Second Session – Forty-First Legislature

of the

Legislative Assembly of Manitoba

Standing Committee
on
Public Accounts

Chairperson
Mr. Matt Wiebe
Constituency of Concordia

Vol. LXX No. 4 - 10 a.m., Monday, May 8, 2017

ISSN 0713-9462

MANITOBA LEGISLATIVE ASSEMBLY
Forty-First Legislature

Member	Constituency	Political Affiliation
ALLUM, James	Fort Garry-Riverview	NDP
ALTEMEYER, Rob	Wolseley	NDP
BINDLE, Kelly	Thompson	PC
CLARKE, Eileen, Hon.	Agassiz	PC
COX, Cathy, Hon.	River East	PC
CULLEN, Cliff, Hon.	Spruce Woods	PC
CURRY, Nic	Kildonan	PC
DRIEDGER, Myrna, Hon.	Charleswood	PC
EICHLER, Ralph, Hon.	Lakeside	PC
EWASKO, Wayne	Lac du Bonnet	PC
FIELDING, Scott, Hon.	Kirkfield Park	PC
FLETCHER, Steven, Hon.	Assiniboia	PC
FONTAINE, Nahanni	St. Johns	NDP
FRIESEN, Cameron, Hon.	Morden-Winkler	PC
GERRARD, Jon, Hon.	River Heights	Lib.
GOERTZEN, Kelvin, Hon.	Steinbach	PC
GRAYDON, Clifford	Emerson	PC
GUILLEMARD, Sarah	Fort Richmond	PC
HELWER, Reg	Brandon West	PC
ISLEIFSON, Len	Brandon East	PC
JOHNSON, Derek	Interlake	PC
JOHNSTON, Scott	St. James	PC
KINEW, Wab	Fort Rouge	NDP
KLASSEN, Judy	Kewatinook	Lib.
LAGASSÉ, Bob	Dawson Trail	PC
LAGIMODIERE, Alan	Selkirk	PC
LAMOUREUX, Cindy	Burrows	Lib.
LATHLIN, Amanda	The Pas	NDP
LINDSEY, Tom	Flin Flon	NDP
MALOWAY, Jim	Elmwood	NDP
MARCELINO, Flor	Logan	NDP
MARCELINO, Ted	Tyndall Park	NDP
MARTIN, Shannon	Morris	PC
MAYER, Colleen	St. Vital	PC
MICHALESKI, Brad	Dauphin	PC
MICKLEFIELD, Andrew, Hon.	Rossmere	PC
MORLEY-LECOMTE, Janice	Seine River	PC
NESBITT, Greg	Riding Mountain	PC
PALLISTER, Brian, Hon.	Fort Whyte	PC
PEDERSEN, Blaine, Hon.	Midland	PC
PIWNIUK, Doyle	Arthur-Virden	PC
REYES, Jon	St. Norbert	PC
SARAN, Mohinder	The Maples	Ind.
SCHULER, Ron, Hon.	St. Paul	PC
SELINGER, Greg	St. Boniface	NDP
SMITH, Andrew	Southdale	PC
SMOOK, Dennis	La Verendrye	PC
SQUIRES, Rochelle, Hon.	Riel	PC
STEFANSON, Heather, Hon.	Tuxedo	PC
SWAN, Andrew	Minto	NDP
TEITSMA, James	Radisson	PC
WHARTON, Jeff	Gimli	PC
WIEBE, Matt	Concordia	NDP
WISHART, Ian, Hon.	Portage la Prairie	PC
WOWCHUK, Rick	Swan River	PC
YAKIMOSKI, Blair	Transcona	PC
Vacant	Point Douglas	

LEGISLATIVE ASSEMBLY OF MANITOBA

THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

Monday, May 8, 2017

TIME – 10 a.m.

LOCATION – Winnipeg, Manitoba

CHAIRPERSON – Mr. Matt Wiebe (Concordia)

VICE-CHAIRPERSON – Mr. Reg. Helwer (Brandon West)

ATTENDANCE – 11 QUORUM – 6

Members of the Committee present:

Messrs. Bindle, Helwer, Johnston, Ms. Klassen, Messrs. Lindsey, Maloway, Mrs. Mayer, Mr. Michaleski, Ms. Morley-Lecomte, Messrs. Wiebe, Yakimoski

Substitutions:

Mr. Lindsey for Mr. Marcelino

APPEARING:

Mr. James Teitsma, MLA for Radisson
Mr. James Allum, MLA for Fort Garry-Riverview
Mr. Norm Ricard, Auditor General

WITNESSES:

Hon. Kelvin Goertzen, Minister of Health, Seniors and Active Living
Ms. Karen Herd, Deputy Minister of Health, Seniors and Active Living
Mr. Perry Poulsen, Chief Information Officer, Manitoba eHealth (by leave)

MATTERS UNDER CONSIDERATION:

Auditor General's Report–WRHA's Management of Risks Associated with End-user Devices, dated July 2015

Auditor General's Report–Follow-up of Previously Issued Recommendations, dated May 2015

Section 2–Economic Development: Loans and Investments under The Development Corporation Act

Section 5–Animikii Ozoson Child and Family Services Agency

Section 11–Report on the Rural Municipality of St. Clements

Section 12–Citizen Concerns, North Portage Development Corporation

Section 16–Office of the Fire Commissioner

Auditor General's Report–Follow-Up of Recommendations, dated May 2016

Animikii Ozoson Child and Family Services Agency

Northern Airports and Marine Operations

Report on the Rural Municipality of St. Clements

Citizen Concerns, North Portage Development Corporation

Office of the Fire Commissioner

Citizen Concerns, Town of Lac du Bonnet, Bulk Water Sales

Rural Municipality of Lac du Bonnet

Lake Manitoba Financial Assistance Program, Parts C and D

Auditor General's Report–Follow-Up of Recommendations, dated March 2017

Citizen Concerns, North Portage Development Corporation

Rural Municipality of Lac du Bonnet

Provincial Nominee Program for Business

WRHA's Management of Risks Associated with End-user Devices

* * *

Mr. Chairperson: Good morning. Will the Standing Committee on Public Accounts please to–come to order.

This meeting's been called to consider the Auditor General's Report–WRHA's Management of Risks Associated with End-user Devices, dated July 2015, and several sections of the following reports, as listed on the agendas in front of you: the Auditor General's Report–Follow-up of Previously

Issued Recommendations, dated May 2015; the Auditor General's Report–Follow-up of Recommendations, dated May 2016; and the Auditor General's Report–Follow-up of Recommendations, dated March 2017.

Before we get started, are there any suggestions from the committee as to how long we should sit this morning?

Mr. Tom Lindsey (Flin Flon): At 11:30, we have a meeting we need to be at.

Mr. Chairperson: Okay, we will shoot for 11:30 to have the meeting then wrapped up. Is that agreed by the committee? *[Agreed]*

Committee Substitution

Mr. Chairperson: I would like to inform the committee that under rule 104(2) the following membership substitution has been made for this meeting: Mr. Lindsey for Mr. Marcelino.

*** * ***

Mr. Chairperson: It is my understanding that there's a willingness to deal with the sections of the 2015, 2016 and 2017 follow-up reports first. Is that agreed? *[Agreed]*

Are there any questions or comments on these items?

Seeing none, with regard to the Auditor General's Report–Follow-up of Previously Issued Recommendations, dated May 2015–does the committee agree that we have completed considerations–consideration of section 2, section 5, section 11, section 12 and section 16? *[Agreed]*

With regard to the Auditor General's Report–Follow-up of Recommendations, dated May 2016, does the committee agree that we've completed consideration of the following sections: Animikii Ozoson Child and Family Services Agency, the Northern Airports and Marine Operations; Report on the Rural Municipality of St. Clements; Citizen concerns, North Portage Development Corporation; Office of the Fire Commissioner; Citizen concerns, Town of Lac du Bonnet, Bulk Water Sales; Rural Municipality of Lac du Bonnet and Lake Manitoba Financial Assistance Program, parts C and D? Is that agreed? *[Agreed]*

With regard to the Auditor General's Report–Follow-up of Recommendations, dated May 2016, does the committee agree that we have completed consideration of the following sections: Citizen concerns, North Portage Development Corporation; Rural Municipality of Lac du Bonnet; and Provincial Nominee Program for Business? Is that agreed? *[Agreed]*

The remaining items on today's agenda, then, are Auditor General's Report–WRHA's Management of Risks Associated with End-user Devices, dated July 2015, and the Auditor General's Report–Follow-up of Recommendations, dated March 2017–the WRHA's Management of Risks Associated with End-user Devices. Are there any suggestions as to the order in which we should consider these items?

Mr. Reg Helwer (Brandon West): I would suggest that we consider them globally, so they–because they do relate to each other.

Mr. Chairperson: The suggestion has been that we will consider them globally. Is that agreed? *[Agreed]*

Now I'd like to invite the deputy minister to join us at the table. Thank you very much.

And, at this time, I'd like to invite the deputy minister to–sorry, the minister and the deputy minister to introduce their staff that they have with them today.

Hon. Kelvin Goertzen (Minister of Health, Seniors and Active Living): Mr. Chairperson, members of the committee, I'm pleased to welcome to the table aforementioned Deputy Minister of Health, Seniors and Active Living, Karen Herd and Perry Poulsen, our chief information officer, to take questions from the committee.

Mr. Chairperson: Thank you very much.

We will now proceed with the business of the committee.

Does the Auditor General have an opening statement?

Mr. Norm Ricard (Auditor General): Yes, I do. I would like to first introduce the staff member that I have with me today. With me to my left–to my right is Fraser McLean. He was not a principal at the time that we conducted the audit but is now my IT–audit–my director of IT, audit, security and operations.

***** (10:10)

Mr. Chair, the Manitoba health-care industry is increasingly relying on electronic records and automated processes. As end-user devices such as laptops, smartphones and flash drives become more and more powerful, their proliferation within the health-care system is understandable, but this proliferation increases the risk that health care information could be accessed by unauthorized individuals.

In conducting this audit, we wanted to know how vulnerable the Winnipeg Regional Health Authority was to confidential personal health information falling into the wrong hands. As such, we looked at whether the authority properly managed the risks associated with personal health information being stored on and accessed by end-user devices. We focused our efforts on assessing the adequacy of management policies and practices. We concluded that the authority was not properly identifying and managing these risks. As a consequence, there were significant cybersecurity control weaknesses. These weaknesses resulted in the authority being unnecessarily vulnerable to personal health information falling into the wrong hands.

Throughout our audit, we observed that the authority was focusing on ensuring compliance with The Personal Health Information Act. While PHIA does include some security requirements, compliance alone does not ensure strong cybersecurity. It is important that the authority implement a security program based on sound risk management. We believe that such a program would invariably ensure compliance with PHIA security requirements.

Mr. Chair, we also tried to understand what may have led to the authority's limited attention to end-user device, cybersecurity risks and controls. We observed that plans were not developed for how to manage the proliferation and use of end-user devices within the authority. Proper planning would require the assessment of significant risks and the development of needed strategies and controls to mitigate those risks. We also noted that security safeguard audits as required by the authority's own policy were not conducted. Such audits may have detected the control weaknesses we identified.

Our report includes 12 recommendations. In our March 2017 follow-up report, we note that one of these recommendations has been implemented. Our next follow-up will occur as at September 30th, 2017.

Mr. Chair, given the ubiquitous nature of end-user devices, these deficiencies may also be present in other Manitoba government organizations. We encourage all such organizations to consider the findings and recommendations outlined in this report. Thank you.

Mr. Chairperson: Thank you very much, Mr. Ricard.

Does the deputy minister wish to make an opening statement? Mrs. Herd?

Ms. Karen Herd (Deputy Minister of Health, Seniors and Active Living): I do.

Good morning, everyone.

In response to an incident where a laptop had been stolen on Health Sciences Centre premises, the Winnipeg Regional Health Authority informed the general public and contacted all individuals impacted by this incident. In response, the subsequent security audit conducted by the Auditor General, the department, Winnipeg Regional Health Authority and Manitoba eHealth collaboratively sought to address a series of gaps in both security awareness and training to prevent similar incidences from occurring.

Of the 12 recommendations indicated, 10 were deemed applicable to the Winnipeg Regional Health Authority and two applicable to Manitoba Health, Seniors and Active Living, the department.

The Auditor General's primary concern was the risk of storing and sharing personal health information using personal computers without appropriate controls to protect personal health information.

Since the report has been issued, work has been initiated to update policies and to also provide relevant and responsive privacy and security awareness tools for staff across the Winnipeg region, as well as other regional health authorities in Manitoba and across the department. The department is now focused on reviewing auditing practices and improving technical safeguards across the province's health-care system. This is complex work that will require multiple years to complete and will likely require additional investment to achieve over time.

The department currently permits external entities including hospitals, pharmacies, medical clinics and the First Nations Inuit health branch to access departmental health information systems for various purposes related to both the administrative and clinical provision of care to Manitobans. The department has a continuing obligation under The Personal Health Information Act, PHIA, and ministerial guidelines for records of user activity to audit, or require these entities to audit their systems' user accesses to ensure all accesses are for authorized purposes. To give you a sense of the scale, on a monthly basis, in excess of 2.5 million personal health records are accessed by stakeholders external to the department.

Auditing and review of this level of access is a resource-intensive activity and, as such, the department, in conjunction with Manitoba eHealth, is examining methods by which we verify and guarantee the safety and security of this information while also assisting users' compliance without negatively impacting the economy, efficient and effectiveness of our health-care system.

A proactive response includes both the development of direction and guidance as well as actively monitoring compliance, including examination for the potential establishment of an auditing service, supporting legislative requirements for all ICT-based systems within Manitoba. In direct support of this important need as well as in the interest of continuous and responsive improvement, The Personal Health Information Act requires that a comprehensive review of the act be undertaken. The intent of this review is to ensure that this important piece of legislation continues to appropriately balance the interests of patients and the needs of service providers. The department is currently conducting this review of PHIA, which includes inviting feedback on the act from the public and stakeholders in our health system. It is expected that this feedback will help refine the act and ensure it continues serving both the public interest and our health system. Thank you.

Mr. Chairperson: Thank you very much, Ms. Herd.

Before we proceed further, I'd like to inform those who are new to the committee of the process that is undertaken with regards to outstanding questions. At the end of every meeting, the research officer reviews Hansard for any outstanding questions that the witness commits to provide an answer for and we'll draft a questions-pending response document to send to the deputy minister. Upon receipt of the answers to those questions, the research officer then forwards the response to every PAC member and to every other member as recorded of attending the meeting.

At the next PAC meeting, the Chair then tables those responses for the record. Therefore, I am pleased to table the responses, provided by the deputy minister of Finance, to all the questions pending responses from the November 30th, 2016, meeting. These responses were previously forwarded to all members of the committee by the research officer.

Before we get into any questions, I'd like to remind members of the committee that questions of an administrative nature are placed to the deputy minister, and that policy questions will not be entertained or are better left for another forum. However, if there is a question that borders on policy and the minister would like to answer that, or the deputy minister wants to defer it to the minister to respond to, that is something that we would consider.

The floor is now open for questions.

Mr. Jim Maloway (Elmwood): Well, I guess I would have a question of the information officer and perhaps directly or through the minister. I'd like to know what the relationship is between his position and the BTT.

Mr. Perry Poulsen (Chief Information Officer, Manitoba eHealth): Sure. I can answer that. We have an arm's-length relationship with BTT. We are looking at significant changes that we want to start to collaborate a lot more than we've done in the past. Many of these issues that we're challenged with resolving or mitigating risks are common, and we think there's a great opportunity for us to work together.

Mr. Maloway: Now the BTT–under the BTT, there is a security apparatus in there that has, I think, worked very effectively in the past. Why have they not been more involved with your security issues? *[interjection]*

Mr. Chairperson: Mr. Poulsen.

Mr. Poulsen: Sorry. I would comment–I don't know the detail exactly of the challenges they have, but I would assume there is some commonality with the two-factor authentication and the products that we're using today to ensure the safety of the information that we manage today.

***** (10:20)

Mr. Maloway: Well, I guess my question is if you see opportunities to improve your security and these are the recognized experts in the field, then, why wouldn't there be more consultation as to how to solve and deal with the problem on a, you know, daily basis?

Mr. Poulsen: So there has been collaboration. I will–I'll go back to the commonality, and I know we could assume that they're an expert, but I still would agree that we all have common issues that we need to resolve. The review of what we share, there's some infrastructure changes of what network we run on, et cetera, that are quite technical on how we manage some of those risks together. They take significant efforts for us to pull those services together to make them, I'll say, one, if that makes sense.

Mr. Maloway: So are you suggesting or telling us now that you are co-operating with them on a more involved way than you were in the past?

Mr. Poulsen: We are in regular conversations with BTT today.

Mr. James Teitsma (Radisson): I'm just continuing on along the same lines as the question from the previous member.

Is there any consultations or co-operations that have been occurring with other eHealth departments in other provinces such as Saskatchewan?

Mr. Poulsen: There certainly is. We are very close with Saskatchewan and their eHealth counterparts. We, in fact, share our enterprise architecture and the common vendors that we look to for resolving some of these issues and implementation, such as FairWarning, which is one of the auditing products, the RSA tokens, the two-factor authentication. We do that across both jurisdictions.

Mr. Teitsma: I noticed that the personal health information regulation section 8.1 requires an audit of security safeguards to be conducted every–at least every two years. When was that last audit conducted, and what were the results?

Mr. Poulsen: I don't have that date right now.

We are doing–as a result of the audit, we are doing an ongoing threat-risk assessment that we've been rolling through with a number of internal audits, and we've actually had an external auditor come in to take a look at what we could do. These are the–out of–based on those findings, that's what we're actually building our plans to mitigate those risks around.

Mr. Teitsma: Which external auditor did you choose? *[interjection]*

Mr. Chairperson: Mr. Poulsen.

Sorry, can you repeat that? I don't think we caught that on record.

Mr. Poulsen: Sorry, I don't recall the vendor's name.

Mr. Chairperson: Okay.

If I can just ask for members of the committee, for witnesses as well, please indicate if you are wishing to speak, very clearly, so that I can make sure that we capture the information on Hansard and we can identify you correctly.

Mr. Teitsma: So you mentioned that in response to the–to an audit, you were engaged in some work, you mean in response to the Auditor General's report or in response to your own internal–the one that's required every two years under PHIA?

Mr. Poulsen: That would be both.

Mr. Teitsma: And, in terms of the nature of the threat assessments and the vulnerability assessments that you're doing, are you doing any testing to discover the effectiveness, shall we say, of the mechanisms and the training that you are putting in place? So an example of a simple test might be to have malware embedded on–or, not really malware, just pretend malware, embedded on some USBs and scattered on the WRHA parking lots and see how many end up in managed devices and the like.

Mr. Poulsen: So we've already acted on the USB, so if you plugged a USB port into a computer today, it would immediately be scanned prior to accessing any files that were on there. We're not really thinking that's the end state, and certainly we want to encourage–and we've taken every opportunity to have people not use a secure USB card as well. We've also got Dell SecureWorks that does penetration testing with us on a biannual basis.

Mr. Teitsma: So, just to be clear, on the USB sticks, you are still allowing unencrypted USB access in your managed devices or are you not? I was quite not clear.

Mr. Poulsen: The end state would be for us to disable the USB ports in total, and that would in–either be through two methods: one, you plug it in, it would instantly encrypt and secure that non-secure device. It's in the plans.

Mr. Helwer: I'm not sure if the deputy can answer this but if you were not an end-user, if you are a patient, for instance, how would you best access your health records? Is it through your health-care provider, or is there another way that citizens can access their information?

Ms. Herd: Currently, today, if people want to access their records, they can send a request to eChart to view their records, but there are many activities under way across the country to be able to access or for patients to have a greater role in their health-care services. So we've seen projects in some other jurisdictions funded through Canada Health Infoway and other partners, where people begin to be able to book appointments online, that they are also able to access tests online–test results online.

So there's a lot of things happening across the country and across the globe in terms of greater involvement of the patient in their medical journey.

Mr. Helwer: So does that, then, add to the complexity of security, or is it all-encompassing and opening your system essentially to individuals? I assume we'll have to have passwords and that type of thing. But that does have another security risk.

Ms. Herd: I would say that it's–it is a constant challenge, but it is the way that Manitobans and others across the globe will–are expecting to access their health care into the future. So it's–it is a complexity, but it is something that we have to deal with. I think the challenge that this particular audit highlights is that the provision of health information to physicians and to other caregivers and to the public can only benefit them, but it's that tension between protecting the information from others who should not see it while being flexible enough that we allow health-care providers and the public to access their information.

So I'd say it's no different than you see in other domains. Cybersecurity is an ever-involving–evolving and increasing challenge for organizations to deal with and, really, the Winnipeg region and the department is no different.

Mr. Helwer: So the unique information is required to be secure from the patient side, but there's also a movement to open data, where the aggregate data is more accessible by the public at large. And is that something that the department's looking at in terms of budget access or health data on a whole? Is that something that could be available or any interest in at all?

Ms. Herd: The department has recognized that this thirst for access to the information is a challenge that we will have to address and deal with. A couple of years ago, we implemented an information management and analytics study, where we grappled with these very issues of how to ensure that information is available for evidence, informed decision makers–making, by both clinicians and patients, but also how to ensure that we do safeguard information.

So they've–the review is now completed, and there's a plethora of things that we could focus on. But, I think, at the moment, it's trying to ensure that we find the balance, especially for clinicians, that we don't make it too onerous for them to access health records. Because our experience has been if we make it too onerous, people, especially younger people, find ways to work around the technology.

***** (10:30)

So I think we're trying to find a sweet spot between making technology accessible to people for decision making but securing it to the greatest extent we can. We've observed cases where, if the password is too onerous for, say, a young resident in the emergency department, they may take their cellphone and take a picture of something and send it. So we don't–we want to try to stop those things from happening, so it's finding the sweet spot that does not make things too onerous, especially for younger people that are more versed in the technology.

Mr. Maloway: The last time I had a briefing with BTT was a couple of years ago, and it seemed to me that they said that they had the capabilities of having sort of remote usage in their system for government employees, but it was the government itself that was refusing to allow them to–the idea was that the employees were going to be able to work from home. And it's the government itself that said, no, we'd like to keep you working out of your offices. So, if that's the case then, presumably, they have the security issues worked out, as far as the core government is concerned. So, then, why would this–why would the e-help people end up having all these vulnerabilities when the other core people don't seem to have the same vulnerabilities?

Ms. Herd: I, too, have VPN access, and it does require the use of a token and a significant password to access information.

And, to my earlier point, the challenge that we sometimes see, especially with clinicians in high-paced environments such as an emergency department, is if you go beyond, say, six digits of a password, oftentimes it prompts clinicians and others to find workarounds to the system. So I think we want to–it's not that these technologies are not known to eHealth; it's finding the way that brings users along, and oftentimes we have to recall that some of these users are not direct employees of the system. They may be fee-for-service physicians that often are working in facilities but are not under the direct employment of facilities.

Mr. Teitsma: Just continuing along, I mean, the lines of what you're talking about is actually usability versus security, right, and some of the challenges there. I know that there's some advances being made in this regard in a variety of contexts. I think of some US-based hospitals of–that I'm aware of that have, as an example, each employee has a card that they carry and they go to a computer that says, I'm in room 1701, right, bed No. 8, and they say, oh, you're the doctor. So you're allowed to access all this information, you're in the room, so here's this patient's information. And, really, from a usability perspective, it comes up instantaneously. And there's no password, right, because there's a physical security component. So that's not been given to those kind of improvements.

Mr. Poulsen: We have implemented that technology and it's–it actually still is two-factor authentication. The card is the tap-on; just to give you–the problem we're trying to solve is for a physician to log in in emergency takes around 90 seconds. The ability for us to tap and put in something, you know, like a six-PIN password, is what they've got today and, in fact, that session following that you described we've got in most facilities within the WRHA today.

Mr. Teitsma: That's good to hear. Part of what the Auditor General's report talked about was the differentiation between the managed devices and the unmanaged devices and the challenges that you face there. What kind of controls do you have around unmanaged devices? What kind of records are we keeping so that we know how many we have and where they are?

Mr. Poulsen: A lot of what we're talking about today, although we have controls, people carry a number of devices that I'll say are considered personal. What we really need to do is to get people to drive to the technologies that we actually manage, so we talk about managed services.

So we do have managed services. What the challenge is for us is to get people to adopt those managed services and leave the personal device behind, and that allows us to put in controls like a six PIN password, 10-try wipe, and it's very difficult for us to get a non-employee to actually adopt those technologies. And the approach we've taken really is around training and education.

Mr. Teitsma: My personal belief is that that's wrong-headed. I'm pretty sure that you're not going to get success in that regard because the whole industry is moving towards being able to bring your own device. So managing these diversity of devices or providing secure access would be better, I think.

Now, so do you have a list, you know, or an inventory of the unmanaged devices? Do you know who has them and what kind of device they are and how many there are? And do we have that information?

Mr. Chairperson: I just want to indicate, and I know this is sometimes a challenge in a committee room like this, where, you know, there's a conversation at the end of the table, so to speak, rather than through the Chair. And just in terms of communicating and allowing everyone to hear, if I could just encourage everyone to direct your comments towards the Chair, at least, so that we can hear everybody.

Mr. Poulsen–oh, I'm sorry. You know what? There's been a request to repeat the question. Could you just quickly repeat the question, Mr. Teitsma?

Mr. Teitsma: Just getting back to that first question: What kind of inventory controls and what do–you know, is there a list of unmanaged devices, who has them, what kind of device there are–they are?

Mr. Poulsen: So we manage all devices at a certain level. The appreciation of the audit actually indicated where we weren't managing them to the appropriate level.

When I talk about unmanaged services and–for lack of better words–our frustration is when somebody uses a Gmail account. So when I talk about education and telling people to use the appropriate services that are secure, encrypted, on a network that actually has some management, that's where the challenge that we have is ahead of us.

Mr. Maloway: So the–I guess the whole area of electronic health records is, you know, nothing new about that. It's been around for probably since Filmon government days with the eHealth program they had, but it's certainly advanced in the United States because of, you know, legal liability issues and stuff like that. They've got a–systems in place that–probably way ahead of us.

The vendors selling in there are probably, my guess is, vendors selling here, and I don't know how many, you know, different vendors there are and how many platforms there are, but the question is: Is this an implementation problem or is this a software problem that we're dealing with here?

Ms. Herd: I'd say that it's definitely been a journey. If we look at how this technology started, it was often with individual hospitals or individual community programs. Through the time of regionalization, the technology then began to become more streamlined to one particular regional health authority. It's only in more recent years–I'd say from 2012 onward–that a lot of the provincial strategy and approach came to be we're going to look at provincial solutions, provincial technology solutions that will be implemented across the province in a more provincial approach.

So I'd say it's part of the evolutionary journey we're on that right now we're in a time where individual physician offices or individual facilities or clinics are still using some of their own technology or initially purchased technology. And when we begin to implement large-scale projects, we come at it with a provincial solution.

***** (10:40)

So, as an example, the emergency department information system, that was something that originally began in large Winnipeg hospitals, it's now in the process of being rolled out to major provincial hospitals, but the same technology. So that over time, somebody, say, as an example, in Churchill, who has an accident or has an injury, their diagnostic imaging results could be viewable to somebody in Churchill, even though the results may have been taken in Winnipeg.

So that's the goal, but we're certainly not there on a provincial basis, so that's some of the challenge that we're currently in.

Mr. Maloway: So, I guess, the question I have is this: like, for example, that a number of years ago the central government decided to pick SAP as their vendor. There had never been a government anywhere that was on SAP. They're basically–they do pulp mills and stuff like that. They're from Germany. Manitoba was the first government to do this. And, presumably, they put more governments on the system. But what that did was when they ran SAP, they had to get rid of all these old legacy systems that were basically collapsing on their own, anyway. I'm sure there were some systems that did work with it.

Is that the same system here in the health-care field? Is there, like, a series of one or two vendors that you have to deal with, or is it just a big mess where there's multiple vendors in each jurisdiction that are trying to sell a product?

Ms. Herd: I would say, candidly, it's a bit of both.

If we look at financial systems, yes, the health system has moved to SAP in Winnipeg. That meant convincing independent organizations such as St. Boniface hospital to agree to come on board with a regional solution. But you may have private personal-care homes that have different financial systems.

So it's a case where, over time, we tried to convince people that participate in the provincial system to see the merits of collaborating to try to advance provincial systems because we know that patients move across various regional boundaries or various hospital boundaries, and it's advantageous from a safety perspective for them to have records accessible. I will say, though, it remains a challenge with individual physician offices and systems because they are independent businesses that may not always want to move their office functions to a uniform technology. And, oftentimes, those decisions aren't made until they're at a point in their office functioning that they need to replace systems. So there probably is never a time when everything can be changed at the same time to a uniform system. It is more an evolutionary process.

Mr. Maloway: I don't really get why this is such a big problem. I mean, I know in Nova Scotia SAP, they saved a ton of money by having the–I think the big hospital in Halifax and the government of Nova Scotia and I think a municipality, all sign on, and they save money by doing that.

And here we have in Manitoba, City of Winnipeg, you know, went, I think, with Oracle. So I don't see how we're going to have any, you know, efficiencies if we have people just going with totally different systems. And particularly with the government, I mean, government funds these operations. So what do you mean, there's an argument about one hospital wants to go with some other system? I mean, you're paying for it; why don't you just simply say, look, you–we're on SAP, you'll have to be on there too?

Ms. Herd: I would say in the area of SAP, the province, yes, as you've indicated, uses SAP as does the Winnipeg region and Hydro.

For organizations that do use SAP, we have to try to work in a collaborative way, in terms of how we can advance the use, how we can support the system in a more co-ordinated way. We've had discussions with organizations such as Diagnostic Services of Manitoba or other regional health authorities about how the investment can be leveraged.

I would say, though, the challenge in Winnipeg has been that we do have independent board-governed hospitals, and we've chosen to take the approach, for better or worse, that we would like the organization to see the benefits and sign on, and we are happy to say that in Winnipeg, those independent hospitals–independently board-governed hospitals have signed onto the project. But again, I'd say it's a realization to those organizations that they have to give up some control over things in order to benefit from a shared solution.

So I think we've not taken a heavy-handed approach, but we've instead tried to get them to see the merits of moving forward in a way to invest in technology that they probably couldn't afford to do individually.

Mr. Maloway: Does SAP have a suite of health-care modules or is it something that they would be considering developing or are you stuck with vendors that just specialize in health care?

Ms. Herd: We use SAP for our administrative functions, finance and administration, payroll, HR, but we in the department have partnered with Manitoba Blue Cross on the medical claims system, which is how we pay physicians in this province and conceivably could use that system, which has now completed development, for the payment of other claims that we have that we offer as insured benefits.

So that's one area where SAP has been quite effective for us. We've been very happy with the physician payment system, as, I believe, has Blue Cross been on their claims payment system.

There are other lines of business, though, that SAP is not in, that oftentimes in the health system we need to use other technology. And the other point I'd make is that in some areas, the IT system is so closely integrated to the machines now, so as an example, linear accelerators, CTs or MRs, that there's different vendors that have niche markets. So the point we need to ensure is that because there's never going to be a scenario where the–there's only one solution available, we have to ensure that more organizations support a common technology so that we're not building interfaces with a half dozen different financial systems. In a scenario, we'd only want to build the interface once with SAP between that and a surgical information-management system.

So that's one of the reasons why we try to advocate that organizations should try to move to the provincial solution for things so that the amount of interfaces that we have to build is minimized.

Mr. Maloway: And, of course, the time to do that is when your legacy system is collapsing, right, which I assume a lot of them are, so, I mean, you just simply offer them the solution to their ongoing problem. The problem is, if they buy a new system and they implement it, and they're only, like, a couple years into their implementation, how are you supposed to now tell them, well, we want you to go to a different system? Which you're going to have to have some more consistency in your approach here, I would think, but that's a ministerial responsibility, so.

Ms. Herd: That's one of the reasons why, at the same time–or I guess a year prior to doing the information-management and analytics study, we also did an information and communication technology study, which is to try to assess the hot spots that exist across the province in terms of end-of-life technology to try to identify–as you can imagine, there's many more things we could invest in than we have resources available to do where ICT is involved, so it's to try to identify the areas of highest priority for investment, just as you say, for things that are at end of life or at higher risk of failing.

***** (10:50)

Mr. James Allum (Fort Garry-Riverview): I welcome the deputy and Mr. Poulsen to the table today.

In your opening–in the deputy's opening statement, talked about the considerable resources and investments that are required. So could you take us through the kinds of dollars that we're talking about, over how many years and whether these have been earmarked by the department to date?

Ms. Herd: Okay. So every year we have an annual allocation of $40 million for ICT investment and that's a static amount, year to year, but what we try to ensure is that the ICT planning that happens priorizes within that $40-million allocation.

So, for example, there's a proportion of that money that's used to refresh existing infrastructure. There's a proportion that's used to invest in new technology. For example, last year we used some of it to look at a consumer health strategy, which is that focus of getting consumers easier access to health information that they can use to manage their own health needs. So it's all within that annual allocation of $40 million, but that's how we priorize within it. Every year can vary.

Mr. Allum: I appreciate that. One would think–one knows that it's a–these are national problems. Government has yet to sign on to the Health Accord, but is the federal government a player in any way, shape, or form in helping to either finance these issues or help to bring common solutions across the country?

Ms. Herd: Yes. There's a pan-Canadian organization called Canada Health Infoway that is funded by the federal government, and in its first 10 years of existence the premise that it generally used is that it would provide 50 per cent of the funding for projects. And provinces and territories would have to match the other 50 per cent cost.

So, as an example, we implemented a radiology information system and diagnostic imaging digital imaging as part of the Infoway investment in some other provinces that weren't as advanced on drug programs. Over the years they've moved forward with drug information systems in those provinces, and so Canada Health Infoway, which is fully funded by the federal government, does work on a pan-Canadian basis to try to even advance the concept of intraoperability across provinces and territories. So that, for example, if somebody in BC in a skiing accident needed to access health information in Manitoba, that was the ultimate goal of Infoway.

I'd say it's not been fully successful from a pan-Canadian basis but there are examples where you've seen provinces and territories support common technology for things like public health information systems, called Panorama. Right now, Canada Health Infoway is focused on a e-prescribing option that they're piloting or moving forward in a pilot phase with Alberta, Ontario and probably Nova Scotia next, so they do try to advance things on a pan-Canadian basis.

Mr. Allum: Thank you for that. I just–quickly, for the Auditor General, the deputy identified the $40 million a year is generally allotted for the issues that we're discussing.

From the Auditor General's point of view, is that a sufficient amount of investment, or is more required or less or how does the Auditor General view the amount of dollars being invested into the system?

Mr. Ricard: The amount of dollars is really a policy issue and it's not an area that I can–the adequacy of that is not an area that I can opine on.

Mr. Allum: Well, if the Auditor General and the staff do an evaluation of the practices and policies and other elements that go into designing this work, and so you have opinions about the process but not about the dollars? If there weren't sufficient dollars, would you say so?

Mr. Ricard: We would be looking at–for example, we would look at the processes the department uses to allocate the $40 million. We'd look to see if they had proper risk-based processes or proper ways of prioritizing their projects, but the determination of the amount, whether, you know, is $40 million enough, is $60 million enough, is $20 million enough, is $100 million enough, we would not comment on that. We would look at, for the amount that is allocated, how is it being expended? Are they getting the most possible value for the $40 million? So that's what the focus of an audit on the $40 million would be, as opposed to it's not enough or it's too much.

Mr. Maloway: Thank you, Mr. Chair.

Before there was BTT, there was OIT, which was essentially the same thing, and they were instructed by the government to, where possible, avoid the huge costs of developing, you know, software from the ground up, because, you know, certain companies love to do that, and–where you'd have a different program in every different province to develop an exchange system.

And it worked out okay, but a lot of times it ran into trouble with the legislation in a given province and with the department of the government in that province, too, because the bureaucrats in the department always want to develop their own program because they're special. They want it to be different, unique system in the world. And so the government had to order them to go with a standard system. And I remember, on securities commission perhaps, that they–that we were offered it free by Alberta or BC, and they didn't want it. They wanted their own system because it's got its Manitoba stamp on it.

What is the situation, right now, with sharing, like, taking software programs in this Infoway–Canada Health Infoway or any other part of your daily lives? Is there any sharing going on? Or is there still that resistance to not share?

Ms. Herd: I think I can safely say that we don't develop major systems in the province. Manitoba is too small a province, in terms of population, to drive that kind of in-province development.

We would normally purchase world-class systems through a process where we would require what it is we need, we assemble our requirements, we go to the market to have organizations that already develop software come and bid on that, offer that service along with an implementer. That's the normal practice that we use. I would say on–potentially on smaller organizations, maybe like some physician offices that run as independent offices, they may choose to do things that we would not really have a say in. Some may buy out-of-the-box solutions. Others may develop things in-house. That's a bit of an unknown to us because, again, they're running as independent clinics, but our general principle is that we would always purchase following a requirements-identification process and then a selection process. And that's–I would say even this recent experience with Canada Health Infoway on e-prescribing, they went out to the market to find a provider who would offer that. They weren't developing in-house e-prescribing.

Mr. Maloway: So examples like in the old Filmon government, where they spent, like, $50 million developing the eHealth program–there was a number of other programs at the time–you're saying these are pretty much nonexistent now as far as Manitoba's concerned?

***** (11:00)

Ms. Herd: Sorry. I believe that was SmartHealth and, no, we do not develop in-house. It would be very rare. I mean, if I think of our Drug Program Information system, that's quite an old system now. It was one of the first in Canada that was developed. At that time, it was developed in-house, that's in the circa 1970s-'80s, because there weren't as many packaged solutions that you could go to the market to buy. When the time comes that we will replace that, we would look for a system that's already developed that could meet our requirements. And I think we recognize that these systems that you're buying may never meet all your requirements that you need, but you have to find the one that's the closest fit. It's just too cost-exorbitant to build and develop in-house.

Mr. Teitsma: Section 4.4 of the personal health information regulation requires audits of user activity to determine security breaches. Can you maybe just describe how that's being done and how live the audits are in terms of detecting inappropriate access?

Mr. Poulsen: There's two factors there. One is that we do real time through Dell SecureWorks for anybody trying to penetrate, so if you'll look at it as security. On the other side, for access to patient records, we do have proactive auditing happening where we have a number of samples that we do, and this is quite manual and intensive work that we do, specifically around the systems that we've implemented. We are looking at automating that process with the understanding that the majority of the data that we capture today is not about patient information, it's really about who accessed what record. And it's important to remember, although we look at something that looks suspicious, it doesn't mean in every time everybody is guilty. And what we look for is certain things that match, like a last name of an individual looking at a family member and things like that. Those rules are established.

Mr. Teitsma: Those–and those kinds of rules or those, where you're, say, finding somebody accessing a family member, is that a live monitoring or is that as a result of a later audit?

Mr. Poulsen: There's a little bit of both in the sense that, in particular, with eChart, we do actually have some automation happening. In others, some of the–typical in health care, some of the systems and the applications that we have, although they're world-class enterprise systems, they lend themselves to quite complex back ends required to actually do the automation. And there is an investment for us to make that automated.

Mr. Teitsma: Can you describe the procedures that you have around managing reports of stolen or lost equipment, whether that's a fully managed device or one of these bring-your-own-to-work kind of things, what does a user–what's a user's obligation, and then–and how does it flow after that?

Mr. Poulsen: The audit initiated of a stolen laptop was actually somebody who sat down and did entry into a PC. They copied and typed into a PC. It had no controls. It wasn't a managed–typically what we would consider a managed device.

I think the important thing to remember is for–going to your question around reporting, we do have a process and a policy for reported and stolen devices. I think the other part of a managed device is that, in most cases, there is no patient data on an end-user device. It's back on a mainframe. And people are typically viewing into a mainframe. Saying that, on a managed device, it won't allow you to access or log on to that machine; it would force the–whoever stole that device to really re-image that device if they wanted to use it again.

Mr. Helwer: Most of government has moved to a BYOD or bring your own device, and it enables connection to the network for email and that type of thing, but as these end-user devices, smartphones have become more powerful; it creates a bit of a problem. You may have somebody that snaps a picture of an X-ray or of a scan and sends it to a colleague to get immediate consult-type thing, which is great for the health-care system, but on the flip side if it's not through an encrypted system, it creates problems.

So is it an education process that you have to move forward on that or how do you see the department dealing with those issues?

Ms. Herd: Education is a huge part of it, and if I think of the example that Perry had cited about the medical student or resident who had her laptop stolen, we have to ensure the conditions exist that people are not afraid to bring those cases forward because we need to be able to respond to that breach in a way that's needed. But we can't make it so punitive that people then become afraid when it's an unmanaged device to report it. In this case it was a resident who had a personal laptop that had input information into it that wouldn't have been a normal scenario envisioned.

On the issue with people with cellphones or smartphones taking pictures, the other challenge that we try to educate about is that if they–if the residents or others do it very quickly to help in a diagnosis, that workaround actually leaves information out of the patient's record that could also pose a safety–the health and safety risk to the patient.

So it is through education. The challenge I'd say is that at times you're not always dealing with your own employees. At times they may view themselves as independent fee-for-service physicians. So it's trying to meet people where they're at and bring them into a greater understanding of the risks that they're causing by working outside of the managed environment.

Ms. Janice Morley-Lecomte (Seine River): With these gaps that are created, how are you addressing these gaps so that they don't exist or to as great an extent?

Mr. Poulsen: The–there are two sides to that, and one is the enhancing and more efficiency in dealing with patient issues. We are looking at technology such as extending the Telehealth program to actually anything that would be related to a patient, that information would be captured and become part of the patient record.

Other ones that we're looking at are with the–with secure messaging, as well, with the understanding that that's a safer way, and getting physicians and clinicians to actually leverage a system that's much more secure than just over public services.

Ms. Judy Klassen (Kewatinook): Previously, you mentioned Churchill being able to access something in Winnipeg. I believe Churchill is part of the WRHA, so I'm wondering for an area such as Thompson or other hospitals that we have access to in the North is there that sharing ability? And if the best practices in learning so far if there have been a way that they're shared with other regions and, if not, what is the timeline for doing so?

Mr. Poulsen: We, Manitoba eHealth, although we're administratively housed under the WRHA, do work across all the RHAs, including Thompson and every other regional health authority. The policies that we implement and the concept of the journey was that we would get to one system, one network. In there those controls, those policies and going back to the systems that we invested in, those systems we're going to purchase once and we're going to deliver across the province. And really what we offer is the interoperability across the province of Manitoba.

Ms. Klassen: So what is the timeline for doing so?

***** (11:10)

Ms. Herd: I'd say that we generally look at it by system so picture archiving and digital imaging so that's the example I was citing in Churchill. So that is–predominantly exists across the province already. Emergency Department Information System, that exists in Winnipeg; and the rollout, it has now happened to larger rural hospitals across the province. We tend to do it by the software solution that we've procured and the plan for rolling it out.

So I can't say that we have a timeline in total for every solution, because some haven't yet been procured as a provincial solution, but generally the principle that we try to follow now is that we're identifying what is needed on a provincial solution–that's what's taken into account in the selection process–and then an implementation plan exists to roll it out on a provincial basis. So each significant software investment in, say, surgery or internal medicine, cardiology, cancer even, those things are taken with that provincial approach.

Mr. Teitsma: In one of his–the previous responses, I believe Mr. Poulsen talked about a mainframe. So that brought me back to when I was studying computer science many decades ago at the University of Manitoba, and it kind of made me wonder in terms of the age of the technology and the nature of the technology that is back ending some of these systems. Can you maybe talk about where that's at?

Mr. Vice-Chairperson in the Chair

Ms. Herd: Well, it's–I'd say it's in varying stages. So, as an example, when the Province moved to SAP for administration and finance as part of its Y2K project, a significant portion of funding, which sits in the Health Services Insurance Fund was not moved into SAP. That project only happened a couple of years ago. Some of the legacy systems that have existed on mainframes are things like the medical claims system. That was a circa 1970s system that we only replaced within the past two years.

The next sort of long-standing legacy mainframe system that exists is the drug program information system. But as we contemplate moving forward with an improvement like that, which is a huge investment, we are also contemplating doing that investment for the Pharmacare program, which is what DPIN is used for, but also for how drugs are managed within CancerCare, within the regional health authority system, so that we'll try to find one drug solution–drug-system solution that could be–serve multiple purposes. So that's how our planning occurs.

Mr. Teitsma: All right. Just, again, getting back to the personal health information regulation, it is requiring you to take precautions to protect the information from disasters, if I can bucket all those things together, fire, theft, vandalism, et cetera, what kind of disaster recovery program, then, do we have, because I imagine that would be a challenge in the context of the kind of hardware that you're describing.

Mr. Poulsen: So, as Karen mentioned, there are some legacy systems that still do not lend themselves easily to the newer technologies. Health care tends to lack–lag the rest of the technologies like banking industries, et cetera. But for a majority of our services that we provide today, they're what–on an environment they call virtual servers, so in that virtual servers, it allows us to actually–if a server fails, it automatically fails over.

We've got a number of services in play where we've got the network backed up over a tricord through the managed services through BTT, for example. We've got a data centre, and, in fact, one of the opportunities we're looking at with BTT is leveraging a secondary data centre. So although we have ability to fail over within our facility, St. Boniface to HSC, HSC to Air Canada, Air Canada has a significant amount of investment in servers and services and networks. It's a level–*[interjection]*–the Air Canada Building is really a very secure building with a lot of redundancy in it, and we purposely picked that building to provide those services today.

Ms. Morley-Lecomte: With the managed devices that you would use through health and the safety of these devices, how would you be able to stop that device from being activated by a hacker if it should get into the hands of a hacker?

Mr. Poulsen: I think there's always going to be the opportunity for a hacker. The technology that is being developed today–just out in the cloud and on the Internet, we've got a lot of things to be aware of. The Internet of things–we mentioned memory sticks before; we've got–and in that sense, I can appreciate the audit because I think for all of us, we need to be aware of what those threats might be and it's actually forced us to look at things like cybersecurity insurance and things that we haven't really looked at before. The managed device–it's intended, if somebody tries to get onto that device, after 10 tries that device wipes itself out. That's not to say I could ever give a guarantee, and I could never give a guarantee, that something cannot be accessible.

Mr. Chairperson in the Chair

Ms. Morley-Lecomte: So, if someone were–and hackers are very smart individuals, if they were able to then get into the device before the five times, is there a secondary 'stopmet' to the individual?

Mr. Poulsen: I think the concept of us not having anything resident on that device would mean they'd have access to, if they did take pictures, and the likelihood of that being something that they could manipulate or understand what they're looking at, I guess that risk is there.

Ms. Morley-Lecomte: So, if that risk is there, have you been able to or have you looked into the cybersecurity technology to sort of stop that?

Mr. Poulsen: We are having those discussions with BTT and the investment required, and it's mobile-device management. It's an application or there's a number of applications. Some are better than others, some are more expensive than others, and we are actively looking at what that might look like for us to improve over the services we provide today.

Mr. Chairperson: Mr. Johnston.

Mr. Scott Johnston (St. James): Oh, I guess I put my hand up in the air. Well, okay, well, you've got me, Mr. Chairman. Don't scratch your head, all right?

Thank you, Mr. Chairman. I did–I was curious about one thing, is–do you have different categories of confidentiality of patients' care?

Ms. Herd: I'd say that's really an area of work in progress. There are certain things that we're examining in terms of differing levels of classification, but it's not in widespread use at the current time in a systematic way. I'd say in some–with respect to patient care, I'd say in some other areas with respect to financial and administrative systems, there's differing levels of access with information systems used for, say, research purposes like, for example, when we send information out to the Manitoba centre for health policy, there's–that data is de-anonymized–or, sorry, is anonymized. So I'd say in differing data sets and for differing purposes, there's differing levels of access, but in the clinical realm, that's still area that we have to do some improved–some additional work in.

***** (11:20)

Mr. Johnston: Would you anticipate, by creating more categories, et cetera, that it would be very difficult to effectively manage?

Ms. Herd: Part of the challenge in the environment we're in is that care is moving to multidisciplinary teams, so there may be very valid reasons why people beyond the physician or beyond the nurse level need to have access to the data. And as we increase the number of health-care providers that are fundamentally involved in the patient's care, including the patient and potentially their family, that's what adds to the complexity of trying to find standard rules of controlling access. So that's some of the dilemma that we found as we try to operationalize recommendations to look at differing levels of security.

Mr. Johnston: Final question is in regards to staffing upgrades in regards to this whole issue. What mechanisms do you have in place right now where you're continuing to upgrade your staff in meeting the challenges of changing technology and this whole evolving arena?

Ms. Herd: We have differing levels of training, so if you're talking about the awareness and understanding of The Personal Health Information Act and the requirements for clinicians and others in the system to follow and abide by PHIA, there's ongoing training that happens, and it's refreshed, for example, in the WRHA, on a three-year basis. Clinicians and others have to take that PHIA training.

If you're referring to the capacity within the ICT sector, to provide services, we usually go with a combination of in-house staff that moves forward on projects, but we also procure outside assistance as we're implementing projects so that we're aware of, like, the leading technology and skill set that exist across the country and across the globe.

Mr. Helwer: Question to the Auditor General. I assume, then, you have a follow-up to this report as well that you'll be maybe in progress now, and the department has gone through several scenarios. They're working with something that obviously moves all the time with new technology, and many of them are a work in progress. Are you comfortable with the progress that the department has been making on your recommendations?

Mr. Ricard: Well, today, we've conducted one follow-up, and that was as at September 30th, 2016, and so, one of the recommendations of the 12 that we had has been implemented.

I really can't comment on the progress that has been made since then. Our next follow-up will be scheduled as at September 30th, 2017, and so we'll see, you know, what progress is made until then. And some of these recommendations are complex and time-consuming, so we expected, I think, in all fairness, that it would take at least two years to get through the bulk of them.

Mr. Chairperson: Seeing no further questions from the committee, I will call the question.

Auditor General's Report–WRHA's Management of Risks Associated with End-user Devices, dated July 2015–pass.

Does the committee agree that we have completed consideration of the WRHA's Management of Risks Associated with End-user Devices of the Auditor General's Report–Follow-up of Recommendations, dated March 2017? *[Agreed]*

This concludes the business before us.

Before we rise, appreciate if members would leave behind any unused copies of the report so that we can use them at the next meeting.

The hour being 11:24, what is the will of the committee?

An Honourable Member: Committee rise.

Mr. Chairperson: Committee rise.

COMMITTEE ROSE AT: *11:24 p.m.*

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

http://www.gov.mb.ca/legislature/hansard/hansard.html