



Second Session – Forty-Third Legislature  
of the  
**Legislative Assembly of Manitoba**  
**Standing Committee**  
**on**  
**Public Accounts**

*Chairperson*  
*Mr. Josh Guenter*  
*Constituency of Borderland*



Vol. LXXIX No. 2 - 7 p.m., Wednesday, March 5, 2025

**MANITOBA LEGISLATIVE ASSEMBLY**  
**Forty-Third Legislature**

Member	Constituency	Political Affiliation
ASAGWARA, Uzoma, Hon.	Union Station	NDP
BALCAEN, Wayne	Brandon West	PC
BEREZA, Jeff	Portage la Prairie	PC
BLASHKO, Tyler	Lagimodière	NDP
BRAR, Diljeet	Burrows	NDP
BUSHIE, Ian, Hon.	Keewatinook	NDP
BYRAM, Jodie	Agassiz	PC
CABLE, Renée, Hon.	Southdale	NDP
CHEN, Jennifer	Fort Richmond	NDP
COMPTON, Carla	Tuxedo	NDP
COOK, Kathleen	Roblin	PC
CROSS, Billie	Seine River	NDP
DELA CRUZ, Jelynn	Radisson	NDP
DEVGAN, JD	McPhillips	NDP
EWASKO, Wayne	Lac du Bonnet	PC
FONTAINE, Nahanni, Hon.	St. Johns	NDP
GOERTZEN, Kelvin	Steinbach	PC
GUENTER, Josh	Borderland	PC
HIEBERT, Carrie	Morden-Winkler	PC
JACKSON, Grant	Spruce Woods	PC
JOHNSON, Derek	Interlake-Gimli	PC
KENNEDY, Nellie, Hon.	Assiniboia	NDP
KHAN, Obby	Fort Whyte	PC
KINEW, Wab, Hon.	Fort Rouge	NDP
KING, Trevor	Lakeside	PC
KOSTYSHYN, Ron, Hon.	Dauphin	NDP
LAGASSÉ, Bob	Dawson Trail	PC
LAMOUREUX, Cindy	Tyndall Park	Lib.
LATHLIN, Amanda	The Pas-Kameesak	NDP
LINDSEY, Tom, Hon.	Flin Flon	NDP
LOISELLE, Robert	St. Boniface	NDP
MALOWAY, Jim	Elmwood	NDP
MARCELINO, Malaya, Hon.	Notre Dame	NDP
MOROZ, Mike, Hon.	River Heights	NDP
MOSES, Jamie, Hon.	St. Vital	NDP
MOYES, Mike, Hon.	Riel	NDP
NARTH, Konrad	La Vérendrye	PC
NAYLOR, Lisa, Hon.	Wolseley	NDP
NESBITT, Greg	Riding Mountain	PC
OXENHAM, Logan	Kirkfield Park	NDP
PANKRATZ, David	Waverley	NDP
PERCHOTTE, Richard	Selkirk	PC
PIWNIUK, Doyle	Turtle Mountain	PC
REDHEAD, Eric	Thompson	NDP
SALA, Adrien, Hon.	St. James	NDP
SANDHU, Mintu, Hon.	The Maples	NDP
SCHMIDT, Tracy, Hon.	Rossmere	NDP
SCHOTT, Rachelle	Kildonan-River East	NDP
SCHULER, Ron	Springfield-Ritchot	PC
SIMARD, Glen, Hon.	Brandon East	NDP
SMITH, Bernadette, Hon.	Point Douglas	NDP
STONE, Lauren	Midland	PC
WASYLIW, Mark	Fort Garry	Ind.
WHARTON, Jeff	Red River North	PC
WIEBE, Matt, Hon.	Concordia	NDP
WOWCHUK, Rick	Swan River	PC
<i>Vacant</i>	Transcona	

**LEGISLATIVE ASSEMBLY OF MANITOBA  
THE STANDING COMMITTEE ON PUBLIC ACCOUNTS**

**Wednesday, March 5, 2025**

**TIME – 7 p.m.**

**LOCATION – Winnipeg, Manitoba**

**CHAIRPERSON – Mr. Josh Guenter (Borderland)**

**VICE-CHAIRPERSON – MLA Jim Maloway (Elmwood)**

**ATTENDANCE – 11 QUORUM – 6**

*Members of the committee present:*

*Messrs. Blashko, Brar, MLAs Chen, Compton, Devgan, Mr. Guenter, MLAs Lamoureux, Maloway, Messrs. Nesbitt, Oxenham, Mrs. Stone*

*Substitutions:*

*Mr. Blashko for MLA Dela Cruz*

**APPEARING:**

*Tyson Shtykalo, Auditor General*

**WITNESSES:**

*Scott Sinclair, Deputy Minister of Health, Seniors and Long-Term Care*

*Sandra Henault, Executive Financial Officer, Health, Seniors and Long-Term Care*

*Chris Christodoulou, Interim Chief Executive Officer, Shared Health*

*Kevin Holowachuk, Director Cybersecurity (CISO), Digital Shared Services, Shared Health*

*Christine Pawlett, Executive Director, Clinical Digital Solutions, Digital Shared Services, Shared Health*

**MATTERS UNDER CONSIDERATION:**

*Auditor General's Report – eChart Manitoba, dated October 2018*

*Auditor General's Report – Forensic Audits, dated October 2018*

*Pharmacare: Special Audit of Financial Irregularities and Controls*

*Auditor General's Report – Main Street Project Investigation, dated June 2021*

*Auditor General's Report – Follow-up of Recommendations, dated March 2020*

*eChart Manitoba*

*Pharmacare: Special Audit of Financial Irregularities and Controls*

*Auditor General's Report – Follow-Up of Previously Issued Audit Recommendations, dated March 2021*

*eChart Manitoba*

*Pharmacare: Special Audit of Financial Irregularities and Controls*

*Auditor General's Report – Follow-Up of Previously Issued Audit Recommendations, dated April 2022*

*eChart Manitoba*

*Pharmacare: Special Audit of Financial Irregularities and Controls*

*Auditor General's Report – Follow Up of Previously Issued Recommendations, dated February 2024*

*Main Street Project Investigation*

\* \* \*

**The Chairperson:** Good evening. Will the Standing Committee on Public Accounts please come to order.

**Committee Substitution**

**The Chairperson:** Before we begin our business today, I would like to inform the committee that we have received a membership substitution for this meeting only. This evening MLA Blashko will be substituting for MLA Dela Cruz.

\* \* \*

**The Chairperson:** This meeting has been called to consider the following reports: The Auditor General's Report–eChart Manitoba, dated October 2018; Auditor General's Report–Forensic Audits, dated October 2018, Pharmacare: Special Audit of Financial Irregularities and Controls; and the Auditor General's Report–Main Street Project Investigation, dated June 2021; and the Auditor General's Report–Follow-up of Recommendations, dated March 2020, eChart Manitoba, Pharmacare: Special Audit of Financial Irregularities and Controls; and the Auditor General's Report–Follow-Up of Previously Issued Audit Recommendations, dated March 2021, and that's eChart Manitoba, Pharmacare: Special Audit of

Financial Irregularities and Controls; and the Auditor General's Report-Follow-Up of Previously Issued Audit Recommendations, dated April 2022, and that's eChart Manitoba and Pharmacare: Special Audit of Financial Irregularities and Controls; and lastly, the Auditor General's Report: Follow Up of Previously Issued Recommendations, dated February 2024, and that's the Main Street Project Investigation.

Are there any suggestions from the committee as to how long we should sit tonight?

**MLA Jim Maloway (Elmwood):** Sit for an hour and then revisit.

**The Chairperson:** There's been a suggestion that we sit for an hour and revisit. Is that agreed? *[Agreed]*

I believe there was prior agreement that this committee had complete consideration of the following items without further discussion: the Auditor General's Report-Main Street Project Investigation, dated June 2021; and the Auditor General's Report-Follow Up of Previously Issued Recommendations, dated February 2024, regarding the Main Street Project Investigation.

Does the committee agree to complete consideration of these items? Agreed? *[Agreed]*

In what order does the committee wish to consider the remaining reports? MLA Nesbitt?

**Mr. Greg Nesbitt (Riding Mountain):** Pharmacare first, followed by eChart. Is that correct?

**The Chairperson:** Okay, there's been a suggestion that we consider the Auditor General's Report on Pharmacare, followed by the report on eChart. Is that agreed? *[Agreed]*

At this time, I will also ask the committee if there is leave for all witnesses and attendants to speak and answer questions on the record if desired. Is that agreed? *[Agreed]*

Leave has been granted.

Before we proceed further, I'd like to inform all in attendance of the process that is undertaken with regard to outstanding questions. At the end of every meeting, the research clerk reviews Hansard for any outstanding questions that the witness commits to provide an answer to, and will draft a question-pending-response document to send to the deputy minister. Upon receipt of the answers to those questions, the research clerk then forwards the responses to every Public Accounts Committee

member and to every other member recorded as attending that meeting.

We will now consider the chapters on Pharmacare: Special Audit of Financial Irregularities and Controls.

Does the Auditor General wish to make an opening statement?

**Mr. Tyson Shtykalo (Auditor General):** I'd first like to introduce staff members I have with me today. I am joined by Jeff Gilbert, assistant auditor general and Jacqueline Ngai, audit principal.

Mr. Chair, in November 2014, the Winnipeg Police Service notified Pharmacare of a potential misappropriation of funds. The police had an individual in custody who was in possession of a cheque from Pharmacare and was unable to provide a reasonable explanation for why they had the cheque. Pharmacare conducted a preliminary investigation and found an employee was entering unsupported transactions into the Pharmacare system, which resulted in illegitimate payments being issued to several individuals.

In 2015, the former minister of Finance requested that my office conduct a special audit of the Pharmacare claims process and the transactions made by a specific employee. This request, made under section 16 of The Auditor General Act, was accepted. Our audit focused on payments resulting from the manual entries made by the suspected employee during the employee's entire period of employment. These transactions totalled \$1.1 million.

Mr. Chair, we determined that between 2007 and 2015, the former Pharmacare employee processed over \$236,000 in suspicious payments, without the proper receipts or supporting documents. These payments were generally of higher dollar amounts and processed repeatedly to the same group of individuals.

Through our audit work, we found an internal control environment at Pharmacare with many significant gaps. This enabled the employee to process transactions with no support. These unsupported transactions resulted in payments being sent to several individuals. We made five recommendations that would help prevent similar issues from occurring again. We conducted our third and final follow-up on these recommendations in 2022. We noted that as at September 30, 2021, only one of the five recommendations had been implemented: that Manitoba Health forward our detailed audit findings to Civil Legal Services.

\* (19:10)

I'd like to extend my thanks and appreciation for the co-operation and assistance received from the many dedicated employees of the former department of Health and Healthy Living. I would also like to thank my audit team for their due diligence and hard work in completing the report, and I look forward to the discussion today on this report.

**The Chairperson:** Thank the Auditor General for his opening comments.

Does the Deputy Minister of Health, Seniors and Long-Term Care wish to make an opening statement, and could he please introduce his staff joining him here today?

**Mr. Scott Sinclair (Deputy Minister of Health, Seniors and Long-Term Care):** So I'd like to start off by introducing Sandra Henault, who is the department's chief financial officer—or, executive financial officer, sorry—my apologies. I'd also like to start by thanking the Auditor and the Auditor's team for the work that they've done on this audit and appreciate the recommendations and the work that they've put into this system.

As the Auditor noted—or, the Auditor General noted, this was a matter that was referred to them given the significance of the concerns, and this is an audit that we view as helping us to understand where there's vulnerabilities in a large-volume transactional program that supports Manitoba's having access to low-cost medications.

The Non-Insured Benefits Branch is under the oversight of the Insurance Division in the Department of Health, Seniors and Long-Term Care. This branch is responsible for the administration of the provincial Pharmacare program, as well as the residential charges for long-term-care residents and the ancillary services program—which includes prosthetics and orthotics—the Seniors' Eyeglass Program and the Manitoba Adult Insulin Pump Program as examples.

Pharmacare is a drug-benefit program for eligible Manitobans, regardless of age or disease, whose income is significantly affected by prescription drug costs and these costs are not covered by other provincial and/or federal programs or private insurance. Pharmacare is a deductible-based system that is based on the total family income adjusted for the number of dependents in the family. Administration of the Pharmacare program occurs through the Drug Program Information Network, also known as DPIN

system. These system—or, this system was developed and implemented in 1995, has been the primary method of service delivery for the Pharmacare program both by the department as well as prescribing pharmacies.

In 2018, as the Auditor General notes, they released a report on Pharmacare entitled special audit of financial irregularities and controls. That was in response to an incident in the Pharmacare program dating back to pre-2015.

Since the initial report was released, the Auditor General has released three follow-up reports on March 2020, March 2021 and April 2022. The audit highlighted opportunities for improvement to internal processes and controls with considerations for DPIN enhancements to automate manual processes, and it noted the irregular payments over many years were made through manual adjustments in DPIN under the Pharmacare program that totaled more than \$236,000. A total of five recommendations were made in the 2018 report.

The department accepts and agrees with the recommendations in the report and has been working since the report release on addressing these recommendations through review of internal processes and controls to address the findings and enhancements of the DPIN system. The department has either implemented or is working towards addressing the recommendations outlined in the report, and work continues on updating policies to support implementation of the recommendations where appropriate.

Since the release of the report, Pharmacare special audit and irregularities controls, the department has referred the audit findings to Civil Legal Services and as a result, considers that recommendation to be resolved. The department has been updating and enhancing DPIN to build in 'automatted'—automated internal controls for processing of manual transactions where it has made sense to do so.

A cost-benefit analysis has not been completed; however, the department has completed many enhancements to the DPIN system over the past seven years to reduce the potential for fraudulent activity and to build internal controls and applications for processing of manual transactions that are consistent with the intent of the Auditor General's report finding and recommendations. Some of these enhancements continue to be in progress, and the department considers this resolved. Ongoing and continuing

enhancements to DPIN are expected and will never be fully resolved.

We've implemented a supervisory view of manual transactions where the business administration unit manager reviews a sample of weekly claims to ensure appropriate documentation for processing is present. The Non-Insured Benefits Branch does not have sufficient resources nor supervisory staff to complete a review of all manual transactions. However, the business accountability unit manager and the executive director verification of these samples will provide sufficient oversight required to mitigate potential for fraudulent activity.

Enhancements to the DPIN system have been made to document entries made into the DPIN system. Most manual adjustments—either reversals, adjustments, receipts, applications, deductible adjustments and checks—already had a user ID attached to the transaction and functionality has been developed that has allowed for the addition of an additional employee ID, and a reason to document each manual entry relating to client expenditure adjustments are made in DPIN.

Process automation has now been implemented when a client is a Canadian resident. Programming rules have been established where daily CRA income verifications load directly into the client's profile without manual intervention. When Manitoba Health and CRA information matches, the deductible is then automatically populated based on daily information that is received from Canada Revenue Agency.

The department has recognized that both technology limitations and reliance on manual claims processing and adjustments will not eliminate the potential for fraud or error and the department approaches to reducing allocation to address the recommendations in the OAG report is based on balancing the business risk with the financial and operational cost of implementing the recommendations fully as proposed by the Auditor General.

The scope of the work does continue to evolve, and the department will continue to collaborate with its partners to define opportunities to address all of the recommendations.

**The Chairperson:** I thank the deputy minister.

The floor is now open for questions.

**MLA Maloway:** Well, thank you very much, and it sounds like you've made a lot of improvements on those recommendations, but what assurances do we

have that a person like that could not repeat the same thing that he did? Like, get away with that amount of money over a seven-day period. Like, what is our certainty to know that all the changes you've made guarantee that that couldn't happen today?

**Mr. Sinclair:** So, thank you for that question. I think that's the, I mean, really, like, I would suspect is the crux of the concern around the other report is that is there continued vulnerabilities for an individual to repeat what was a known vulnerability that the Auditor General looked into.

The response to that would be twofold: primarily—or, not primarily—the first would be the daily audits of the records to see what's being—some of the transactions so that we would be able to note irregularities far sooner than the ability to—somebody to fraudulently process transactions in amount of \$238,000.

So this wasn't a single transaction of \$238,000 as I understand how this was done. This was a series of multiple transactions, small transactions, that were occurring over a period of time that were related to a single individual going into the system with a single log-in point and adjusting an individual's deductible back to the beginning of the year that would allow for them to then reset their deductible limits, and there would be some—we assume, don't know for sure, as I wasn't looking at the police component of it or any of those—would be shared with an individual.

So these were small transactions that were designed not to alert the system to a big transaction, so we would see these irregular transactions on a daily basis through their—through the regular auditing.

The other piece to it is the—as I referenced—was the individual was logging in singularly; one individual was making these transactions. There now requires to be a second employee ID logged into the system in order for those transactions which will then indicate that a second person is aware of the manual transaction that's happening and should increase the probability—or reduce the likelihood that somebody is singularly doing these multi small transactions over a period of time.

**MLA Maloway:** Yes, my follow-up question is that this was—this software was quite revolutionary at the time; this was, like, the Filmon government bringing this in. And it was—I don't know whether it came out of SmartHealth at the time, the program they had. But anyway, it was a very, very good program at the time.

So how has all the software changed over the years? Like, are we using the same system now? I'm assuming we're on a cloud-based system now, or no?

**Mr. Sinclair:** So, it—no, it is the same system. I appreciate you seeing it as a visionary system of the time, and it continues to be in 2025, 30 years on, the same system that's used.

\* (19:20)

It's not a cloud-based system; it's an on-prem solution of more of a traditional build from that time. It has undergone a number and series of enhancements and that, so it isn't this same program.

Obviously, it's gone through a number of enhancements just in working on different operating systems, so 1995—I'm not even going to try to remember what the operating system was then—but as we moved through various iterations of Windows, the system would have been updated to operate on those server systems and, at the same time, we would make program enhancements, functionality enhancements, including enhancements that came out of the audit itself to address some of the Auditor General's findings and recommendations.

So, yes, it's the same solution that was brought in in 1995. It is technology that would be considered no longer best in class, but it underpins a program that processes in excess of \$250 million a year in drug claims in a fairly efficient and effective manner, and we will continue to monitor its feasibility and effectiveness in that space.

And like we do with all of our IT assets, both in health and government more broadly, there's a process by which we bring forward opportunities to rebuild or enhance, and our IT experts make determinations and decisions about where our greatest vulnerabilities lie and make those investment decisions about where to move forward. And, at this point in time, it appears that our IT professionals believe that the system continues to have some life left in it and we continue to operate with that as our solution.

As I indicated, it's not just a solution that's operated by the Department of Health. It is also the system by which pharmacies transact with us, and a replacement of DPIN while at some point may be a necessary requirement, would be a significant undertaking because it would require changes both at the department level as well as the individual pharmacy level. And the vast majority of those operations are private businesses so we do need to respect, you

know, the costs and change management related to a system replacement at that level as well as ourselves.

**MLA JD Devgan (McPhillips):** To the second recommendation through the Chair, but correct me if I'm wrong, I heard mention about automated internal controls. So I'm wondering if we're using the same system and that there were some technical limitations previously, how those were maybe reconciled in order to implement these new internal controls. If we could hear a little bit more about that.

**Mr. Sinclair:** So just confirming, when you refer to the second recommendation, is it the one that the department conducted benefit cost analysis for making enhancements to the system to build automated internal controls?

So, some of those were—we didn't do it through a cost-benefit analysis; we undertook what we understood to be, or believed to be the most critical enhancements that needed to be required. The solution or the change enhancements stop short of a full automation of the solution. That would have been a fairly expensive and costly undertaking, so we automated the areas where we believed there was greatest risk in the context of being able to do individual transactions or manual transactions for many of these things.

So again, deductible resetting, rebates or reversal of transactions, those sorts of things that now require the second staff ID login so that there is a record of who is doing it as well as that there's a confirmation that a second individual is involved in those manual reversals or transactions, as opposed to those being automated through the system.

Many of those automated solutions would certainly be beneficial but would be in the context of a very large-scale system replacement. It's sort of—its functionality that's been noted as a part of a potential system replacement but it hasn't been built into a pathway for updating the existing system right now.

**MLA Carla Compton (Tuxedo):** I have a question around user feedback in terms of how are the people who are using the system finding it? Were they consulted in the development for where these holes were identified? And in the rollout, you know, talking about the practical application, many pharmacies, for example, are private businesses.

Has there been pushback with second login required—you know, additional task component? How has that been received? And also, have there been

identified catches that, you know, the second login and stuff applied to be filling those holes—have we actually found that they've been working? Do we know?

**Mr. Sinclair:** So thanks, I appreciate the question around staff feedback, and I can't comment at the time as to whether we did a, you know, an engagement, a survey, or anything around that to staff about what would work for them, that perspective. I would certainly like to think it did because that would be certainly a best practice in any sort of system change or a change management process.

Those that are using the system should be engaged and consulted in that development, but certainly in terms of your question around the feedback in terms of today's utilization of it, we haven't heard any concerns from staff with respect to the second login or the additional steps that are around that. That could be a function of it's been six or—five or six years since they've had to do that and it's—for most of the staff, it's what they've always known.

There's a fairly high staff turnover rate in the Pharmacare program. It's lots of clerks, and we like to see our staff elevated in more senior positions so they do move into the department and we bring individuals in, and, over this period of time, most people just have probably accepted that this is the way we do the work and they wouldn't know any different.

In terms of the additional catches, I'm just going to check with Sandra. I'm not aware of any significant fraudulent activity, so that's either an indication of, you know, there's enough deterrence in the system that people feel that there is not a means to do what was done before, or we are catching small ones when they're happening before they get to be too big.

But certainly I can follow up with the department to see if there's any—been any significant catches that we were not aware of, but I think the sense is that we haven't had any significant indication of fraudulent activity. It's a good sign that people are aware of the controls. They're aware of the fact that the audits are happening. They're doing what audits are intended to do, which is to discourage inappropriate behaviours and actions because you may get caught on that front, and as a result, we're functioning at a place that's better than it was in 2018.

**The Chairperson:** Hearing no further questions or comments, I will now put the question on the Pharmacare: Special Audit of Financial Irregularities and Controls chapters.

Does the committee agree to complete consideration of the chapter Pharmacare: Special Audit of Financial Irregularities and Controls within the Auditor General's Report—Forensic Audits, dated October 2018? *[Agreed]*

Does the committee agree to complete consideration of the chapter Pharmacare: Special Audit of Financial Irregularities and Controls within the Auditor General's Report—Follow-up of Recommendations, dated March 2020? *[Agreed]*

Does the committee agree to complete consideration of the chapter Pharmacare: Special Audit of Financial Irregularities and Controls within the Auditor General's Report—Follow-Up of Previously Issued Audit Recommendations, dated March 2021? *[Agreed]*

Does the committee agree to complete consideration of chapter Pharmacare: Special Audit of Financial Irregularities and Controls within the Auditor General's Report—Follow-Up of Previously Issued Audit Recommendations, dated April 2022? *[Agreed]*

We will now consider the reports on eChart Manitoba.

Is there leave for a brief recess while the staff from Shared Health prepare for questioning? *[Agreed]*

All right. We will now briefly recess.

*The committee recessed at 7:28 p.m.*

*The committee resumed at 7:31 p.m.*

**The Chairperson:** All right. We will now consider the reports on eChart Manitoba.

Does the Auditor General wish to make an opening statement?

**Mr. Shtykalo:** Like to introduce the staff I have with me today. I'm joined by Wade Bo-Maguire, assistant auditor general.

In Manitoba, personal health information is stored on a number of electronic systems, each with their own clinical objective. Launched in 2010 by Shared Health, formerly eHealth, eChart pulls the information together for many of these systems, giving authorized health-care providers quick and easy access to their patients' medical histories.

Authorized users include physicians, nurses, administrative staff and other health-care professionals. In our 2018 audit report, we wanted to see



whether Shared Health was sufficiently managing the risks that could result in eChart's intended benefits not being realized, unauthorized access to private health information and eChart being unavailable when needed.

We found that Shared Health needed to better manage the risks that might prevent it from achieving eChart's intended benefits. We made five recommendations for improving their management of risk and note in our follow-up report that all five recommendations have been implemented or resolved.

At the time we also found several weaknesses in eChart's access controls that could have compromised the confidentiality of Manitobans' personal health information. For example, we noted that more than 87 per cent of eChart users could access personal health information of any Manitoban, and that eHealth's monitoring of user activities had gaps. Given the high percentage of users with full access to eChart, there was a heightened need to effectively monitor for inappropriate activity.

Finally, we found that eHealth had good practices in place to back up and restore eChart's data. However, eChart's disaster recovery plan was not complete.

This report included 15 recommendations in total for Shared Health to better manage the risks associated with operating eChart. In our April 2022 follow-up report, we noted that three recommendations are still in progress.

Like to extend my thanks for the co-operation and assistance received from the many dedicated public servants we met with during this audit. I would also like to thank my team for their due diligence and hard work in completing this audit. Look forward to the discussion.

**The Chairperson:** I thank the Auditor General.

Does the interim chief executive officer of Shared Health wish to make an opening statement, and would he please introduce his staff joining him here today.  
*[interjection]*

Sorry, Mr. CEO. Just need to recognize you for the purpose of Hansard. So, go ahead. You have the floor.

**Mr. Chris Christodoulou (Interim Chief Executive Officer, Shared Health):** Thank you very much.

Good evening and thank you for the privilege to present to the Public Accounts Committee and respond to questions related to Shared Health's completed and ongoing work related to the following Auditor General's reports: eChart Manitoba, dated October 2018; follow-up of previously issued audit recommendations, dated March 2020; and Follow-Up of Previously Issued Audit Recommendations, dated April 2022.

My name is Chris Christodoulou, interim chief executive officer of Shared Health. I'm joined today by Christine Pawlett to my right, executive director of clinical solutions, and Kevin Holowachuk, director of cybersecurity and chief information security officer of digital shared services for Shared Health.

I would like to extend my appreciation and gratitude to the Auditor General and the office of audit professionals. I want to acknowledge their professional and collaborative relationship with Shared Health and all our staff.

On behalf of Shared Health, I want to acknowledge the findings and recommendations contained within the ordered reports. I will speak today to the status of our response to a number of specific recommendations with my colleagues in attendance with me and look forward to the opportunity to respond to any outstanding questions.

As indicated by the Auditor General, since implementation, we can inform you that 99 per cent of hospitals in Manitoba, 96 per cent of nursing stations and 87 per cent of primary-care sites across Manitoba are covered by the eChart system. It is integrated into over 20 clinical source systems and receives from the systems in excess of 6.5 million messages per month, and eChart information is in excess of 10 million access points per year.

The eChart order published in 2018 examined whether Manitoba eHealth was sufficiently managing the risks, as outlined by the Auditor General in three categories: realizing its intended benefits, ensuring its information is accessed only by authorized individuals and ensuring it is available when needed.

The key findings, as outlined by the Auditor General, included the risks of not achieving eChart's intended benefits and the need for those to be better managed. eChart access control should be strengthened and good practices be put in place to ensure eChart's availability.

To address concerns identified in the findings, the office of the Auditor General provided 15 recommendations as outlined. Five of those were linked to define and better manage the risk of non-achieving intended benefits, nine of those were for strengthening eChart's access controls and one recommendation defined for ensuring eChart's availability.

Progress on addressing the ordered recommendations was subject to three follow-ups, as outlined. The 2022 status update provided by the office of the Auditor general indicates that approximately 53 per cent of the 15 recommendations were considered to be addressed, as shown in the status overview. Seven recommendations were the status of implemented or resolved, one recommendation with the status of action no longer required, four recommendations with a status of do not intend to implement and three recommendations with a status of work in progress.

Since the last status update, progress in addressing the recommendations has increased to a compliance of 73 per cent through the implementation of three recommendations, including two of the four previously defined as do not intend to implement. Planned work for the fiscal year of 2025 and 2026 will address further recommendations, bringing our progress to 80 per cent in addressing the 15 ordered recommendations.

I will now provide an update on addressing the recommendations in each of the categories. The first five, as the Auditor General outlined, have been addressed.

Recommendation 6, which indicated that we recommend that eHealth update the eChart user access guidance to specifically link health-care roles to appropriate eChart views and establish a process to handle any necessary exceptions identified by the sites was originally, as of 2021 September, a do not intend to implement. The update we can provide is that Shared Health's current site on boarding practices provide guidance to ensure appropriate eChart views are defined for the health-care roles at the site.

Recommendation 7: We recommend that eHealth is part of the periodic ordered sub-user activities that sites obtain assurance from each site that eChart users have signed the personal health information confidentiality pledges. This is no longer required.

Recommendation 8: We recommend that eHealth ensure that consultant staff attend personal health

information training sessions and sign confidentiality pledges. This is implemented and resolved.

Recommendation 9: We recommend that eHealth ensures site privacy officers are trained upon implementation of eChart or upon being assigned to this role and periodically thereafter. The status of it September 2021 was to not intend to implement. The latest update is that revisions to Shared Health practices have addressed this recommendation.

Recommendation 10: That eHealth define and communicate minimum timing requirements for sites to request removal of eChart users that no longer require those privileges. The original status update indicated to not intend to implement; the update is Shared Health has taken actions to implement this recommendation.

Eleven: We recommend that eHealth require sites to certify the quarterly user account management report as reviewed and communicate any needed changes in use over use and authorized users in a timely manner.

\* (19:40)

Originally, this was do not intend to implement. The update is that Shared Health agrees with the value of the recommendation and we will continue to explore opportunities to implement a technical solution to address the recommendation.

Recommendation 12: We recommend that eHealth update the eChart audit methodology to include a site selection process that is both random and unpredictable; and (b) that monitors users' activities through automated triggers and alerts; 12(a) has been implemented and resolved; 12(b) continues to be a work-in-progress recommendation. The update that I can provide is that analysis is currently under way with plans to implement the technical component of this recommendation after the eChart upgrade is completed in fiscal year 2025-2026.

Recommendation 13, that eHealth, in collaboration with the Winnipeg Regional Health Authority chief privacy officer, update the eChart privacy incident handling processes to clarify responsibility for patient and public notifications, has been implemented and resolved.

Recommendation 14: We recommend that eHealth promptly implement the cybersecurity control recommendations presented in the letter of management. The status as of September '21 was work in progress. An update that I can provide is that Shared

Health has addressed the cybersecurity control recommendations listed in the letter to management.

And, finally, recommendation 15: We recommend that eHealth develop, communicate, implement and test a disaster recovery plan for the data, systems and infrastructure, which would include eChart. This status as of September '21 was work in progress. The update that we can share with you today is that Shared Health will address this recommendation, with the upgrade of the eCharts scheduled for the fiscal year 2025-2026, and the upgrade will include new cloud-based hosting which will include a full disaster-recovery capability.

We're now prepared to take questions on administrative-related items posed by the committee and any recommendations that we've commented on. We will endeavour to answer any and all inquiries here today. I have a note that some questions may need to be taken as notice, in which case we will provide a specific response in writing.

I will pause there. Thank you.

**The Chairperson:** I thank the interim CEO for those opening comments.

The floor is now open for questions.

We've a question from MLA Maloway.

**MLA Maloway:** I'd like to ask you, then, presumably at the moment, then, you're—all these health records are being stored on a server farm somewhere. Where is this server farm?

**Mr. Christodoulou:** Thank you, member, for the question. I will confer with my team.

**The Chairperson:** The interim CEO, go ahead.

**Mr. Christodoulou:** The information is stored in servers in a data management centre in Winnipeg that is operated by digital health shared services.

**MLA Maloway:** And so this year, or later this year, you're going to be moving all this information to the cloud. And can you name the software you're using, your cloud-based software that you're going to be using? And then I assume you don't need the server farm anymore, right? So you'll be—what are you going to do then?

**Mr. Christodoulou:** I will confer with my team, and thank you to the member for the question.

To answer the member's question, the Altera software solution is the product that we will be using.

And the systems will transfer to this cloud-based system.

**MLA Compton:** As someone who has used these systems before, I have questions kind of through that user lens.

I'm curious how much consultation with the people using the system, like on the wards, on the floor, has been done or plans to be done as the system evolves in terms of direct feedback of understanding PHIA needs but also finding the balance of keeping things secure and functioning as well as being able to use it quickly—you know, efficiently—for the needs of serving our patients and clients and their families. And I know I haven't received, in the years that I worked on the floor, any sort of surveys or feedback on how are things working. Is that planned in the future, to check in with the people using it?

**Mr. Christodoulou:** I thank the member for the question. I'll confer to my team.

**The Chairperson:** Yes, go ahead, interim CEO.

**Mr. Christodoulou:** I'd like to request of the Chair that Christine Pawlett respond to that very important question on user feedback.

**The Chairperson:** Ms. Mullan *[phonetic]*.

**Ms. Christine Pawlett (Executive Director, Clinical Digital Solutions, Digital Shared Services, Shared Health):** Thank you for the question.

We do have surveys that are sent out to authorized sponsors. Those are typically—

**The Chairperson:** Sorry, Ms. Pawlett. I just wanted to recognize you for Hansard. My apologies. Go ahead. You have the floor.

**Ms. Pawlett:** Thank you.

We do have surveys that are sent out annually to authorized sponsors. As far as feedback goes, when we implemented the solution, we did look for feedback, but we do encourage users to provide feedback generally throughout the year.

As we do upgrades, we also look to involve user groups in testing the product and making sure it fits the needs.

**MLA Compton:** Kind of a follow-up to that in terms of, like, application: Have there been more notice, you know, when someone's maybe not following their PHIA protocol properly? Because it sounds like a lot

of things, even from the Auditor General's report, more things have been implemented for that.

Has there been—has that been identified as, you know, we're—I don't want to say catching people, but being able to mitigate, decrease inappropriate access of patients' information, things like that? Has—are you able to identify if that's happened?

**The Chairperson:** If the executive director or the CEO, when you are prepared to answer, just feel free to raise your hand, and I can recognize you at that point.

Go ahead, CEO.

**Mr. Christodoulou:** I'd like to thank the member for that question. I'll just confer with my team for a moment.

**The Chairperson:** The interim CEO.

**Mr. Christodoulou:** I would like to thank the member for that question. I have in previous roles with Shared Health as provincial anesthesia specialty lead and head of the department of anesthesiology, perioperative and medicine been involved in the processes that are undertaken if there is inappropriate eChart access.

There are routine audits that are undertaken. There are internal controls that can determine when individuals are accessing information that is not authorized within their user role. And in those circumstances, those individuals have been addressed from a performance-feedback and/or a disciplinary process that's led forward to deal with those violations.

\*(19:50)

**MLA Compton:** Oh, gosh, I had it. My question pertains to, we have eChart, but we also have other electronic record systems. So, like, I come from St. Boniface, for example, but the Manitoba Renal Program, so we had multiple programs, multiple kind of record systems that we were working with. What are potential vulnerabilities that are being considered around communication or a lack of communication between these differing systems? Because I know there would be inconsistency in actual information. So in terms of patient health information being consistent between these different ones, there could sometimes be discrepancies.

Is there plans to try and integrate the different systems to have consistent patient information along them or to keep them fully separated so that, again, for just safety reasons, security reasons, there's no

potential of overlap? Is there any consideration around that? Because I know clinical application can get cumbersome if you have a whole bunch of different systems that you have to access, so I'm just curious.

**Mr. Christodoulou:** I'd like to thank the member for the question. I'll confer with my team.

I'd like to thank the member for the question. We'd like to take this question away. The scope is much larger than the eChart in and of itself. What I can share with you, being an active user of both the electronic systems at the facility that you reference as well as an eChart user, is that you required username and password to access eChart through the integrated electronic clinical record that exists. So there is a username and password that's defined that has to be entered. But the scope is much bigger in terms of the integration piece, and we would like to take that away for further consideration to provide a response.

**MLA Devgan:** Actually, my colleague sort of stole my question, so I'm going to maybe look at it from a different perspective, but the transition to cloud storage and I guess the progression of this system that we're using, does that present an opportunity to consolidate these other systems? Because just anecdotally, I know from those who I know who work in the health-care system, there are some challenges with different systems and access, but perhaps down the road, that could be an opportunity and more of a question.

**Mr. Christodoulou:** I'd like to thank the member for that excellent and visionary forward-looking question. I'll confer with my expert team. Thank you.

I'd like to thank the member again for that excellent question. The purpose of eChart is to integrate multiple sources of information—just give you two examples, laboratory and diagnostics information—into one source of truth. And as to the question of does this pose opportunities in the future to better integrate solutions, the potential for that exists. But eChart in and of itself is a program that actually integrates many of the facets of information that puts one source of truth for clinicians, providers across the province. So whether you're in Flin Flon, Manitoba or Winnipeg, you can access the same information in those facilities that I've outlined that have this system.

Thank you.

**The Chairperson:** Before we go into MLA Devgan's question, five minutes to go before our agreed-upon

hour, is there a suggestion—[interjection] Okay, all right, so eight—we have 10 minutes. Okay.

**MLA Devgan:** I won't take all that time. Just to go back on the question that my colleague asked earlier regarding the cloud system.

Is that—the system that we're using, is that based out of Canada? Manitoba? And just, with regards to overall information security, is that system—how do I ask this question? Is it Canadian or is it American?

**Mr. Christodoulou:** I'd like to thank the member for a great question. I'll confer with my team.

Thank you, again, member. The company that we're contracted for cloud-based services is a Canadian company.

**MLA Maloway:** I recognize that there is same kind of problems that you have—other organizations have as well. And in the past, like Autopac, whether it's a server farm or cloud-based, whatever the point is, that there are many instances in the past where people are employed with agencies and they decide to look up famous hockey players and, you know, check on what kind of cars they own and stuff like that. And we know that can happen with the health-care system, too, right?

And I know that you have to draw some line somewhere, but if you go into a walk-in clinic, you'll find that the doctor there might only have access to a limited piece of your medical history, when you would like them to have more, right? But the danger of that, as you know, is that people can be shopping around looking at the whole thing.

But I am concerned about the security issue, because right now you're on a server farm—like the Autopac server farm is not even in Manitoba, it's in Ontario. Is that dangerous? I don't know. But you say it's here. But at least I'm a little more confident that you're telling me it's on a server farm and it's here, backed up onto there.

But once it gets into the cloud, I don't know where it is. You can tell me it's a Canadian company, but maybe it's a Canadian company today. But maybe a week from now it's going to be, you know, another country's going to own it. As far as I know, cloud-based systems are almost 100 per cent American, but, you know, so I'd like you to comment on that.

I mean, it's not really saying anything's gone wrong here, but there's certainly—the more you go cloud-based, to me, the more chances you're taking

that your information's going to end up in—and especially with AI, who knows where this is all going to end up at the end of the days.

**Mr. Christodoulou:** To address the member's question, I'll confer with my team.

**The Chairperson:** Just a general reminder to members of the committee just to direct questions through the Chair.

**Mr. Christodoulou:** Thank you, again, member, for that question.

We are aware that the data servers that support the cloud are located in Canada, but we will have to get back to you on the specific locations of those data centres. And they're all protected based on industry standard security protocols.

**The Chairperson:** All right, hearing no further questions or comments, I will now put the question on the eChart Manitoba Reports.

Auditor General's Report—eChart Manitoba, dated October 2018—pass.

\* (20:00)

Does the committee agree to complete consideration of the chapter eChart Manitoba within the Auditor General's Report—Follow-up of Recommendations, dated March 2020? [Agreed]

Does the committee agree to complete consideration of the chapter eChart Manitoba within the Auditor General's Report—Follow-Up of Previously Issued Audit Recommendations, dated March 2021? [Agreed]

Does the committee agree to complete consideration of the chapter eChart Manitoba within the Auditor General's Report—Follow-Up of Previously Issued Audit Recommendations, dated April 2022? [Agreed]

Before the committee rises for the day, I would ask that all members please leave behind their copies of the reports so that they may be used again at future meetings.

The hour being 8:01, what is the will of the committee?

**Some Honourable Members:** Rise.

**The Chairperson:** Committee rise.

**COMMITTEE ROSE AT:** 8:01 p.m.

The Legislative Assembly of Manitoba Debates and Proceedings  
are also available on the Internet at the following address:

**<http://www.manitoba.ca/legislature/hansard/hansard.html>**