin with introductions. We'll start with the committee members introducing themselves. I'm going to ask if we go down the front line and then start at the back line and come back up. We'll begin with you, Ms. Roberts.

[The committee members introduced themselves.]

THE CHAIR: Just a couple of reminders before we start. You're asked to please keep your mask on during the meeting unless you're speaking. In order to facilitate the back and forth, I'm not going to be wearing my mask, but I think we have enough distancing at this point.

We're asking also, in an effort to limit movement within the Chamber, for you to stay in your seat as much as possible. In order to accommodate all this, we'll take a short break about the one-hour mark of the meeting. To do that, we have to ask for an agreement from the committee to extend the length of the meeting by 15 minutes. Is it agreed? Thank you.

When you leave the Chamber, you'll go out the side exit. If you come back in, come back in through the main doors. I think that looks after all the preamble that's taking place before this morning's meeting.

On today's agenda, we have officials from the Nova Scotia Health Authority to discuss cybersecurity and fraud risks from the October 19th Financial Report of the Auditor General.

To begin, we'll ask the witnesses to introduce themselves, please.

[The witnesses introduced themselves.]

THE CHAIR: Thank you. We'll ask the witnesses to make their opening remarks. Dr. Carr.

DR. BRENDAN CARR: Thank you very much. Good morning, Mr. Chair and committee members. Thank you very much for the opportunity to meet with you today. My name is Dr. Brendan Carr and I have the privilege to serve as the President and Chief Executive Officer of Nova Scotia Health Authority.

I'm very pleased to be here today with my colleagues: Derek Spinney, our Vice President of Corporate Services, Infrastructure, and Chief Financial Officer; Andrew Nemirovsky, our Senior Director of Information Management, Information Technology, and Chief Information Officer; and Karen Hornberger, our Provincial Director of Privacy.

As you know, we were originally slated to be before you back in April but as we're all aware, COVID-19 changed many of our plans. We are pleased to be here with you today. We welcome this opportunity to discuss questions about cybersecurity and fraud risks as reported in the October 2019 report of the Auditor General. We do accept the findings from that report and we're committed to continuing our efforts to address any outstanding issues.

I'd like to first provide a bit of context around our organization. We are the largest health organization in Atlantic Canada, and indeed the largest employer in Nova Scotia. We serve a population of about 971,000 Nova Scotians and provide some services to other residents in Atlantic Canada.

Within our $2.3 billion budget, we're responsible for hospital and community-based services, including mental health and addictions, public health, and primary health care.

Our settings range from the highly specialized QEII in Halifax to nine regional hospitals and more than 30 community hospitals and health centres. Within the organization there are about 24,700 employees, 6,500 volunteers, over 5,500 learners of

various descriptions working with us, 2,900 physicians and medical residents, 160 contracted continuing care service providers, 37 community health boards, 41 hospital foundations and 33 auxiliaries.

Overall there are probably in excess of 40,000 people working within our health system who are part of our system, members of our communities and, as it pertains to today's discussion, interacting with information within the health system.

As you can see, we operate a large, complex organization with many important stakeholders, and we are committed to being accountable to you and to every Nova Scotian. There has been significant progress following the creation of one health authority, and we know that work is ongoing.

The October 2019 Auditor General's Report contained two themes of concern relating to Nova Scotia Health Authority. The first dealt with that office's assessment of the status of our internal controls and the potential for fraud or error, and our continued progress against strengthening these controls. As a non-accountant, I understand internal controls to really be systems, rules, and processes put in place to ensure the integrity of our financial information and to prevent fraud or loss. They include things like how we control access to our systems, how we reconcile accounts, how we conduct physical audits of particular materials, and what sort of specific approval processes we have in place to ensure that we're using the right resources for the right thing.

There are literally hundreds of such controls in any large accounting system, and we always balance the cost of establishing the control and maintaining that control with the inherent risk associated with the item being protected by that control. So maybe to explain that in a way that I can understand, if we think about the risk of theft of losing track of a large piece of equipment like a CT scanner or an anaesthesia machine that would be by its nature quite conspicuous, there would be inherently quite a minimal risk that we would lose track of one of those kinds of items, whereas if we were looking at a large quantity of cash, we would inherently be very concerned with having specific controls around that.

If we were thinking about a small amount of petty cash less than $100, let's say, we would balance the energy or the effort required to put controls in place around that very small, insignificant relatively, amount of money compared to a large ledger with millions of dollars of receivables or some other significant assets within our system.

We must always find balance and we typically ask ourselves, what's the real potential for loss and what makes sense in terms of the control processes that should be put in place around those specific assets. I would say as stewards of the public resources, we are constantly mindful of this and we're constantly working to develop and understand our control environment better. This is something that is of great importance to our senior leadership team and to our board as well.

Strong internal controls are of the utmost importance to us, which is why several comprehensive strategies have been implemented and are under way to strengthen and support our financial control environment. In Mr. Pickup's report, we are pleased to see his first key message, where he stated that Nova Scotians can rely on government's financial information, including that of the Nova Scotia Health Authority. That says really a great deal.

Do we have gaps? Absolutely, and we have every confidence that we will address the points identified in the report as we continue to move forward. Will we always have some gaps? Given the size and complexity of our organization, probably. This is an area that we understand we will be continuously working on to try to improve our control environment in the context of our changing organization.

We appreciate that the concept of significant control weaknesses, as they're described in the report, may be a cause for concern. As a point of clarification, an organization can have significant control weaknesses, but still have an unmodified or clean audit opinion. That would mean that its financial statements are fairly presented and accurately represent the organization. That's exactly the case with Nova Scotia Health Authority and our financial statements to March 31, 2019 and also to March 31, 2020.

We are also reassured by the fact that neither the Office of the Auditor General nor our own internal audit team have identified any inappropriate activity or expenses and that the weaknesses that have been identified have not really resulted in any significant impact to the organization or our financial statements. We believe this is a recognition of our successes in meeting our obligations to protect the funding allocated to us to provide quality health care to Nova Scotians.

The second theme of the report dealt with cybersecurity and Nova Scotia Health Authority's responsibility in recognizing and mitigating risks, particularly in light of the increasing frequency and sophistication of cyber attacks. We certainly agree that cybersecurity is of paramount concern as a society and as an organization, particularly as we move forward with new technologies like electronic health records.

Unlike the internal control environment we talked about - which is fairly well understood and is practised well, I think - cybersecurity is not quite as clear. It's something that is emerging and it continues to grow and evolve. As such, several years ago a decision was made jointly to manage the technology environment across government, including Nova Scotia Health Authority through Nova Scotia Digital Services.

A shared service model has benefits as we have confidence in our governance partner to make the necessary investments to ensure the security of our technology assets. We continuously work in partnership with NSDS to ensure controls in security.

The privacy and security of the personal information of our employees, physicians, and those we serve is a top priority for Nova Scotia Health Authority. The Auditor General's Report suggests that while the enterprise concepts are Nova Scotia Digital Services' responsibilities, our specific clinical applications are ours and can be at risk.

We agree with that, that we have a responsibility, and that our efforts to educate our employees, our physicians and learners on cybersecurity best practices, and to have policies and procedures in place that govern our use of technology are a critical component of protection. We've been making progress in this field and we're pleased to speak about this to you today. Mr. Nemirovsky will deal with your specific questions in this area.

I would be remiss if I didn't acknowledge that a substantive part of addressing the issue raised by Mr. Pickup relates to our ongoing work bringing together diverse processes and systems from nine previous district health authorities. We marked five years as an organization on April 1st of this year and we are justifiably proud of the significant progress that has been made. There is more work to do and we will continue our efforts to develop and implement the most efficient and appropriate processes across all of our programs and services.

With that, Mr. Chair, I'll thank you again for the opportunity to appear before you today. We look forward to our discussion. We recognize that there may be questions that we can't answer here on the spot so we commit to providing you and your committee the answers as quickly as we can - certainly within the next couple of days. We look forward to offering assurances that we remain accountable for the valuable financial resources entrusted to us as part of our mandate to govern, manage, and deliver quality health services to the people of Nova Scotia.

THE CHAIR: Thank you, Dr. Carr. We'll go now to the first round of questioning; 20 minutes per caucus beginning with the PC caucus. Mr. Halman.

TIM HALMAN: Dr. Carr, thank you very much for your opening remarks. Thank you to all the staff at Nova Scotia Health Authority for their ongoing work to protect Nova Scotians, especially in the COVID-19 era.

You certainly clearly outlined that this is a massive organization with enormous responsibilities. I think Nova Scotians certainly understand that. With 40,000 working within our health system, there's certainly a lot of moving parts. However, COVID-19 has taught us how critical it is to adapt and pivot to changing circumstances. When it comes to fraud risk - when it comes to cybersecurity - I think you said it really well, Dr. Carr: Privacy is paramount. It is paramount to Nova Scotians and Canadians.

That being said, with respect to the status of the internal controls which you've indicated, Dr. Carr, your understanding is that this relates to the systems and rules and various processes that are in place to ensure safety. You indicated that there are gaps. Could

you or staff be specific? What are those two or three perennial gaps and what steps are being taken to address those gaps as it relates to internal controls?

[9:15 a.m.]

BRENDAN CARR: I'll pass that question on to my colleague, Mr. Spinney, to respond.

THE CHAIR: Mr. Spinney.

DEREK SPINNEY: Thank you for having us here today. It is truly our privilege.

It's a great question and with all of those moving parts, how do you focus? How do you even tackle such a thing? We can look to some guidance that's actually provided - some industry standards. In particular, we look at the Committee of Sponsoring Organizations of the Treadway Commission framework. There's a framework that says that there's really five domains that you can pay attention to that can kind of structure your conversation as you go through it.

The first one is your environment. An easy way to explain that is, what's the tone at the top? How are things being set in that organization? To one extreme, is it a cowboy organization - if I can use that analogy - or is it an organization that has the appropriate policies, procedures and framework in place to take internal controls very seriously? Of course, we're here today to talk about us being on the far right of that.

As an example, some of the things that we have is a code of misconduct. Every time an employee joins the organization, they have to read and sign the code of conduct. That's reviewed every year.

Another key part for us that sets this tone at the top is the policy around our board of directors. Our board of directors is also tasked with governance and so they are an independent body that sits and meets with us on a regular basis - that they have the stewardship and the governance of the financial results as well.

Those are just two examples of the environments that you're setting at the top. The next one is around assessing the risks. When you assess a risk, as Dr. Carr mentioned in his opening comments, you really start to take in a few things: the likelihood and the impact.

Step 1 is: What's the threat? If you were dealing with cash, for instance, the risk is that the cash would disappear. In our business office, for instance, if somebody paid something and gave us cash, there's a risk that would end up disappearing. Then the next thing we do is assess that. The way that we assess that is, what's the likelihood that cash could go missing? In this example, we'll say that it was high. Then what's the impact? In

this case, we'll say it's maybe medium because it's smaller amounts of cash. So when we take those two things together, we conclude we need a control to put on top of that.

So there's an inherent risk. We put controls on top and then we re-evaluate it to say, what does that risk look like now? What's the residual risk after those controls have been put into place?

The next part is around communication. We need to make sure that our staff and volunteers - and everybody that actually touches us, including researchers, in fact - that they understand what controls we have in place and what their role is in that.

The last one is around monitoring. It's one thing to have a control; it's another thing to make sure that you're actually monitoring it to make sure that it's actually taking place. Two of the things that were identified in our last audit with the Auditor General were around time reporting. As you can appreciate, with 22,000 people on our payroll - again, a very large organization, as you pointed out - there's an inherent risk that something could go wrong in that process.

We had an external risk assessment done on our payroll. Our payroll is about 70 per cent of our total expenses. That assessment identified 21 inherent risks. After going through all of those - applying controls and so on - we were left with two that we said they still have residual risk that we needed to deal with.

The two in particular were the possibility that people could book overtime and not work overtime - the theft of time, if you will - so you could be paid for an overtime shift that you didn't work, perhaps. The second one was around sick time. It was conceivable that people are taking sick time, but not necessarily being sick, if I can say it that way.

What we've done to mitigate those risks is have five different time systems across Nova Scotia - again, that residual effect of bringing together nine health authorities. We've brought those five systems together at one place so that we can actually see all of that activity and see who's approving their time, because it is required that your time gets approved all the way up to Dr. Carr, in fact. Our board chair actually approves Dr. Carr's time. In that process, we are able to report that our compliance rate was 61 per cent in this previous past year. 2018 was the calendar year of that.

What we've done is bring that system together to make it easier. We actually report that on a monthly basis now, particularly on my team - my team is about 3,500 of the 20,000 - and seeing what we can do to increase that compliance rate. We're already above 70 per cent, and not to preclude what the Office of the Auditor General will say this year, but we think we've done a pretty good job and we'll see what this year's audit concludes around that.

The other thing that we do is we have a budget variance report that goes out to all cost centre managers. A cost centre is kind of like it sounds: a centre that has costs in it that you're responsible for. The finance team issues a report to you that identifies any supplier compensation that was missing your budget by either $50,000 or 10 per cent variance. Even if you've got a smaller budget, a 10 per cent variance would flag you. The system requires you to put in a comment to address that. What was the issue? Until COVID times, we were running at 90 per cent. So 90 per cent of managers that had these variances were actually responding that way.

In addition to that, what we've done - and we've walked through the AG's office some of these numbers - is identify how much overtime is actually exposed there of the people who are not reporting, not signing off of the time. If it's Dr. Carr, for instance - to pick on him today - if he didn't get his time approved, what is the actual inherent risk there? It looks a lot different than somebody who works a lot of overtime.

We're going through there to understand even of those who didn't approve, what the residual risk still left is over there. We're pleased with our progress on that. We think we'll have more progress to go through with Michael MacPhee and team that I keep looking down at this year as we go through it.

Then on the sick time, there's a bit of an industry standard of around 4 per cent for your sick time, so any time something comes up greater than 4 per cent, it gets flagged through HR with the manager to say this situation is greater than 4 per cent. Then they look at it on an individual basis. Just given the subject matter there, we are okay with providing more latitude there. Again, just because there's a risk doesn't mean that you need to go extreme on it. So we do look at it case by case as the sick time things come up to make sure that it's okay.

Those are the two examples that I would say: the time reporting, and within the time reporting, the overtime and the sick time.

TIM HALMAN: Thank you very much for that response. I appreciate you taking the time going over the components of that framework.

We all know in point of fact by October of 2019, when the financial report comes out from the Auditor General, that the cybersecurity risk management program continues to evolve. That's the conclusion. We know even before 2019, risk management and cybersecurity is paramount as a priority to Nova Scotians.

You've outlined what components need to fall into place to ensure we're prioritizing this - whether it's the culture at the top, tone at the top. I'd like you to provide us a history lesson. What were the factors that led to this financial report concluding that there's still a lot of work that needs to be done? Perhaps what is being done differently now? If you could provide us that history lesson, I think that's critical.

DEREK SPINNEY: That would be great. In the case of our internal controls, maybe I'll take two stabs at that: both the cybersecurity piece, which has a shorter history, and then internal controls, which has the longer history.

In the case of internal controls, we became an organization in 2015. Again, we brought together the nine health authorities, trying to figure out how we can do this from a people-process-technology point of view to create the value that was envisioned at the time that took place. In doing so, as you can appreciate, all of those existing controls started to collide into one group.

We used the framework that we've been through to ask, okay, how can we actually structure this? The whole process is a journey, although some parts can go in parallel. You can also think of it as a chronological journey, in that the first thing is that you kind of start with your control environment, and from there you say, okay, what are the different risks in the organization, what controls am I going to put in place, how can I communicate this, and then how do I monitor it?

The communication and the monitoring, those two things in particular are kind of at the tail end of that process. Until you actually have something, you've identified your risks, you've evaluated what was inherent, what is residual after you put the controls in, you're not sure what to communicate and you're certainly not sure what to monitor.

Not to speak for the AG's Office, but part of what they've concluded is that our internal control environment is incomplete. By incomplete I would expand that to say in particular on the tail end of that chronological process, in that we have gone through the first three, and in my words, not theirs, I think we did that quite well, and the last two are the areas that we're really working on.

We've done a couple of things with that. One of them is, again, we engaged outside assistance to look at our current state, look at where we need to be, and then to give us that road map on the very specific steps. One of the things that we want to make sure of, and we've got a register of the steps, is what the specific steps are that we're going to take in order to get to that end piece.

Around the information and the communication, for instance, a very tangible example that we're using in relation to fraud which is today's topic, is the fact that the AG pointed out in the report that mandatory fraud training was not taking place everywhere. We were one of those organizations. By the end of 2020, so by the end of December 2020, in the last couple of months here, we will have in our LMS - our learning management system - mandatory fraud training. The materials have been put together, we've been through it, we're just waiting to launch the site, if you will. There will be that mandatory training.

Another thing that we're doing, even with our finance and audit committee, is in November there will be a half-day session where again we're bringing in outside help to help educate even our own board members, our finance and audit committee members, what is a good internal control environment? What's the benchmark? They're tasked with governance to make sure that we achieve that.

We want to make sure that they understand what that benchmark looks like, and then understand where we are so they can get very specific and understand the AG's observations and say, where do we have yet to go on that?

Around the monitoring aspect, what we're doing is documenting and having evidence recorded. We use SAP as our ERP system, there's a governance risk and compliance module, and it allows you to store documentation and these sorts of things. That's for when the AG is auditing us and they ask, how do we have proof that you did monitor that, if you will, the documentation is actually available. That's a bit of the history lesson on the internal controls.

On the cybersecurity, as Dr. Carr pointed out, it has been more recent, I guess I could phrase it that way. The different risks that are coming forward and who's actually responsible for it. In 2016 the Province would have initiated and hired a CIO, and part of their role was to set up a cyber risk program. They did that. Two years before that was the shared services legislation in 2014, and it was envisioned in there that further clarity would be given to the government entities on who is responsible for what and who would get what service from whom.

In 2014, shared services; in 2016, the CIO came in; and then between 2016 and now, people have really been trying to create those delineations, if I could say it that way. What we've done in particular is engage another outside firm and their report is almost final - I've been through it with Andrew, and it's final by the end of this month. We'll go through it with our finance and audit committee, that again outlines what in particular our policy should say. As Dr. Carr pointed out, we agreed with the Auditor General's statement that we are responsible for our clinical applications and its data, so what is our policy and what is the framework that we're going to put around that.

The National Institute of Standards and Technology actually has a framework that I won't go into around that as well, but suffice it to say that there is some guidance. What we're provided there is an industry standard, and the outside consultant has gone through that and really helped us focus on what specifically should be our role, what is the necessary governance structure, and then also a bit of a road map to get from where we are today to where we need to be.

Although we do share services from NSDS, there are some things that are more specifically ours than theirs. Strategy, governance, compliance - those first three things are really coming out to say that's really what is more owned with us, but the performance

management and the operations of that - it is recognized that we have a heavier reliance on NSDS because sometimes they're the experts in some of these particular things that we rely on.

That needs to be documented and agreed upon and written down. That's kind of the journey that we've taken on in cybersecurity.

[9:30 a.m.]

TIM HALMAN: I appreciate that. With respect to examples, where we're hearing through the media about cybersecurity breaches. I have three articles in front of me here from the CBC: two from Jack Julien, one from Yvonne Colbert. The one from Yvonne Colbert outlines, "N.S. government acknowledges system failed to protect privacy of 10,000 people." That's related to workers' compensation; the other two are related to health care privacy breaches.

One of the individuals who had a privacy breach said the following: "I wanted to speak out just to let people know that this is something that is happening. There were almost 60 people involved in this particular breach . . . and I don't see any changes being made . . . There's no internal policies that have changed or procedures that may protect somebody else in this situation."

What would you say to this individual? Why does there seem to be a discrepancy between what you've outlined in terms of the improvements NSHA is making in terms of what we're hearing from Nova Scotians?

DEREK SPINNEY: I'm going to get Mr. Nemirovsky to help me with the particulars of the example that he may wish to go through. I think some of that, just to intro that, is really around progress. They are points in time as we go through it. "We can't be good enough" is really kind of our mantra, and we recognize that we have work to do, absolutely, and I don't know that we'll ever get there, if you will. I don't know that you can get there because it is so important to us and to Nova Scotians, but there certainly is progress that is under way, and improvements.

As you indicate, there are certainly examples where we as a province, I'll call it that way, is certainly susceptible and some things have happened. But there's also literally thousands of examples that don't make the news that take place every day that are adequately defended against, for instance. Andrew?

THE CHAIR: Mr. Nemirovsky.

ANDREW NEMIROVSKY: To dig into that one a little bit, the staff who are essentially breaching patient information - a lot of that actually isn't related to cybersecurity per se. It's more a control piece around access, auditing - and that's actually

where Ms. Hornberger's team comes in, because the privacy office actually looks after a lot of that policy work.

I'll let her speak to the updates because there have been a few, but it's really not a cybersecurity threat because we look at cybersecurity more as an external threat coming in as opposed to an internal, where it's a staff member accessing stuff inappropriately. Karen?

THE CHAIR: Ms. Hornberger, can you try to get it in in about 20 seconds?

KAREN HORNBERGER: Some of the audits with those articles by Mr. Julien - the breaches that happened this summer were found as a result of improved auditing. I can't speak to specific cases. I'm familiar with both of the cases that were reported on this summer and the case that that person in the article is quoting, but I'm unable to speak to the specifics because of privacy reasons.

Some of the improvements we've made in our auditing led us to discover the breaches that were reported this summer, where there were some 211 people notified because we did improve our auditing process.

THE CHAIR: The time for the PC caucus for the first round is up. We'll move now to the NDP caucus. Ms. Roberts.

LISA ROBERTS: Thank you all very much for your work and for being here. I have about 20 minutes, and right now the answers are running about eight minutes. I'd like to get through a few more questions, so I'm going to try to ask a couple of quick snappers.

One is, has the NSHA implemented a fraud risk hotline?

DEREK SPINNEY: The short answer is yes, but if I can elaborate just a little bit. In March of this year, Dr. Carr actually announced the organization's latest whistleblower policy, so there is a policy. That really brought together existing policies again into that one new Nova Scotia Health Authority one. There are two aspects of that whistleblower policy. There's an email address that people can use and there's also a 1-800 number. Yes, it is implemented and up and running.

LISA ROBERTS: That's good to hear. I guess I'd invite either Dr. Carr or someone else to comment as you see fit. It strikes me that in such a large organization with such a large budget, the risk is not just of fraud with cash or time, but also effort. How are we ensuring that the effort that we collectively as Nova Scotians are paying for is actually serving the best health outcomes for Nova Scotia?

Is there a way in which information and observations about that can actually get from the front lines like administrative staff up to the leadership in a way that helps to shape the organization?

BRENDAN CARR: While we might not consider waste or inefficiency as fraud, in an organization such as ours where, as Mr. Spinney said, 70 per cent of our costs relate to people and people doing work, having an awareness around what we're achieving with the efforts that people are putting in is equally paramount if not more paramount.

I would say that every organization in the country is constantly trying to figure out how, with the resources they have, they can deliver the best value for citizens. That value comes both in terms of the quality of health outcomes and, increasingly, our ability to create healthy environments that prevent illness and our ability just to support people in their health every day.

Just like the conversation around privacy and cybersecurity and information security, when we talk about the tone at the top, I think what's critical is that we establish a culture in the organization that is extremely mindful of the concept you're talking about. That's indeed exactly what we're trying to do.

My response to the how or what have we done differently is our first job is to create a leadership culture in the organization that recognizes the stewardship role that we have and the accountability that we have. Not just to be making sure that people are working the hours that they're booking, but to make sure that their effort is actually delivering some value for Nova Scotians.

I think from a culture point of view, it's critical but then we have to follow that with specific consequences as it pertains to fraud - and development for our staff and our teams such as how they can ensure that they're delivering the best value. I think it's a very important concept.

LISA ROBERTS: Briefly turning to cybersecurity, what privacy considerations were weighed when developing the COVID-19 testing strategy? I think, as many people, I was struck that I actually got my results for the one time I went for a COVID-19 test sent to my Gmail account. I was super happy with that. It was negative.

Clearly, there must have been some deliberation and maybe that can help illustrate the progress that has been made since this audit in October of last year. Again, briefly, if possible.

ANDREW NEMIROVSKY: My team was tasked with developing that negative result email process. One of the key activities that we undertake when we're developing any new software process is a privacy impact assessment in conjunction with the privacy office.

We also do something called a threat risk assessment. What that does is looks at ways that the system could be infiltrated from an external bad actor, as we call them, or the data could be found somewhere else, or the underlying architecture or servers could be

hacked. All that was reviewed by a third party in addition to the privacy impact assessment to make sure the data was safe. It was also vetted by the Department of Health and Wellness.

LISA ROBERTS: I assume that here at this committee, I am looking at the heads of the cybersecurity governance structure that was identified as missing in October 2019. Can I make that clear?

ANDREW NEMIROVSKY: I'm going to say a kind of yes. It is a work in progress. That is the work in front of us. It is really to define who needs to be there, what their roles and responsibilities are and how that rolls up to Dr. Carr and to our partners at both Nova Scotia Digital Services and the Department of Health and Wellness.

LISA ROBERTS: We have not met very many times in the last eight months. We haven't actually had the opportunity to ask any questions related to health care since 2018, I think. There is an outstanding recommendation from a 2017 audit that was mentioned in the May 2020 follow-up audit related to home care complaints. I'm wondering, Dr. Carr, if you might be able to address that because we just haven't had an opportunity to ask about that.

In 2017, the Auditor General raised a number of concerns around home care contracts and contract management evaluation of service provider performance. Specifically, there was a recommendation that there should be an integrated record of home support complaints received. That was a recommendation to the Department of Health and Wellness and to the Nova Scotia Health Authority. Anecdotally, we have heard of widespread challenges in home care during COVID and we know that, in fact, the workforce issues that affect long-term care are also very interrelated with the labour force issues in home care.

I'm wondering if you can share with me why that recommendation - at least as of May 2020 - has not been completed, and what the consequences of that are in this particular moment of challenge during COVID.

BRENDAN CARR: Great question. I'm not familiar with that specific recommendation. Although I have reviewed the Auditor General's previous reports, that one eluded me.

As you indicated, the health care environment is a little bit complicated in Nova Scotia where home care and long-term care are largely under the jurisdiction of the Department of Health and Wellness. It means in terms of managing the day-to-day relationships with home care providers, et cetera, it would generally be our colleagues at the Department of Health and Wellness who would be interacting with those providers.

That being said, from the point of view of the average citizen in Nova Scotia, we think like a system and I think I would agree with what I think is the spirit of your comment, which is it matters to people just as much in their experience in home care as in the hospital system.

I can't speak to where we are vis-à-vis that specific recommendation and how we're advancing that, but I would agree, though, that one of the things that we're learning through COVID is that it is emphasizing the fact that our ability to effectively - with good quality and reliably - provide support to people in their homes is critical to a high-functioning health system. It is an area that was recently underscored in a report that was done in the long-term care sector and I think that there is a general commitment on the part of the Department of Health and Wellness and the Nova Scotia Health Authority to work collaboratively to try to improve this.

LISA ROBERTS: I'll have to review that report again from November 2017 to understand exactly why that recommendation is joint to the NSHA and to the Department of Health and Wellness, but I'm glad to have at least brought your attention back to it.

I'm going to return then to the October 2019 report. The AG Report identified five significant control weaknesses. Is there specific progress that you haven't spoken to in terms of capital asset additions that you'd like to share with us in terms of the progress that has been made?

[9:45 a.m.]

DEREK SPINNEY: The five that you mentioned - I touched on two already. One was the time reporting. One was the internal control environment being incomplete, where we talked about the tail end of that chronological process being completed now. The other three were capital-related, as you pointed out. Those three are no longer, in our last audit, significant deficiencies, so the AG auditors have downgraded that, if you will.

There's still a note - a weakness identified there. The three aspects around it - even though we've done a lot of work with them and it has now been downgraded - the three things in particular are that we don't currently have a system to monitor our capital assets, like a computerized system, if you will.

The risk there is - and Brendan would have used some of this in his opening - a computerized tomography scanner, for instance. When you're trying to figure out your controls, you figure out what's the risk. So what's the risk that a CT scanner is going to disappear? The risk would be lower, obviously, than if it were an ultrasound, which is a much smaller box that somebody could actually get into a van and it could disappear.

A system would help track the physical location of where all of those things are. That is really a function of where we've come from and we simply don't have a

computerized system to do that. That said, what we have implemented this year - and we'll be going through with Mr. MacPhee's team later as he commences the audit this year - is not a computerized system but a process that people are running that we interact with all of the cost centre owners of the equipment, so that we do know what is where.

The second part was around impairment: What our regular review process is to ensure that, if an item is to be impaired, that you are in fact doing that - reducing the amount that you've got on your balance sheet for it.

The third one is around disposal. If you've disposed of an asset, it should be taken off your balance sheet. What is our process to ensure that when an item is disposed that accounting knows so that it can come off our balance sheet? Again, there is this process that we'll be going through with the AG this year. It's not through a computerized system yet, although we are looking at that as well, but at least a process where we can say we've engaged the owners - if I can call them that - of the equipment and the assets. We engage with them to understand: should it be impaired, has it been disposed of, what is the current state?

If you were to look at our balance sheet from our financial statements, you'd see that we have about $1 billion in assets, and about $141 million of that is medical equipment. Most of the rest is really buildings. It's a lot easier to deal with that. That just kind of gives you a sense as to what are we talking about here in the capital piece. That's $1 billion, $141 million is medical equipment, and that is a large part of what we're focusing on with this process to ensure we know what is where, what is its current state, and should it be removed from the balance sheet.

LISA ROBERTS: I'd like to pick up on some of the comments around controls around time reporting, and particularly your comments about sick time. Of course, COVID must have thrown all previous benchmarks for what is typical sick time right off the rails for many different reasons, including for a parent who lost child care, for parents who now have children back in school and are, like all parents, whether they're in the health care system or not, encountering delays related to testing for their kids if they have the sniffles. How are you maintaining controls while recognizing the circumstances that we're all facing?

DEREK SPINNEY: It's a great question. I think I'm proud of this as a Nova Scotian, but it depends on your perspective, I suppose. I'll start with vacation time and then we'll get into sick time, which I won't be able to be as specific about with the numbers.

With our vacation time this year, our fiscal year starts April 1st of course, and really that's kind of when we were knee-deep into it with COVID. Between April 1st and the end of September, we've seen a very large reduction in vacation time that has actually been taken. So kind of like when a fire is on, a firefighter runs into the building while

everybody's running out - well, the Nova Scotia Health Authority actually ran into COVID while many people were thankfully able to stay the blazes home, if you will.

For us, it is something that we're very much monitoring, and in fact one of our very large planning focuses is around the human resource that we have, because that is so dependent. In fact it's the most dependent variable that we have in our planning right now for the second wave and all of these things. We're very carefully monitoring who is taking vacation. Although we are proud, at the same time we completely understand that there needs to be a work-life balance, so we're trying to follow up with people to ensure that they are getting the time that they need and the supports that they need as well.

In sick time, I don't have the number to quote. I believe that it's actually down as well. Intuitively, I would have expected it to go up, and in fact it's actually gone down during COVID time. I'm purely speculating at this point, but my own personal speculation is that it's for the same reason. People just feel the ownership that we need to be here for Nova Scotians. That's kind of been our experience so far.

LISA ROBERTS: Maybe I will ask Dr. Carr if he'd like to comment on that, because I'm trying to read facial signals from behind a mask, which is challenging.

BRENDAN CARR: First of all, I think your question's a very important question for us. Let me come at it in a little bit of a different direction.

Like everybody in Nova Scotia, COVID has created unprecedented strains and stresses on us in terms of our professional life and our home lives and our community lives, and all of our staff live that every day in their personal lives and have the added responsibility of trying to keep the health system running every day and doing what they do for Nova Scotians. We know that our teams are highly committed and that they have a great sense of privilege in the work that they do and a great sense of purpose in serving the people of Nova Scotia.

They sometimes do that to the point of self-harm, quite frankly. We have people who have not been able to take vacation, or we've probably had people - not somebody with symptoms of COVID, but other people who may in fact be coming to work every day when they would have maybe normally had a normal doctor's appointment or something like that, and they're committed to coming to work because our front-line teams need to be present. At the same time, they've been the people that have been standing up our testing sites and our assessment centres, they've been in the last number of months trying not just to continue or reintroduce services, but to catch up on people who have been lost.

They are working extremely hard, they deserve all of our acknowledgement, and I think it's borne out in the statistics that they do that with a tremendous sense of commitment to the people of Nova Scotia.

THE CHAIR: Ms. Roberts, 18 seconds.

LISA ROBERTS: Again, thanks very much, and I know that my colleague will have more questions after the Liberal caucus.

THE CHAIR: Now we'll move on to the Liberal caucus for 20 minutes. We'll start off with Ms. DiCostanzo.

RAFAH DICOSTANZO: Thank you for all the information. It's been a wonderful understanding, a lot of it. In the Auditor General's Report, they referenced clinical and non-clinical programs. Could you just expand on that and let us know what the difference is and how it affects maybe the staff as well?

ANDREW NEMIROVSKY: To delineate the two, we take a clinical system as one that's being more patient-facing, something where we enter lab information, results, documentation, X-rays. That would classify as a clinical system.

The non-clinical systems would be things that support business process like Systems Applications and Products in data processing, a time-tracking system - those are the kinds of things - Microsoft suite of products. Those would all be non-clinical. That's how we delineate the two. Sometimes it's grey, because some systems cross the border, but we try to use those as our metric.

RAFAH DICOSTANZO: Which one takes more of your effort in regard to cyber attacks? Where do you concentrate your efforts?

ANDREW NEMIROVSKY: They're split pretty evenly. Cyber criminals look at health care overall. They don't sort of delineate between clinical versus non-clinical. They look for any opportunity to get into the system to wreak havoc. Their favourite mode of entry is email, so that's the one we spend a lot of time working on - me, my team, the privacy office under Karen Hornberger and Scotia Digital - spend an inordinate amount of time monitoring and mitigating email risks.

RAFAH DICOSTANZO: That brings me to another question in regard to passwords. Is there a way that passwords are more complicated than my passwords, for example? I find it really difficult to remember them all and where I put them. How do you manage that within the health system?

ANDREW NEMIROVSKY: At this point, we have done a lot of work around passwords. It was a finding in one of the recent audits that we need to do some work on that. My team has been looking at passwords across the organization - both clinical and non-clinical - doing an assessment of what the complexity is that's required in the systems, what the current provincial standard is, and working to bring our systems up to that standard, if possible.

Some of the issues that we run into is that many of our systems are fairly old and, as such, don't actually support the standard. We're working on the ones that are especially tied closely to the financial systems to make sure that they have the most security, and the ones that have patient data.

Again, we are bound by the limitations of the software, but we are actively working to bring all of those up to at least that provincial standard, and there is work afoot at a provincial level to modify that standard. It has been delayed due to other work with the province at Nova Scotia Digital Service. We're waiting for that new standard to come and then we will re-evaluate where we are, but we are actively working to bring things up to that level.

RAFAH DICOSTANZO: You said the new standards or the standards that you're hoping for. Where are we in comparison to other provinces? Where will that bring us once you have those standards?

ANDREW NEMIROVSKY: I don't actually have the answer to that question because we don't know what the new standard looks like as being set out by Nova Scotia Digital Service, and Service Nova Scotia and Internal Services. We are kind of waiting for them to give us the standard and we'll work towards it. They would probably be best to comment on where that is in terms of relation to other jurisdictions.

RAFAH DICOSTANZO: One last question and then I'll pass it on to my colleague. There was also the reference for networks and clouds, the locations of them. What are you using and if you can explain to somebody like me, why would you use a cloud over network?

ANDREW NEMIROVSKY: The term "cloud" gets thrown around a lot. All it really is, is a data centre run and managed by someone else. The Microsoft Azure Cloud is just a number of data centres scattered around the world. In Canada, I believe there are three from Microsoft that we call the cloud. It is just a very fancy, relatively easy-to-use set of servers and networking equipment that we as consumers can access.

We have our own data centre as well - a number of them actually - in the province, run by Nova Scotia Digital Service. That is where 99-plus per cent of our data and applications are stored. There is a shift happening to more cloud-based software. That's because that's where the vendors are headed. A lot of them are moving to cloud-based solutions. It does allow for less complexity from a technology perspective that we need to manage here in the province because we give that technical work to that vendor, and then we actually just manage the software that's on the server.

It actually makes the work simpler from a technical perspective. We're not there yet. There is work afoot to make sure they're secure. That is being done in conjunction

with Nova Scotia Digital Service to make sure they have appropriate firewalls and anti-virus and that we're comfortable putting patient data or applications up there.

[10:00 a.m.]

RAFAH DICOSTANZO: One last one. Now with COVID-19 and people working from home, how did you manage that to keep out cyber attacks while people are working from home?

ANDREW NEMIROVSKY: We did a number of things to facilitate people working from home. A lot of physical devices that we had on site, we actually sent home securely with staff because they're fully encrypted; they have an encrypted connection back to the hospital system. That was one way we did it.

The other way was through something called virtual desktops. We, in conjunction with Nova Scotia Digital Service, set up an expanded pool of virtual desktops. What that allows someone to do is work from home, log into a secure site with their secure login and password, and it will encrypt everything on that connection while giving them access to all the clinical applications that they'll need, even though they're home.

It facilitated physicians, nurse practitioners, and others to continue to be able to see patients remotely right from their home. Everything was done in the computer information system and it was all on secure connections. It helped them maintain as much service as possible in what was a very trying time for everyone.

THE CHAIR: We'll move on now to Ms. Lohnes-Croft.

HON. SUZANNE LOHNES-CROFT: It's interesting to hear some of these updates. I'd like to get some information on the proposed One Person One Record. We've heard a lot of buildup for it and there seems to be excitement, especially with the amalgamation of all the different health districts that are now one. Where are we in the timeline and, as part of that, I'd like to know where the risk management has fit in or where it's fitting in?

BRENDAN CARR: In terms of the timeline or the process around One Person One Record, essentially we are at the end of the procurement phase. From a procurement point of view where, over the last number of months and years, in fact, there has been work done around identifying vendors who could meet the needs that have been articulated around this clinical information system.

That process is working through government. I understand that it is nearing its completion, having evaluated various vendors, looked at the total cost of ownership, looked at those kinds of issues. That process will lead to a decision by Treasury Board and Cabinet within the near future, notionally.

On the health system side, while we've contributed to the specifications around the system from the point of view of what it is that we're trying to achieve here, why it is important, and what a system like this would need to do or to help us with, a lot of the work that has been going on within the health system has been around what we call readiness work. It's looking at how the conditions can be created in our organization and what kind of work we could do on the front end of this to really streamline and to flatten the change curve for people as we're heading into implementation. Should we move in that direction?

From a timeline point of view, we've done a lot of front end work around understanding what the needs of the system would be, identifying potential vendors, and working through a process around the total cost for this. We're at the penultimate point where that would be a decision made by government. The work that we're doing to ready the system has been largely around implementing a system like this.

ANDREW NEMIROVSKY: You're going to have to repeat that for me - the second part.

SUZANNE LOHNES-CROFT: I wanted to know about the risk management, where the process is during this and what do you hope to have in place?

ANDREW NEMIROVSKY: Throughout the procurement, we've engaged an independent vendor to assist a third party by advising on all those risks around procurement, around the system, and about how it's going to be implemented. There will be more work that happens once we identify who that vendor is, if one ultimately gets approved by Treasury Board.

There's not much we can really talk about until we know who that is. Depending on how they implement and what the actual approved schedule looks like, that will speak to those risks and allow us to mitigate more as we understand exactly how we're going to roll out what modules are going to come, what processes will change, but we really need that vendor name so that we can start to do a lot of that assessment with them because it will be very much a partnership.

SUZANNE LOHNES-CROFT: Do you have any goals in your mind that you would like to see put in place with risk management?

ANDREW NEMIROVSKY: I think one of the biggest goals of the One Person One Record program is to make sure that clinicians have access to the patient information they need to provide the best possible care. From a risk perspective, that's one of the ones we're looking to mitigate - the risk of not having the right information at the right time to provide care.

As I'm sure you're aware, we have a disparate number of systems across the organization - all from the different DHAs and whatnot - where physicians and clinicians

need to go to multiple systems to get the information. OPOR by itself is a risk mitigation in and of itself because it allows that consolidation of that information to one single source.

There are risks in implementing any software program, but again, that's why that vendor needs to be on board, so we can work with them to identify those - make sure we have the right plans in place as we look to roll that out. But it really is somewhat vendor-dependent, because the risks change.

SUZANNE LOHNES-CROFT: Are you working on a communications plan to educate the public on how you're going to protect their information. Is that in the works?

ANDREW NEMIROVSKY: I don't know that the OPOR program changes our perspective on patient data safety or how we safeguard it. It's just a different piece of software. As we've talked, the Privacy Office under Mrs. Hornberger have done a lot of work around policy changes to make sure we're keeping patient data safe. We manage patient data on a day-to-day basis. My department also houses the health information department, so we are always making sure we have patient data stored appropriately. We control access to it. That doesn't change with OPOR. It's just a different tool to help us manage that patient information. We already have a lot of that in hand.

BRENDAN CARR: I'd like to add to my colleague's response. On the question of risks, I guess I'd like to look at that from another perspective. There certainly are risks that we're very aware of in terms of the risks associated with a significant change initiative in a large, complex organization. We have an extensive governance structure that's been designed around those risks that includes all of our partners that we've talked about. That includes the Department of Health and Wellness, Nova Scotia Digital Service and our board.

There are also some risks. We're aware of many risks, but there are also some very tangible risks that we're trying to address with the One Person One Record system. Those are largely risks around inconsistencies and information that support or don't support good clinical decision making.

The third leading cause of mortality in Canada, in North America and the world is really system-related error. Sometimes we refer to it as medical error, but it's not a physician's error - it's the system. When you think about the complexity of our system, there are many risks inherent in our system, particularly with medication management and things like that. These systems are very specifically intended to reduce those kinds of risks that translate into fewer deaths and less harm to patients every day.

When you ask a question around risks, there are risks around the implementation of this, but there is also - what are the risks that we're trying to improve? Those are largely patient safety and quality risks where there are tangible opportunities for benefit.

In terms of the environment with our citizens and members of our community, absolutely this will constitute a significant shift and it will be something that will change the way that people interact with their own health information and the way that their providers are interacting with health information. We've started to, but we've been in this readiness phase.

As we would move into implementation, we would absolutely contemplate a very active process by which we would be engaging with our communities and with citizens, both to make them aware of what's coming, but also to seek their input. It's really important that they understand not just what we're doing, but why we're doing it - why this is important for them - because o matter how we do it, this will be disruptive in our system for a period of time.

It's important that people understand why it is that we're doing this in terms of the benefits that we expect to realize certainly from a quality point of view, a safety point of view, quality of data and the ability of that data to support individuals in managing their own care and decision making in health care going forward.

SUZANNE LOHNES-CROFT: Dr. Carr, you mentioned about the handling, the fraud-risk management being put in for large sums of money, our foundations and all our regions have them, and even some are within regions. I know I represent Lunenburg, and the South Shore Regional has their foundation, but there's a little Fishermen's Memorial Hospital Foundation as well.

How are you looking at risk management with all these different, you know, they all have their own treasurers and committees and whatnot, yet we're one health authority. How are you managing that risk? There are large sums of money, millions of dollars in these accounts, and there's a big procurement piece with that, and I'd just like to hear how that's being handled now.

BRENDAN CARR: I think Mr. Spinney might have something to add to this. Just to acknowledge that is a material concern and issue that we are talking about large sums of money, and they are citizens' donations to support health care, so this is important.

Under the auspices of our board, we engage with all of our foundations. Both Mr. Spinney and another one of our vice-presidents have managed our direct relationships with our foundation partners on issues like how we safeguard those resources, how we ensure that we are accounting for these resources in a way that is consistent with generally accepted principles, et cetera. Those are all matters that we deal with on an ongoing basis with our foundations.

I feel that it is kind of an extension of the work that we do that is important. I don't know, Derek, if you wanted to comment.

DEREK SPINNEY: I saw a stat one time that 500,000 Nova Scotians have donated to a foundation. That speaks volumes to the engagement that we have in this province and how important it is in all the different communities. They know best their local environment and what is needed and how they're bringing that together for us. It's over $10 million a year that they would actually contribute for medical equipment specifically, for instance.

We do have a dual partnership as Brendan just mentioned, myself and our Vice-President of Research and Innovation, who meet with the foundations to ensure that they have that one-on-one contact, that they understand what we see as the future needs in the different areas and that they're actually able to speak into that so that we can have this two-way dialogue.

I also meet on a regular basis with Stephen Harding, and not only does he chair the Dartmouth General Hospital Foundation, but he also chairs the association of foundations across the province. Just two weeks ago actually, while I was over there, what we were talking about in the cafeteria was around payroll for the foundations. We, Nova Scotia Health Authority, have brought forward to him an opportunity that he's taking back to his organizations around a shared service for payroll and those sorts of things.

As you said, the level of sophistication in the foundations can be very different, if you're one of the larger ones in HRM versus the South Shore or Soldiers Memorial. We're encouraging and providing options, but really as an interested partner, because it is also very important to understand that we are completely distinct organizations. We are legally distinct, we have separate bank accounts, we have separate policies, these sorts of things.

That delineation is very important, that we're able to keep that. They have their own boards that are responsible for their stewardship and governance, but we work very closely with them to ensure that even, for instance, if a foundation was to say, we'd like to raise $1 million to contribute towards something, if we enter into an arrangement with them and say, okay, let's go do that, that's a great thing, let's do that together.

We encourage feasibility studies through the different foundations so that they are not biting off more than they can chew, if you will - to put it that way - and a bit of a payment schedule so that we can actually understand that this is a viable thing.

This isn't out of a place of mistrust; in fact, it's the opposite. We need the partnership to be very productive for everybody. We want it to be successful so we do spend a lot of time mentoring, if I can put it that way, but not being directly responsible at the same time.

THE CHAIR: The time for the Liberal caucus has expired at this point. We'll take a 15-minute break. We'll come back to our seats around 10:31 a.m. and we'll do the second

round and we'll have the division of time after that. We're back here at 10:31 a.m. Thank you.

[10:15 a.m. The committee recessed.]

[10:31 a.m. The committee reconvened.]

THE CHAIR: Order, please. We'll call the committee back to order and we'll begin the second round of questioning of the witnesses. This second round will be eight minutes per caucus. We'll start off with Mr. Halman.

TIM HALMAN: We've certainly established that cybersecurity is paramount to Nova Scotians as a concern. One thing I've noted in my three years as an MLA is how large the Nova Scotia Health Authority is and with respect to that, I think it's fair to conclude that information sharing is a critical success factor in improving health care delivery.

To that end, is there a plan to report to Nova Scotians on the progress to demonstrate accountability and transparency for the implementation plan that you've outlined here today?

ANDREW NEMIROVSKY: I just want to clarify: implementation plan for . . .?

TIM HALMAN: As it relates to cybersecurity. You've outlined a framework that you're working with. I've cited a couple of examples where there have been breaches. I believe Nova Scotians want a progress report. Will you commit to a progress report in the name of accountability and transparency?

ANDREW NEMIROVSKY: I don't know that I can commit to one personally. That would be a discussion with Derek and me. I can commit absolutely to doing the work to make sure we have a framework that does support the safety and security of patients' information and our systems.

As we've said, that work is almost to completion in terms of the initial assessment with that third party vendor coming in to make the recommendations that we then need to take back up through internal governance that has us, Nova Scotia Digital Service, and the Department of Health and Wellness at the table to make sure that we're all in alignment with that plan moving forward. It's going to require resources from all three organizations to make a robust cybersecurity framework a reality. It's not just us. We need to work with those two partners because we're so closely linked.

DEREK SPINNEY: Just to add to what Andrew was saying there, as well: our stop along the way is to our Finance and Audit Committee. That helps us with the governance to ensure that they agree with the progress and the steps. Then progress updates, I think,

are quite reasonable. In fact, that is what we're doing here today through the Public Accounts Committee, and the Auditor General helps very well with that, in fact, with their reports and the performance audits and their engagement. I can certainly take back to see if there's something that we can do more proactively as well. We're certainly open to that idea, for sure. As you outlined it, it is very important.

TIM HALMAN: What we've all learned during the COVID experience is that timely, consistent updates are critical. To that end, if cybersecurity fraud risk management is paramount, let's see those actions and behaviour that align with rhetoric such as that.

To that point, even my understanding - this summer in Eastern Passage at the Ocean View Continuing Care Centre, the computer systems were shut down for three weeks. Why were those computer systems shut down?

ANDREW NEMIROVSKY: I'm not actually familiar with Ocean View. I don't know that it's an actual NSHA-run site. It definitely doesn't fall under my portfolio, so I'm thinking they're independent. Can you speak to it?

BRENDAN CARR: I think Ocean View is a large long-term care facility on the Eastern Shore. They're not part of the Nova Scotia Health Authority family, as it were, and so it would be difficult for us to speak specifically to anything that happened with respect to their information systems at any point in time.

TIM HALMAN: I'll use it as an example to illustrate how critical it is to give updates, to let Nova Scotians know what is going on, to be up front as to the nature of these breaches, to be up front what plan is going to be put into place to ensure mitigation of these incidents.

Of course, this being the Public Accounts Committee, I'm curious if there is an understanding of what level of investment is required to achieve the framework you've laid out here today. Do you have a projected expenditure that you can divulge to Nova Scotians?

ANDREW NEMIROVSKY: At this point, we don't know the full cost. As I said, the report is preliminary at this point. There are some very high-level recommendations that are going to come out of it. The reason I don't really know is because so much of the work is going to be done in conjunction with Nova Scotia Digital Service and they have a significant piece to play and I need to factor in their costs, if the recommendation is endorsed by the governance committee. We need to take it there first to get the finance and audit committee of the board to also sign off.

There is still more work to do to flesh out what's reasonable. It's probably going to require a reconfiguration on both our side and Nova Scotia Digital Service to make these recommendations a reality, so there's still more work to do to determine what those full costs are.

TIM HALMAN: What is the established time frame to arrive at those projected numbers?

ANDREW NEMIROVSKY: Our report should be back in the next three weeks. That's the date we have from our group that we're working with. That is just the Nova Scotia Health Authority portion. We then need to work with our partners at Nova Scotia Digital to determine what else they need. I don't know what their timeline is. I know they're actively reviewing their program, but I can't comment on their timeline and when they're going to have a final suggestion put forward.

TIM HALMAN: Because cybersecurity fraud risk management is of paramount importance to Nova Scotians, will you commit to divulging that estimated cost to arrive at this framework for Nova Scotians? When will we know the numbers?

ANDREW NEMIROVSKY: Ours will work with the board. I think that's probably a reasonable thing to share, but it is a portion of a larger program that needs to be put in place. It would be couched with that caveat, but I think we can probably share what our recommendation will be.

TIM HALMAN: With respect to the Information and Privacy Commissioner's report of 2018, she highlighted issues pertaining to time limits for prosecution. Two years is the typical time for other provincial offences. Will the Personal Health Information Act be amended to lengthen the timelines for prosecution under this Act for a breach? Are you looking at that in terms of deterrence and consequences?

KAREN HORNBERGER: I believe that will be the responsibility of the Department of Health and Wellness. They are undergoing a three-year review of the Personal Health Information Act. I can't speak specifically as to whether or not that's something they're looking at changing. That would be a question for that group.

THE CHAIR: The time for the PC caucus has expired. We'll now go to the NDP caucus - Ms. Leblanc.

SUSAN LEBLANC: Thank you for this discussion so far. I just want to ask a couple of quick questions about the AG Report. We were happy to see that the audit policy around assessing personal health information was created since the AG Report last October.

I'm wondering if you can talk quickly about an internal evaluation plan that would be put in place for the audit policy. Basically, how will we all know if the efforts to create a privacy-conscious environment are working internally?

KAREN HORNBERGER: We do track our privacy breach numbers. The numbers reported for day-to-day breaches are much lower. Part of that is because of the reduction

in service due to COVID, but I think some of it is as an effect of our education to our staff members.

As far as the auditing goes, we're still working on our implementation of our annual auditing policy and looking to improve the types of audits we do on a regular basis, and as part of our operational plane, we are looking at measuring how many audits are completed on a quarterly basis and report that up through to our vice-president.

SUSAN LEBLANC: I apologize if this was asked before. I just want to clarify, though I feel like maybe it was. In the AG report of 2019, it was noted that fraud training is not available to all NSHA employees. Have you addressed that? Is it now available for all employees?

DEREK SPINNEY: It will be by the end of December 2020, this calendar year. It wasn't at the time of that report, absolutely, and thanks to the support of the AG's office and the method that they used to bring that forward, we have in fact agreed to that and it will be rolled out. The content is done. The website's just kind of waiting to be turned on.

SUSAN LEBLANC: Again, my colleague commented that we haven't seen anyone from Nova Scotia Health Authority for many months, and so I just wanted to ask a couple more questions related to the current pandemic.

The recent quality review from Northwood Manor asked for a province-wide health care system response for pandemics - for instance, if we enter a second wave and have to redeploy staff from acute care to continuing care.

In the department's second-wave plan for the continuing care sector released last week, it also highlights the need for health workforce surge capacity and mechanisms that support health workforce redeployment. I'm just wondering if you can tell us a little bit about what those plans look like so far.

BRENDAN CARR: It's nice to be missed, so thanks for your question. I think there's been a collective recognition and understanding that the extent to which we respond as a system is key to our success dealing with an issue like the pandemic. We certainly recognized right up front that health human resources are pivotal.

Part of that planning involves - there's been a lot of training undertaken to train new individuals so they will be prepared to work within this sector - both people that have clinical training as well as non-clinical backgrounds. So if you look at some of the work that we do in terms of testing sites and assessment centres, some of the front-end work does not require clinical skills. It's more logistics and intake. From a scarce resource point of view, it makes more sense for us to be trying to train other people to do that kind of work so that our clinical staff can be doing the true clinical work.

We've been basically trying to build the workforce. We've been working on the notion of creating employment centres, so rather than each individual facility having to try to manage their own human resources - particularly if they're in the midst of a challenging situation like an outbreak - essentially we're creating centres around the province that will provide more collective support to facilities within their zone.

Likewise, the approach contemplates the designation of facilities within the zones that would be places where residents of long-term care who were positive could go to be looked after - sort of regional treatment sites. Part of that plan is also around developing the resource supports that will allow that to happen.

There's quite a bit of work going on in the area of HR and I think it's one of the areas that we recognize, as I think Mr. Spinney said earlier, is key to our success.

SUSAN LEBLANC: I'm wondering if you can talk a little bit in the same vein a little bit about the backlogs in hospital procedures: mammograms and colonoscopies and blood testing and that kind of thing. I understand that during the first wave, we were lucky not to have our hospitals overwhelmed, which we are now hearing in Upper Canada is happening quite a lot. That's because of the hard work of Nova Scotians.

[10:45 a.m.]

Can you explain to us what the strategy was in the first wave and give us the update of where we would be to get back to normal? Again, pause that, and where we are if we do enter a second wave?

BRENDAN CARR: To roll back the clock, we responded like virtually every other jurisdiction. When this was coming, we didn't really know what it was going to bring and we were very focused on creating capacity within the acute care sector, because we thought we were going to experience what had been experienced in Italy, New York and other places. That is not how we're approaching the second wave. The benefit of that was we had capacity and we demonstrated we were effectively able to do that across the province. It worked very well.

I would say that we also recognized a number of unintended consequences of that - both in terms of people who were not able to access regular services during that period of time, as well as other things like how the very strict restrictions around visitation and things like that actually had a huge impact on patients, on their families, on caregivers and on the health of our communities.

These are important things that we've been thinking about as we're moving into the second wave. In the second wave, we're taking more what I would say is an incremental approach, and rather than thinking of the province as a single unit, we are thinking about it more geographically. We're developing more of an approach that will be a scaled approach,

depending upon what's happening within a community, keeping in mind the need to balance both the ongoing provision of services and the ability to respond to COVID. There will be some scaling in that depending upon what's happening in a particular area. Our objective is to try to minimize the amount of disruption of ongoing services.

In the first wave, for the record, we were able to maintain cancer services. We increased the number of mental health and addiction services that were provided to people in the province, which was really important. On the other side with orthopedic surgery, not so much.

We are being mindful of continuing important things that we know are impacting people in Nova Scotia, while at the same time developing a plan that will allow us to escalate should we be required to in a given zone, depending upon the conditions related to COVID, if that makes sense.

THE CHAIR: The time for the NDP caucus has expired and we'll give the final eight minutes to the Liberal caucus. Ms. Lohnes-Croft.

SUZANNE LOHNES-CROFT: I would just like to finish up with my little topic. I was pleased to see that you do have the whistleblower line and email. I've worked in organizations where we've intentionally set some very good policies, but a lot of people didn't know we had them. How are you communicating the whistleblower line and email with the Nova Scotia Health Authority? I'd like to extend that to the foundations and community health boards. Do they know? Do individuals know who sit on those boards and whatnot?

DEREK SPINNEY: It's a great question. There are a few things that we've done. First of all, Brendan communicated with the organization in March. That was followed up with a second communication by our senior director of human resources in June. As well, there are actually posters around, if you will. One of those - you get on the elevator and you see the poster. Those are some of the ways that we're encouraging and educating internally.

It's interesting as well that you had mentioned the other parties, because it is everybody's responsibility - everybody that touches us. So to be honest, I'm not sure exactly what we have done with the foundation. That is something that I'll be taking away from this - to check on that. It's a really good point and something that we can easily facilitate.

SUZANNE LOHNES-CROFT: I'll hand it over to Mr. Jessome.

THE CHAIR: Mr. Jessome.

BEN JESSOME: Dr. Carr indicated that the organization as a whole is upwards of 40,000 strong. I'm curious about how large a faction the cybersecurity team would be within that 40,000.

BRENDAN CARR: I'll pass it over to Mr. Nemirovsky. I'll just say small but mighty is probably the - but Mr. Nemirovsky can give you more details.

ANDREW NEMIROVSKY: As I said, the findings are still in draft from our partner. The team is going to be small but mighty. The thing to remember is that it's not just the team within Nova Scotia Health, it is truly a partnership with Nova Scotia Digital Service.

They currently have a team - upwards of 25 people - that manage cybersecurity across the province. It's not just for Health and Wellness and it's not just us. We will need some internal folks. I'm going to guess somewhere between three and five people based on the preliminary report. They'll be working very closely with that team with Nova Scotia Digital Service. Those numbers are yet to be finalized or confirmed.

BRENDAN CARR: Thank you. I apologize, but I think what's most important here is cybersecurity and privacy is everybody's job in Nova Scotia Health Authority. All 40,000 of those people need to understand that if they're interacting with patients, or are in any way supporting patient care, that they have a duty and a responsibility to be part of that team.

That's job number one: creating the culture in our organization where everybody understands the role that they play. That's our goal. We will be supported by our communications teams, by content experts within the IT-IM portfolio. We will work with our partners. We will be guided by an emerging understanding of how best to manage this in our environment.

At the end of the day, we are only going to be successful when every person who comes to work who is interacting with patient information understands that they have an individual role. As Mr. Nemirovsky said, the greatest form of threat is somebody sending an email, which happens virtually every day to all of us - where somebody is trying to get us to do something that could compromise patients. It's not just a flippant statement. We have to have everybody playing on the team.

BEN JESSOME: As a non-cybersecurity expert myself, I wouldn't preconceive what the size of a team should be to manage this. Certainly, everybody plays a role. I would also highlight again for the record that there was agreement expressed here today that there was a gap between where responsibilities for certain things fit in and then a charted path forward toward trying to button those up, identify where those gaps were, and who was responsible for what. It sounds like there's a strong consciousness to get beyond that and continue to improve.

Upon the amalgamation of our health authorities, are there things that respective health authorities were doing that we've brought with us to the overarching structure? Are there things that have changed? What reassurances can you provide the committee to say that we're taking the good and shaving off the not-so-efficient stuff that's been taking place with respect to enhancement of cybersecurity and protection of privacy?

ANDREW NEMIROVSKY: As with pretty much every other part of the amalgamation of NSHA, we've done exactly what you've talked about. We've taken the good, tried to get rid of the bad practices and keep those things that were effective: keeping patient data safe, keeping our systems secure. It's still a learning process for everyone.

As the cybersecurity landscape changes on a daily/weekly/monthly basis, it's very hard to keep up with the criminals. They're really smart and they have lots of resources. We work as hard as we can, but it's an ongoing challenge. It is not just for Health and Wellness; it is for every organization around the world. It's not just an NSHA problem; it's a government problem, it's a public problem, it's an Amazon problem. There's money to be made, so they put the effort in to try to beat us.

THE CHAIR: The time for the Liberal caucus has expired. That concludes the questioning and we'll open the floor up now to Dr. Carr or if any of your team would like to make some closing comments?

BRENDAN CARR: I'll just make a very brief comment. Thank you very much again for the opportunity to be here today. Thank you for your questions. I would also like to thank the Auditor General for the work that they do and the important role that they play as an independent body that kind of takes a hard look at the work that we do and offers critical appraisal.

I hope you will appreciate that we take that very seriously, we take the accountability that we have as an organization extremely seriously. We do endeavour every day to make sure that the resources that are entrusted to us are being used, that they're being used appropriately, that they're delivering the most value that we can for the citizens of Nova Scotia.

This is the first opportunity that I've had to come to Public Accounts Committee of Nova Scotia, so I would also just like to say thank you for that today. Perhaps another time we'll have the opportunity to kind of talk a little bit more about our health system, not so much about COVID but just generally speaking, but suffice it to say, the citizens of Nova Scotia should be very proud of the health system in Nova Scotia.

As a rule of thumb we spend on average or a little bit less than average of our peers across the country, and our performance is generally average to above average. There are certainly areas that we need to improve, but as a system overall we do a very good job.

I think the last comment that I'll make as somebody coming back into this organization, seeing an organization that has been through a significant change in the last five years, we should all take some comfort in this organization's ability to respond through COVID and do that in a way that has been joined up, that has demonstrated the intention of creating a single system.

We should take a lot of comfort in the fact that, as a province, when we identify particular areas of need like mental health and addictions or attaching people to primary care teams, if you actually look at the data on how Nova Scotia has been performing vis a vis the other provinces, we're actually leading most other provinces and doing better than average.

That is a signal not that we've got everything right, but the system that we're creating is actually allowing us to focus on important things and get those important things done. I would look forward in the future to talking to you more about what some of those important things are, like health equity, about diversity, about how we deal with systemic bias in our system, and many of the kinds of things that are impacting health care in our province. Thank you very much.

THE CHAIR: That concludes the questioning of the witnesses on today's topic. We'll give the witnesses an opportunity if they want to gather up everything. Again, we thank you on behalf of the Public Accounts Committee for appearing here today. COVID did throw a couple of wrenches in because we had planned to meet earlier, but that couldn't happen.

Mr. Halman.

TIM HALMAN: With your permission, I'd like to put forward a motion. On September 28, 2018, this committee embarked on an experiment that was forced upon it by the Liberal caucus. The Liberal caucus' resolution on September 28, 2018, stated that all agenda items for Public Accounts be set through the Auditor General. This narrowed the scope of the committee and decreased the effectiveness and relevance of the committee.

Together with the decrease in the number of meetings, these changes have not served Nova Scotians well, nor have they served our system well. At this time, Nova Scotians expect more accountability and transparency from those who represent them, not less. They expect Standing Committees to deal with issues that impact their lives - not only issues that the Auditor General has examined, but also topics outside of that report.

Therefore I move that the Standing Committee on Public Accounts return to weekly meetings, and that in addition to reports of the Auditor General, committee meetings examine topics brought forward by all three caucuses and agreed to by the subcommittee and entire committee.

[11:00 a.m.]

THE CHAIR: You've heard the motion. Is there any discussion? Ms. Roberts.

LISA ROBERTS: I would be in support of this motion. As members of the Public Accounts Committee, we had the opportunity to attend some online training with the Chair of the Public Accounts Committee in England in September. That training focused on that committee's role in oversight and accountability for the U.K.'s COVID-19 response. That included a whole litany of activities and meetings that really showed the potential of a Public Accounts Committee despite all the various challenges that democracy has faced in the U.K.

The Public Accounts Committee in the U.K. is held up as the exemplar of good Public Accounts Committee - a functioning one. It was just striking to me that during that same period of time when they had had that very robust program of work, our committee had not met until literally one day before that training when we had our first meeting.

As much as I welcomed the conversation today and the opportunity to find out what has happened since October 2019, frankly given all that has happened, we ought to be in a position to be putting forward new topics and being responsive to what best serves the interests of Nova Scotians to learn more about. That includes topics that are being examined by the Auditor General but also other topics that relate to the finances and administration of public resources by the Government of Nova Scotia.

THE CHAIR: Is there any further discussion? Mr. Halman.

TIM HALMAN: I'd like to thank my colleague for her remarks. It's very important and I'd like to call for a recorded vote, Mr. Chair.

THE CHAIR: A recorded vote has been called for. Everybody understands the motion that the Public Accounts Committee will change to weekly meetings on topics that are chosen and submitted to the subcommittee by each caucus. Am I correct with that, Mr. Halman?

TIM HALMAN: That's correct.

THE CHAIR: To the recorded vote: I'll keep a standing record here now.

YEAS	**NAYS**
Ms. Roberts	Ms. Lohnes-Croft
Mr. Halman	Ms. Miller
Ms. Leblanc	Mr. Jessome
Mr. Bain	Ms. DiCostanzo
	Mr. Horne

THE CHAIR: The motion has been defeated 5 to 4.

We'll move on now to other committee business. The first is if you recall from our last meeting there was discussion about requesting updates for the implementation of various recommendations of the Auditor General. We did send those letters out and we got responses from the Department of Education and Early Childhood Development relating to the November 2016 Auditor General Report; from the Department of Health and Wellness, on the June 2015 general report; and from Service Nova Scotia and Internal Services a response from the June 2015 report, as well. That is received for your information.

The next meeting is scheduled to happen on November 11th, which is Remembrance Day. We need to pick an alternate date for that meeting. I'd like to suggest either the 4th or the 18th and the committee can decide.

Any discussion? Ms. Roberts.

LISA ROBERTS: I would like to suggest the 4th and perhaps that will create some potential for an additional meeting in November.

THE CHAIR: Mr. Halman.

TIM HALMAN: I'm fine with November 4th.

THE CHAIR: Any further discussion? Do we agree that the next meeting will be on November 4th?

It is agreed.

Also, the 2019 annual report has been circulated to everyone. There have been no comments or changes received from the members. Can we have a motion to approve the 2019 Annual Report of the Standing Committee on Public Accounts?

BEN JESSOME: I so move.

THE CHAIR: Would all those in favour of the motion please say Aye. Contrary minded, Nay.

The motion is carried.

Next on the agenda is the Subcommittee on Agenda and Procedures for the September 9th meeting. We met on September 9th and reviewed the three reports of the Auditor General, namely the June 2020 report regarding the Nova Scotia Liquor Corporation - Phase I, the July 14, 2020 report regarding the QEII New Generation Project - Halifax Infirmary Expansion and Community Outpatient Centre - Phase II, and on July 28th, the 2020 report regarding government-wide contaminated sites.

The decision from that meeting has been provided to the members so I'm going to ask for a motion to approve that record of decision. Do we have a mover?

SUSAN LEBLANC: I so move.

THE CHAIR: Would all those in favour of the motion please say Aye. Contrary minded, Nay.

The motion is carried.

Our next meeting date is going to be November 4th, as we agreed. Probably one of those three will be on the agenda for the November 4th meeting.

Is there any further business to come before us today? Hearing none, just a reminder before we leave, out the side exits. There are recycle bins out there next to the exits if you want to get rid of your water bottles, papers and everything else. If there is no further business, the meeting stands adjourned.

[The committee adjourned at 11:08 a.m.]