HANSARD

NOVA SCOTIA HOUSE OF ASSEMBLY

COMMITTEE

ON

PUBLIC ACCOUNTS

Wednesday, April 17, 2013

LEGISLATIVE CHAMBER

Personal Health Information Systems

Printed and Published by Nova Scotia Hansard Reporting Services

Public Accounts Committee

Hon. Keith Colwell, Chairman
Mr. Howard Epstein, Vice-Chairman
Mr. Clarrie MacKinnon
Mr. Gary Ramey
Mr. Mat Whynott
Mr. Brian Skabar
Mr. Andrew Younger
Mr. Chuck Porter
Mr. Allan MacMaster

[Mr. Jim Boudreau replaced Mr. Clarrie MacKinnon for the first portion]
[Hon. Graham Steele replaced Mr. Mat Whynott]
[Mr. Gary Burrill replaced Mr. Brian Skabar]
[Ms. Kelly Regan replaced Mr. Andrew Younger]
[Hon. Christopher d'Entremont replaced Mr. Allan MacMaster]

In Attendance:

Mrs. Darlene Henry
Legislative Committee Clerk

Mr. Jacques Lapointe
Auditor General

Ms. Janet White
Audit Principal

Mr. Gordon Hebb
Chief Legislative Counsel

WITNESSES

Capital District Health Authority

Ms. Chris Power,
President and CEO

Ms. Shauna McMahon,
Director of Technology and Infrastructure Renewal

Ms. Catherine Gaulton,
Vice-President of Performance Excellence & General Counsel

IWK Health Centre

Ms. Anne McGuire,
President and CEO

Ms. Ferne Mardlin-Smith,
Senior Advisor of Information Management

Mr. Marc LeBlanc,
Executive Director, Health Information Technology Services

House of Assembly
Nova Scotia

HALIFAX, WEDNESDAY, APRIL 17, 2013

STANDING COMMITTEE ON PUBLIC ACCOUNTS

9:00 A.M.

CHAIRMAN
Hon. Keith Colwell

VICE-CHAIRMAN
Mr. Howard Epstein

MR. CHAIRMAN: Good morning, I'd like to bring the meeting to order. Just before we start I would like to remind everyone to make sure that your cellphones are either turned off, or on vibrate, or silent, and with that, I would like to start with the introductions.

[The committee members and witnesses introduced themselves.]

MR. CHAIRMAN: Good morning, I'm Keith Colwell, chairman of the committee, and I'd like to start with Ms. McGuire to make a presentation.

MS. ANNE MCGUIRE: Thank you, and good morning, Mr. Chairman, members. Thank you for inviting us to be here this morning. I'm pleased to be joined by two of my colleagues today, whom you've just met, Ferne Mardlin-Smith and Marc LeBlanc.

Ferne is Security Advisor, Information Management with the Department of Health and Wellness and, prior to her recent secondment to the Department of Health and Wellness, Ferne held the position of Director of Information Management, Information Technology and Decision Support Services at the IWK. As she mentioned, she did work very closely with the team from the Auditor General's Department through the audit.

Marc is Executive Director, Health Information Technology Services or, as we refer to it, HITS Nova Scotia, and also collaborated with the audit team in areas related to the HITS Nova Scotia mandate. Most recently, as a result of Ferne's secondment, and as we transition to the new Merged Services Nova Scotia structure for IT, Marc assumed a direct IT leadership role for the IWK's IT services.

The IWK Health Centre takes the protection of personal health information very seriously and we are very aware, always, of the trust that each patient family puts in us to keep their information, and their children's information, private and confidential.

We value our participation in this very thorough review and the focus that it brings to the importance of protecting patient information. The IWK has policies, plans, and approaches in place to ensure the security of our patients' information. However, as the Auditor General's review of personal health information systems indicated, the IWK agrees that there is always room to improve and is committed to augmenting current practices. We value and support the Auditor General's review and recommendations to enhance our information technology security and controls.

Our information technology and privacy teams consider patient privacy and systems security their number-one priority and they have already addressed, or are in the process of addressing, several of the Auditor General's recommendations. To date we have implemented 32 per cent of the Auditor General's recommendations, with an additional 40 per cent to be completed in the next three to six months, and a further 16 per cent within a year. The remaining 12 per cent are ongoing and some examples of these efforts are as follows.

We have made progress in updating our IT disaster recovery plan and will be conducting a structured walk-through of the plan within the next six months; we are very close to moving our MEDITECH Patient Information System to the provincial data centre, which will allow for the IWK data centre to become the secondary centre; we have improved our practice related to the consistent documentation of the response and resolution of reported incidents; and we are working with HITS Nova Scotia to implement the new provincial Incident and Problem Management Platform, which is targeted for the Fall of 2013.

We have updated a number of policies related to the access of information and system security, and have others in the final stages of approval. We have updated a number of policies related to the access of information and system security and have others in the final stage.

The Provincial Privacy Best Practice Committee has developed policies and practices in contemplation of the PHIA legislation, which will allow for consistency of practice across the provincial health care system, and we've made significant progress in

our efforts to apply FairWarning auditing software to our largest and most frequently used patient information system, which is MEDITECH.

The review also highlights the importance of working closely with our provincial partners on strategies related to health information security including the Department of Health and Wellness, HITS Nova Scotia, and Merged Services Nova Scotia. Further, the introduction of the new Personal Health Information Act, or PHIA, presents an excellent opportunity for system-wide collaboration on the implementation of best practices for the protection of personal health information.

Of course, as we look to enhancing our information security systems we will need to carefully consider cost and patient care implications. We need to continually ensure we are making the wisest investments across our services.

Once again, thank you for having us here this morning and we welcome any questions you may have for us.

MR. CHAIRMAN: Ms. Power.

MS. CHRIS POWER: Good morning, ladies and gentlemen. Thank you for the opportunity to appear before your committee and provide an update on Capital Health's work and to address the recommendations the Auditor General made regarding our personal health information systems.

As you can appreciate, this is a very complex area of our operations, so I'm really pleased to be joined by two of my colleagues. To my far right, Catherine Gaulton who is Capital Health's Vice-President Performance Excellence and General Counsel and who provides leadership across Capital Health for patient privacy, as well as Shauna McMahon, Director, Technology and Infrastructure Renewal. Shauna was previously the director of Health Information Services during the period of the audit by the Auditor General. She is now responsible for IT hardware, communications technology, and support services.

Capital Health welcomed the review and recommendations of the Auditor General and his staff and collaborated over the course of a year to support this important work. We certainly believe that the recommendations made by the Auditor General will augment the existing information technology control environment at Capital Health. Once again we'd like to express our sincere appreciation to the Auditor General and his team for their excellent work. Given the scope and depth of the audit, Capital Health would never have been able to fund this type of assessment from our own internal resources.

At Capital Health, quality patient care is job number one. We know that our obligation to keep patient information confidential and secure is fundamental to the relationship of trust that is required to provide the best care to our patients and our citizens. We work diligently to protect information and our systems from outside threats. We have

confidence in the strong access controls and see the success of these controls in our record of defending against attempts to breach our security.

Capital Health uses the technology service that monitors our environment for any external security threats. Over the previous 12 months we have recorded over one million possible threats - none has led to a data loss within our system. As custodians of patient information, we also know that timely and appropriate access to patient information is an essential part of modern quality health care. Like the Auditor General, we recognize that an additional risk to the security of personal health information is an internal one. As an organization, we value integrity and accountability, and we remain confident in the ethical practices of employees throughout our organization.

Our ability to do proactive auditing is improving. We are implementing new provincial technology, known as FairWarning, to automate the auditing function. Our ability to upgrade and back up our systems also depends on funding. Creating electronic redundancy and physical duplication of data and equipment requires major investment. In budget planning, we must weigh the value of these investments and the level of acceptable risk associated with each recommendation - but we are already making progress; in fact, for the past two years, we have been working with the Department of Health and Wellness on the relocation of our data centre.

In the larger context, we are also participating in Merged Services Nova Scotia, which has begun the work of establishing a new governance structure for information technology decision making across the health care sector. Capital Health continues to ensure our critical patient care systems are adequately protected and secured and we look forward to answering your questions this morning.

Thank you.

MR. CHAIRMAN: Thank you.

Ms. Regan, you have 20 minutes.

MS. KELLY REGAN: Thank you. First of all I'd like to start off with Capital Health. A year ago, January 10th, a news article appeared in The ChronicleHerald with a headline which read: "Health worker loses job after prying into patient files." In the pages of recommendations offered from the Capital Health District, what specific action has Capital Health taken to ensure a headline like this never appears in the paper again?

MS. POWER: Thank you for that, and I'm going to ask Catherine if she'd like to start on answering that question around privacy and what we're doing.

MS. CATHERINE GAULTON: It's interesting in that case that - of course, it was discovered as a result of some of the systems that are in place in Capital Health -

particularly that the issue was identified through a staff member. Our ability to actually audit that system, our Horizon Patient Folder, allowed us to get very specific in relation to what had occurred, both so that we could take necessary action to follow it up, but also so that we could be very specific with patients when we notified them that it had occurred - we could tell them exactly what sections of their record had been accessed, to what extent, and whether it had been printed or just viewed.

That system is there and we've built on it, so out of that we are exploring, as Chris has said, the implementation, and soon-to-be implemented, the application of FairWarning to our systems so that we will have - we already have reactive audit as evidenced in that case - we will also have proactive auditing from the perspective of setting parameters on the system that would trigger that type of review electronically. So that would be the FairWarning system.

In addition, we have started to run some guided or selected proactive audits. For example, we actually audited all of our health information service workers. You'll remember from the paper that that was the case in January 2012, so we actually were able to proactively audit all of those employees. Those employees necessarily have the greatest access to health information and so we thought that was a good place to start.

As both our CEOs have mentioned, the work that is going on around the implementation of PHIA has contributed and provided us with a real platform to get the message out again around the importance of confidentiality - it's absolutely fundamental to the trust our patients have in us. We have on-line education in that regard; the on-line education requires a recommitment to a confidentiality pledge that is signed on employment - so that and many others, but I'll stop there.

MS. REGAN: Just out of curiosity, when you sign on as an employee, do you go through a course - is there some kind of program that outlines what to do and what not to do?

MS. GAULTON: Sure. Confidentiality and the importance of it, and actually signing the pledge, is part of an orientation for all staff. It's important to remember that while we at Capital Health have a fundamental role in relation to that, we're in the norm dealing with health care professionals, where that is an absolute aspect of their training. For many of them, particularly for health care professionals, it's an ethical obligation through their professional colleges. Our education definitely supplements that, but together, the message is very clear to staff.

MS. REGAN: Are there refreshers?

MS. GAULTON: Absolutely.

MS. REGAN: Let's say you work at the hospital for 20 years, and around the 15-year mark you might just sort of forget - is there a regular update?

MS. GAULTON: Sure. So there's an opportunity for regular updates, and this is offered. Our Privacy Review Officer, for example, does a lot of education - either directed at groups or general sessions, always.

What we're trying to facilitate through the on-line system is that there is both a course and a recommitment to the confidentiality, and that will be required to be completed annually.

MS. REGAN: I can certainly say that I worked at the Grace Foundation 20 years ago, and it was drilled into our heads. I remember talking with nurses who said if we run into a friend in the hallway, don't even say, why are you here? That was sort of drilled in.

According to that same article that we were just discussing, 14 patients were sent a letter which stated: "To the best of our knowledge, your information has not been disclosed to anyone else by this employee." I'm just wondering how the district knew that was the case.

MS. GAULTON: As I've indicated, in the system that we have we can tell whether something was printed or faxed somewhere else out of that system, so that's one way. In addition to that point we would follow up - and not to get into the particular case so specifically, but in that kind of situation we would follow up both with the person who is alleged to have breached, and within our systems to see whether in fact we've had any complaints or any disclosure in relation to that. So both the electronic and our own follow up.

MS. REGAN: So you would go back to the person who was alleged to have leaked the information, or to access the information and say, did you tell anybody else?

MS. GAULTON: That would be one aspect of it, yes.

MS. REGAN: Could Ms. Power give us some indication as to what process is followed by the district when a member of the public believes their personal health records have been inappropriately accessed?

MR. CHAIRMAN: Ms. Power.

MS. POWER: Again, Shauna, perhaps you want to take that, or Catherine, or whoever?

MS. SHAUNA MCMAHON: I can start. Generally someone would call and make a concern that they believe something has occurred. Generally that would go through HR

and the Privacy Office, so they would be involved. They would then coordinate what the collection of data would be, and in some cases that would mean contacting our security person in our IT department. He would run audits on either dates or the information that's given - we do not get the name of the individual, for confidentiality, because you're still in the investigation mode.

Generally he would get information on running reports on a particular system for a particular date. It might be on a particular patient, and it could be the Horizon Patient Folder system, or it might also be the STAR registration system. Then it would be given over to HR and the Privacy Office. What they would be looking to do is to see - for example, if it was a patient, were they in that day and was there a requirement for that health care professional to be looking at that particular information?

A health care professional is only to look at information that they require in the course of treatment of an individual - so that would be a start - once all that data was produced, it would go to the Privacy Office and they would analyze that, then there would be a determination if there was a concern or if they have to get Human Resources in place.

We have to be cautious in doing that, because some people may punch in a wrong number and it would look like they accessed a record, but it was for a couple of seconds. That would not indicate to us that that was what we would call "a breach." If it were someone fishing around for a long period of time, you would see that, and if it wasn't a patient they were directly involved in, that would then lead to the Privacy Review Officer further exploring that.

MS. REGAN: Am I correct in assuming that cases are more often brought to the attention of Capital Health - or potential breaches would be more often brought forward by employees rather than patients? I'm just wondering what the percentage was.

MS. MCMAHON: I can't give you a percentage but I would say I think we're very fortunate that we do not have a high number. In my previous role I know that I had a call from someone in public who was concerned and at that call I would then talk to the Privacy Review Officer and sometimes we have some internal, but it's very infrequent.

MS. REGAN: So how many situations would the district investigate in the run of a year? Let's say for the past two years - how many would have been investigated?

MS. GAULTON: Our protocol around investigation of privacy breaches is actually published on our Web site and it's very much in line with what Shauna has already said to you. It's important to note that throughout the time, the person who is complaining is kept very well informed as to the progress of that investigation. The one piece, and if I can, just on the last, what's very important to know is how strenuous a job it is to truly audit.

An electronic audit that indicates whether a person has access to your record or not is one piece of it; the other piece is then to follow up on what that audit shows. We have health care professionals who necessarily have access to health records and so the job of determining whether they needed access in a particular case is hugely difficult - their manager maybe the only person who can do that cross-connect between what might be hundreds of patients.

Over the last couple of years - in the last year we've had seven where we've done a full investigation. Some of those are, as Shauna indicates, accidental breach, so remembering that if a piece of paper is dropped on the floor and someone picks it up, that constitutes a breach. Over the last year we will have seven that we've done really intensive investigations on, not counting the audit that I talked about in relation to health information services staff, so that huge.

MS. POWER: Perhaps just to put that in perspective, we see upwards of a million patients a year coming through our doors at Capital Health and if you think about all the patients' records we would have in our archives - just to put that in perspective for us.

MS. REGAN: Thank you for that, that does put it in perspective. Given the strenuous nature of doing an audit, do you feel you have the appropriate staff to be able to do that kind of thing? Am I correct in understanding that it is a nurse manager who begins the audit or begins doing the investigation?

MS. GAULTON: The complaint normally comes in and is somehow directed to the Privacy Review Officer; if it doesn't come there initially. The audit, the electronic audit is actually run, as Shauna has indicated, between the Privacy Officer and the security people. If we determine that the person has had access to that particular person's record, it usually then triggers a wider audit to say what other access have they had, and there would then be a review. So it has to be someone who knows the patient population, and that might be a health services manager, it might be a health information manager. It really depends very much on where the employee who is being complained about, where they work.

MS. REGAN: So do you feel you have the appropriate staffing to be able to conduct full and complete investigations if, in fact, it is a strenuous job to do a full audit?

MS. GAULTON: There is no question that is a huge resource pull and yet it's important enough that we direct resources to it. It is huge. Do we have enough? We could definitely use more assistance on that front, but we make it a priority when it occurs, it is just that fundamentally important.

MS. REGAN: What would a district like Capital Health do if a breach was reported by a staff person and the breach involved the record of another employee as a patient?

MS. GAULTON: The same process is followed. So in that instance we're not dealing with staff and staff, we're dealing with staff and patient because that is the context in which we have a record for that person.

MS. REGAN: The district has provided a comprehensive response to the AG's recommendations, the vast majority of which are in progress. Has the district calculated a cost to the district itself to implement all these recommendations - and, if yes, how much, and if no, why not?

MS. POWER: I'll start that. There is no question that when we looked at all of the recommendations we understood that there would be time and cost involved in that. So I'll ask Shauna to speak a little bit more to the process that they followed, but what I will say is Shauna and her team, and others, looked at all the recommendations and prioritized them, and we went from there, recognizing that this work is going to take time, money, and collaboration with the Department of Health and Wellness, and many others. So we have not quantified what all of those costs would be, but rather are working through the recommendations in order of priority and working closely with the Department of Health and Wellness on that.

Shauna, do you have anything to add?

MS. MCMAHON: Thanks, Chris. It is complex in terms of trying to predict a cost, but I can give you some examples. When we were undergoing the audit, we had already embarked with our colleagues at HITS Nova Scotia on - we had done a vulnerability assessment on our data centre a few years ago and we knew that we had to do some work to update our storage component, and we also wanted to create a redundancy between the provincial centre and Capital Health. So that particular work, just on the data centre alone, which is involving us placing all of our backup servers at Young Street, and for Capital Health storage it stays at the Abbie J. Lane, and for HITS Nova Scotia, we're reversing that, we have a nine-, ten- year lease, and that lease is $20 million, so that's just for the storage.

We're also working with the province at this time, the bigger province, Education, Justice, and they're looking at, based on a previous Auditor General Report, on what we call a secondary data centre for the province, which would be for redundancy in the case of anything like a hurricane or something like that that might come through and could affect the other data centres.

Also, as we bring in new technology, I think it's interesting to note that some of the technology we have started coming on board in health care in the 90s, which is a long time ago, and at that time I remind people that health care, even though there's so much in the media about it, it's kind of an immature technology field when you look at something like banking - and I date myself, but I worked in a bank in Cape Breton back when they were first putting in the automated bank machines, and nobody wanted to use them, I can tell you

that, and now you can go anywhere in the world and get your money. So in health care it's a relatively new burgeoning area. So what we're doing now is each time our applications come up for renewal or upgrade, we go back to the vendor and say here's what we have in PHIA, here's what we need to have for auditing purposes, what's that going to entail and do you have it.

We're fortunate, I guess, in some ways, in that many of the large vendors are international so they also have to comply with HIPAA in the U.S. So they are updating their processes much more, so when Catherine refers to Horizon Patient Folder it is Capital Health's scanning and archiving system. All the documents that are produced every day are scanned and then archived electronically, and then the papers destroyed after that. We do 34,000 documents a day; 1 million a month.

That health information services group that Catherine referred to that we audited, I oversaw that group at that time, and that's why we did the audit. They have access to that information. So we audited to make sure that they were compliant with our policies. So, an upgrade for a system, we just did one with the lab system, and that can be - depending on the complexity - it can be half a million dollars; some of them can be $300,000. So as we keep updating, that's what we put in place. So we didn't go through and do a full cost of what everything would be.

The other thing we know that's happening, as folks mentioned with Merged Services, we had already started some projects jointly, so my colleague Marc and our group - one would be a whole new application for our help desk. So the Auditor General talks about ticketing and how the help desk manages its tickets. With the new application we're bringing in, we will have all those procedures written and incorporated into this new application. The one we have is older.

So as those legacy systems are getting upgraded, we're bringing in and we're jointly sharing the costs of those. So we have a couple of things on the go.

MS. REGAN: When you say you're jointly sharing the costs of those, that's Capital Health and IWK - are you receiving any assistance from the Department of Health and Wellness to purchase this kind of upgrading of IT technology?

MS. MCMAHON: In some cases the province will have purchased a system and then we would link into that. An example of that would be the SHARE portal, which is the portal where all of the physicians can access information in the Capital Health system and in the provincial system.

Anne McGuire mentioned about the IWK - there are three core platforms in Nova Scotia, and we're very fortunate. Many provinces have 10 or 20 or more, and that's why it makes it challenging for them to create a more integrated system. Within Nova Scotia there's a MEDITECH platform. The IWK had MEDITECH Magic and Capital Health has

a mixed - we call it a best-of-breed platform, which means that due to some of the services and special needs at the time when we put those systems in place that was an acceptable approach. It means we have different vendors supplying the applications. So we're now working within . . .

MR. CHAIRMAN: Order, please. Unfortunately, Ms. Regan's time has expired.

Mr. d'Entremont.

HON. CHRISTOPHER D'ENTREMONT: Thank you very much, and I want to thank you all for being here today, even though I would much rather you were in your offices doing work in the districts. I'm sure you have a big stack of things to be working on today. I do thank you for taking the time out to be with us today.

I'll ask a few general questions first. As we talk about personal health information, maybe it's going to be a question that Chris is going to answer and one that Anne is going to answer as well.

Do you feel you've gone above and beyond to minimize the risk to the personal health information system? So it's a very general question - how you're doing with it, maybe things that are not in the speaking notes, how is it really going, and are you working really hard to get the AG's recommendations under control? Whichever one wants it.

MR. CHAIRMAN: Ms. Power.

MS. POWER: Thank you for that. Are we working really hard to address the recommendations that the Auditor General has given us? Absolutely we are. We take it very seriously. As mentioned in our opening remarks, we were very grateful for the depth of that audit. In fact, I don't think any of them were surprises to us, because we knew and know that this has been a resource issue and a decision we've had to make on where we balance.

We are very confident in the integrity of our systems. I think if you look at the number of potential breaches and the fact that we've had none from external - we're extremely proud of that and work hard to ensure that that's the case. Because we have so many people who have legitimate access to our records internally, that's been a little bit more challenging. Now we're introducing additional software that's going to help us with that and the diligence with which our staff monitor that to be sure, and the integrity with which the vast, vast majority of our staff work and understand how important privacy is.

We're confident at Capital Health that we're working toward those gaps that have been identified, but that security is absolutely critical for us, and we understand; we get it.

MR. CHAIRMAN: Ms. McGuire.

MS MCGUIRE: I totally agree with all the comments that Chris has made. It's a very evolutionary kind of process to address all of these issues. They are critically important in our day-to-day work, and I think that everyone involved in health care has privacy and protection of information forefront in their minds. Like Capital District, we appreciated the opportunity for the analysis of our system and the identification of the gaps that we needed to address, and we're well down the road doing that.

It is a delicate balance as we go forward to weigh the resources needed versus the absolute requirement to meet all of the requirements in the upcoming legislation, et cetera. Not a day goes by that we're not making progress.

MR. D'ENTREMONT: So 25 recommendations from the AG - how many of them are in process, done, or about to be done?

MS. FERNE MARDLIN-SMITH: As Anne had mentioned in her opening statement, of those AG recommendations, currently 32 per cent are complete, but it's important to recognize that there is another 24-plus per cent that we are actively working on and hope to have those completed within the next three to six months.

We collaborate with our provincial partners and with the Department of Health and Wellness in understanding of those that will take a little bit longer that we need to approach that at a system level. They are going to take a little bit more in planning, but there will be some aspects that will be difficult because of limitations to current technology.

Again, we look forward to the Merged Services work that is ongoing because that is going to open up some opportunities for more of a provincial look at our systems, look at assessments, and introduce best practices, standardization, and move us towards meeting the PHIA legislation.

MR. D'ENTREMONT: Out of that bunch of recommendations that are a little more troubling, or are going to be taking a little longer to do - what kind of examples could you give us of the ones that are going to take a little more time beyond the 32 that are almost complete and the 24 you're working on? What's the other gang of recommendations that are going to be a little harder to do? - just a few examples.

MS. MARDLIN-SMITH: A couple come to mind, and one would be - we're pleased that the province has purchased the FairWarning software that Capital District Health has referred to using. That tool will allow us, for any of our information systems that currently have the ability to produce audit logs, they allow us to know, at a granular level, what people are accessing. Those audit logs are what we are going to be able use - of those systems - move that into FairWarning, which will then allow us to start to do some more in-depth, proactive auditing.

If we've got some legacy systems or systems that do not produce those audits, then that's going to create some difficulty, and that's what I was referring to - prioritizing those systems, working with our colleagues to see - okay, what are the systems? Are there other systems in the province that could be replaced? And if there aren't any, then that's what I'm going to refer to. They are going to be a little bit more difficult because then they're going to require both financial and human resource investments. Those are the ones that are going to be a little bit harder.

The other one is going to be the ability within the PHIA legislation, which is what they call consent directives, or what you and I may know as that ability for families or patients to lock a piece of information. Our current technology does not allow that to happen. So what we need to do is look at mitigation strategies so that if we do get a request for that, it is going to be working with that patient or that family to understand the risks associated with that and then work with them in order to protect that information or their concern, as best as we can, in partnership with the clinical care provider and that patient or family. Those are just a couple.

MR. D'ENTREMONT: I'm going to ask the same question to Capital Health. I know it's pretty general, but there you go.

MS. MCMAHON: In the recommendations we had, we looked at - and I mentioned previously, some of them are a similar theme. So there are a number of them related to the help desk. So that particular project got underway very quickly with our colleagues at HITS. We have an application purchased; we have a project team set up and they are now working through the steps that they have to do, looking at the recommendations and building what the procedures will be for this new service desk system that will serve the province.

Related to our data storage for Capital Health, we are 90 per cent complete on that in terms of - we have almost 300 servers, which are your small, powerful Mini Computers that are being replicated at Young Street; HITS has probably the same number that we are replicating at the Abbie J. Lane - that's 90 per cent complete for those two organizations, and we're also doing it provincially, so I think that's about 75 per cent complete. Those two are very complex projects, so we expect we will finish up the storage this year in rather short order, but we know it's a longer process for us because we need to look at processing and what we need to do with that.

So depending on the complexity of the project, they take longer, so we may be - we've been at them longer, so we're farther along. Some of the other ones we're going through just in our day-to-day work, making sure that our applications all have consistent password logout time, those sorts of things. I would say it's different. All of them are in progress.

MR. D'ENTREMONT: So out of the 33 recommendations Capital Health had, they're pretty much all being worked on in one way or another along the way.

Talking about disaster recovery, you're talking about the servers, and the two locations - Abbie J. Lane and Young Street - they're all in Halifax. If the grid in Halifax goes down, where else is this being replicated?

MS. MCMAHON: Our servers, yes, Young Street, and then at the Abbie J. Lane, but we do have some vendors that do some backing up of data for us at Capital Health. We back up daily, weekly, monthly. We do two backups a day, and we also have some tapes that we store off-site with confidential storage. We try to make sure that we've covered that off. Maybe Marc might have some comments there.

MR. MARC LEBLANC: As mentioned, they do replication of data at both of the data centres for on-line storage, and then that's backed up to tape, which is then stored off-site. That is the data portion, which is the most important part in terms of getting the information and keeping the information.

I think your question relates to if a disaster happens, though. They are both within the peninsula of Halifax. They are on different electrical grids, mind you, and there are significant backup systems at both centres. However, with the province we are looking at a secondary data centre for all of the provincial initiatives - both in health and in government - outside of the peninsula. An RFP will be going out to look at providing a secondary centre, we're calling it, somewhere else in Nova Scotia at this point for that kind of on-line, very near-availability, high-availability data centres.

MR. D'ENTREMONT: What kind of distance from the city would that be? Is it in the Truro-Bridgewater radius? Is it Sydney?

MR. LEBLANC: The high availability that we want to get for our data centres, the technology right now limits us to about a 100-mile area, so yes, you're talking Truro, a little bit further, somewhere in that radius.

MR. D'ENTREMONT: The issue of data centres, as we continue to add programming - whether it's PACS or others - we're getting into tremendous sizes of storage. What kind of storage are we running right now in our data centres? It's getting to be bonkers, I'm going to guess.

MR. LEBLANC: Yes, we're into the petabytes of storage. We're way beyond gigabytes and all that. We're well into 500 petabytes of storage, probably, if you include both Capital Health and Young Street, because they're both very critical to our systems. It keeps increasing. For example, on the PACS side alone, we're probably buying 35 to 40 terabytes of storage every year to manage the increase in volume that we're putting in there, because of newer technologies. Your CT scan now takes huge amounts of data that it

never took before. Every time you do a CT scan it increases your storage. It's increasing all the time, and it is a struggle to keep up with that, both in physical storage and the money to pay for that.

MR. D'ENTREMONT: As we continue to - I mean, we're talking about the connections and stuff in each of your districts, and maybe in some of the connections between the two districts. How is that going? I know right now the IWK is doing some women's health work, and maybe some scans are happening over at Capital Health, so how is the data flowing between the two organizations at this point? And then maybe I'll open the next question up to, how is the data flowing into the other districts across the province?

MS. MCGUIRE: That is an issue that we are constantly working at and not only between Capital District and the IWK is there significant collaboration, but I think as Ferne mentioned, through emergency services, et cetera, there are a whole lot of initiatives where we're looking at improving our ability to collaborate with information, et cetera. But I will defer to, I think, Ferne, to talk a little bit about some of the specifics of that.

MS. MARDLIN-SMITH: Our information system within the IWK - our main system is MEDITECH and we are on a Magic platform, as previously noted. When we have those systems and we need to collaborate between, we are using the provincial's SHARE - Secure Health Access Record project - that will allow our physicians and our clinical care providers to have access to the information at a very high level.

As well as that, we are working between the two facilities so that Capital Health physicians can have access, within the IWK, to Capital Health's data and we can also have the application for MEDITECH so that the physicians at Capital Health can access MEDITECH at the same time. Again, we are looking forward to the merged services. That is quite an opportunity. We are quite excited about it, to look at it from a provincial perspective in regard to what is strategy and vision of all of Nova Scotia so that everyone has access to that information, in a timely manner.

MS. MCMAHON: I think that Ferne answered that quite well and we are looking forward - one of the things that we're looking at now - I mentioned before about scanning - and we've been doing that since 2005, at Capital Health. Our next foray into technology is now working with the provincial colleagues to look at what we would call our next level EMR component. Currently we don't have all of our scanned information available in that portal but our EMR component would enable the health care providers to actually enter their work directly in the computer. They would have order entry on-line and that would automate all of that work.

So hopefully, my dream would be, we would not have to scan the 34,000 sheets of paper every day. That is the ultimate goal. But we have worked very well with the shared portal, over the last number of years, to make sure that the clinicians can access that and get information they need, so they can get all the transcribed reports and view that and some

other information. That has come a long way to help them and they all have access into the X-ray Web1000 and they can view X-rays and other diagnostic results.

MS. POWER: I would be remiss if I didn't say that where we spend a vast majority of our money is in our hospitals. Where the vast majority of health care takes place is in our communities and one of the issues that has been a bone of contention, certainly for our family physicians and people who practice in the community, is the connectivity to understand what happens with their patients, when they come in. We are just starting to launch into thinking about, and working on, an electronic medical record that will connect not only within our organizations but in the community, and it is an essential component of being able to have health records move back and forth, for citizens and patient sake. That's work that is certainly ahead of us but when you talk about connectivity between hospitals that's hugely important but what is just as important is our connectivity in the community.

MR. D'ENTREMONT: Thank you for leading me into my next set of questions.

MS. POWER: Oh, see I read your mind.

MR. D'ENTREMONT: You know exactly where I was going here because sitting down at a number of conferences, over the last 10 years, and we talked about EMR and, of course, connectivity in general, me in Yarmouth getting an X-ray is okay now, because PACS will transfer that, but my medical record doesn't necessarily end up in the city the way it should, from Yarmouth. The same thing happens, should one of us be in Vancouver and something happened to us - well, what's your fax number, I'll ship some of that over to you, hopefully. Again, Canada doesn't have that across-Canada programming that allows us to share a medical record easily, and I think that is the challenge - just getting us on University Avenue being able to talk to each other and then, hopefully, from University Avenue we can go into peninsular Halifax, and from peninsular Halifax we can go to HRM and continue on that route.

As much as these recommendations are good, and I think they show that you've got a lot of work to do internally, I hope that it doesn't deter anyone from looking at those larger issues of providing a true emergency medical record across the province. Again, it's a general question, but some thoughts around that.

MS. POWER: Perhaps I'll start, and anybody else can jump in, and say that that is absolutely part of the vision for our electronic platform for the province. We've known this for a long time, and I think Anne mentioned, it's a balancing act for not only the province but for each of us of, where we put the limited resources we have. There is a plan that's in place and we're a little bit behind the schedule of where we hoped we would be at this point in time, but certainly a plan to have an electronic system for Nova Scotia. The rest of the country, that's - we all came at this doing our own thing rather than looking at it from a system approach and we're kind of running to catch up, and all provinces are doing the same thing, but we do have a plan here and we're marching towards it.

MR. CHAIRMAN: Order, please. Unfortunately, Mr. d'Entremont's time has expired.

Mr. Ramey.

MR. GARY RAMEY: Thank you for coming this morning. I have to say, just before I begin, that my family has been a consumer of your services - both Capital Health and the IWK - and I can assure you that they got the absolute most stellar treatment when they were there, so I want to thank you for that.

I was listening with interest - I think it was Ms. Gaulton who was speaking about the development of software for the health care system. I think ATMs or something were referenced at one point. It was somebody over there anyway who was speaking about this and how they were first looked on in some kind of strange way - and now most people don't even carry cash because they have plastic and go to an ATM and get the money if they need it. I'm just wondering, in terms of the - and this would be both IWK and Capital Health - in putting those systems together that you're using, you had to start somewhere.

I know Johnny Cash wrote a song once called "One Piece at a Time" about building a car, and perhaps, back in the day, systems weren't integrated, or maybe you had to buy from different companies and try to find some way to work it all together - can somebody, either from Capital Health or IWK respond to that and tell me, let's say, about 10 or 15 years ago, where you were and how you got where you are now, could you just briefly tell me that? I know it's not a brief story, but give it a try.

MS. MACMAHON: It's a great question and I can probably make it brief because I wasn't involved in the early days when all this came about. My understanding is that at the time - this would have been back in the 1990s - a group within the health care at that time, and I do not believe that the Halifax Infirmary and VG and some of those organizations were still separate at that time, but I do believe that the VG - and I don't know that the new HI was even built - but the VG was meeting to bring in a system that would serve as – we're an academic research and quaternary hospital, so it needed to meet a lot of needs. At the time, there were very limited systems to select that would give the robust functionality.

It was very acceptable at that time - and I mentioned when I was speaking to Ms. Regan before about the best-of-breed model we have, which means we take different vendor applications, connect them to what might be called the central brain, which is our patient index registration system and write interfaces, so they can all communicate together. So we have McKesson applications; we have Cerner applications, we have GE applications, so we connect those all together - IWK and our other DHAs have one platform called MEDITECH.

None is right or wrong. It is just in the context of the time and what was required and what was available was how Capital Health proceeded with its system. We have now

almost close to 300 applications that would run through that system. It is very complex and, as we move forward, we will re-examine that particular model and see what we can do. At the time, that's how it evolved over the years. It often comes from the fact that starting up, no one system would meet the needs of all those disparate groups, so we went out and we picked what we thought would be the best to service our care providers.

Now the upside of that is that most of those systems have open architecture so we are able to interface some, we are able to connect them very well. When you get a one-package system like MEDITECH, it is a little more challenging to do that.

MR. CHAIRMAN: Ms. McGuire.

MS. MCGUIRE: Just to give a little bit of context from the IWK point of view and then I'm going to pass this over to Marc who was there - well maybe not quite at the beginning - our MEDITECH Magic program was implemented, I would say in 1989. At the time it was a state-of-the-art system across North America. It has, indeed, served us extremely well but we are now at the point where we really can't continue too far into the future to be able to maintain that system. I think that as Shauna and others have pointed out, it makes our system different from Capital District's and makes both of us different from all of the other district health authorities that have a MEDITECH platform, but a different one.

I'll hand it over to Marc to talk a little bit about how effective that has been over the years but then, on the other hand, how it leaves us in a little precarious situation at the moment.

MR. CHAIRMAN: Mr. LeBlanc.

MR. LEBLANC: Yes, the sharing of data has been the trickiest part of all of the hospital information systems that I've put in. As mentioned, the MEDITECH system was an integrated system, so internally within the system, it shared data very well, but you had to buy the whole package in order for that to happen.

In the CDHA case, they had the best-of-breed. Within the lab system it worked very well, but didn't share data with anyone else unless you built the integration to allow it to share data. So there was an awful lot of work that had to be done, at the back end, to make it work, to share that data. There was just a choice that people had to make at the time and today it's becoming more and more important to share data. As has been mentioned, we need to get it to the patient; we need to get it to the doctors; we need to get it out there.

So the systems now are becoming more and more integrated. They are getting away from these best-of-breed- type systems, mostly in North America now. They are going to the integrated systems, which allow the hospital to have better data shared between itself,

but also the systems now have moved ahead with the ability to share data with other integrated systems. So we can do that.

In Nova Scotia what we did to mitigate that problem is we built the SHARE portal, which allowed a certain amount of data to be shared between the three medical systems. You can get lab work done in Truro and someone in CDHA can look up that lab work. That's a huge improvement to what it was five years ago, where that never happened - the patient was the carrier of the data. Now we're able to look up certain elements of the data, not all elements, like Shauna said. Some of it is scanned. We can't get access to that to share that. Some of it still not being put in electronically; you can't get access to that.

It is improving, but it's taking a lot of work to get there and a lot of money to get there.

MR. CHAIRMAN: Ms. McMahon.

MS. MCMAHON: There is a federal agency called Canada Health Infoway that also is doing some work that is helping improve the integration of systems, as Marc said. So now with the systems that are available, you can perhaps purchase from one vendor and they are very integrated, which wasn't the case 20 years ago.

So it has come a long way and some of that Canada Health Infoway is helping the provinces in terms of creating standards that would enable that connectivity and, as Mr. d'Entremont said, at some point be able to then have your health information available as you move, so it would be truly portable.

MR. RAMEY: Which makes total sense to me as well.

One of the advantages, I guess, of asking questions – being the third person to ask - is you get to listen to a lot and then, of course, it prompts more questions while you're listening. I guess the second question I have, and it was prompted by something I heard over there, is the IWK is really the centre for Atlantic Canada as well. I mean, we have children coming from other Atlantic Canadian provinces, and perhaps even from other jurisdictions as well. Are we able to interface the IWK with hospitals in P.E.I., New Brunswick, and Newfoundland and Labrador, and places like that, or do we have glitches there?

MR. LEBLANC: To answer your question, no. We are working towards that with Canada Health Infoway and the pan-Canadian strategies, but right now, sharing of information, beyond PACS information - we do share PACS electronic X-ray information between New Brunswick, Nova Scotia, P.E.I. - but other health information, right now we're still in the paper form; we are not connected to those systems.

MS. MCGUIRE: The provincial Health Ministers are, however, looking at this whole issue and the potential for partnerships to accomplish - and that is a very current topic of conversation, particularly between Nova Scotia and P.E.I., for instance, so I think there are some possibilities to move forward, and there's certainly an interest and a will to do that.

MS. POWER: And I would just add to that that Capital Health is the same as IWK in that we service the Atlantic provinces, and the people who are coming to us are probably some of the most critically ill people that we're taking, so it is a major issue for us, in sharing of information. So we're delighted that conversations are happening to tighten that up.

MR. RAMEY: Thank you, and I guess along that same line, I was wondering how - because I'm sure you folks, at least some of you, and maybe all of you, get to meet your colleagues from other parts of the country, outside of Atlantic Canada as well - I'm just wondering, are we here in Nova Scotia, in relation to the issues we're talking about this morning, in about the same position as most other provinces? I heard an allusion a while ago about other provinces in the country, but are we in the middle of the pack, or are we lagging way behind? Are we catching up, or are we, maybe, a bit ahead? Can somebody just comment ever so briefly on that?

MR. LEBLANC: We are not in a bad position when you compare us to the rest of the provinces in Canada. We're all in different places, the way we've attacked things and the way we've done things. In fact, because Nova Scotia put the one MEDITECH system in for 34 hospitals around the province outside of Halifax put us hugely ahead of some other provinces. Even New Brunswick, for example, though they have eight different hospital information systems, seven of which are MEDITECH, one of them is not, they don't share any better, because they are seven stand-alone instances of the same product. So that doesn't really help you. Ontario, well Ontario is just a huge amount of different hospital information systems, LHINs, and things like that.

Other provinces have gone the Merged Services route, but they're still struggling with getting hospital information systems together, so that one system serves everybody. So they're working towards it, everybody's working towards it, we're all sort of in a different place, but Nova Scotia is not lagging in that instance because of what we did with the MEDITECH system, and the way we've got our SHARE portal now working for our three systems, it's made it much easier, because we only have three systems to integrate, not the seven, eight, or twenty, thirty, whatever they have in Ontario.

MS. MCMAHON: I would support Marc's comments in that we're - actually when we talk to some of our colleagues, in some ways perhaps they are envious of what we have here in Nova Scotia, because in many of those provinces they do have such separate systems. I've even talked to health organizations in Ontario that are part of the same organization but have different hospitals, and those hospitals are not connected. At Capital

Health all of our systems connect across all of our facilities, even those out in the community.

They can look in and see the scanned documents. They can access the archive record and we did that purposely to connect them all. In some ways we're farther ahead and then in other ways we might be behind, but we're certainly not the laggards in the country, that's for sure. I think we will, with our EMR work and some of the plans that we have for the future, we will really jump ahead of other provinces because we do have more integration happening.

MR. RAMEY: It's very gratifying to hear that, and I have to say if I have these percentages right - I may have them wrong but I was paying attention - I heard at one point that 32 per cent of the recommendations were complete, 24 per cent maybe within the three to six months, 16 per cent within the year and then that 12 per cent, and I think Mr. d'Entremont asked the question already about what's in that 12 per cent and received an answer. Really, I think that's pretty good. It sounds like you're moving it.

You also said, I heard this at least twice, I think you were thanking the Auditor General or you were praising the Auditor General - I don't know how he feels about that, he probably feels okay about it - for doing this audit and the comprehensive nature of the audit, which I think you implied it would have been very difficult for you to do internally, largely I guess based on financial considerations. My question is - I'm rapidly running out of time and I know my colleague for Halifax Chebucto is going to ask some questions in the second round, but I'd like to get this one in - is this the first time, and maybe I do know the answer to this one, that an audit of this kind has been done on your operations?

MS. POWER: Well, we are the target of Auditor Generals coming in and looking at us a lot, and so we should be because we're so large. We spend lots of time with the Auditor General's Office on a number of things, but for my recollection and in my time as CEO, this is the first time we've had such an in-depth look at our IT systems at Capital Health.

MS. MCMAHON: That's correct. We are an accredited facility so we have, during accreditation, had just an oversight review of our systems. They were positive. When we do our financial audit, they do controls audit on our IT system. The last one that was done was very positive, no report.

This is the first time that I could find, in any of the records, such an in-depth audit and it was appreciated because, as it has mentioned, we would never be able to do that without a significant cost. I would like to point out that we are working through the recommendations while we continue to keep a complex organization running. So we're working through that while we support our clinical care folks, every day, doing the work that they do. It's been a very positive experience and I do believe the auditor that we had, at

some point they extended it a month because he said this is a very complex place. I said, no kidding.

This morning I just gave some examples of the volumes that we do, so we are very, very busy. It was a pleasure to actually read it and see that we do have some areas to tidy up and, also, it was nice to know that they weren't insurmountable, that we can do it and now we believe we will achieve that within the next year, year and a half.

MS. MCGUIRE: Similarly for the IWK, I believe it was the first time that we have been engaged in an audit, using these particular standards and with this degree of rigor. We do our own internal quality reviews constantly, but this took us to a whole new level and has certainly given us a whole new challenge and direction as we move forward in this area. So it has been very helpful.

MR. RAMEY: Thank you, and again I think my colleague from Argyle, Mr. d'Entremont, was asking some questions sort of around this general area. I guess in this day and age being able to send things electronically, it's so smart and so fast and it works so well. I know that would be a goal, obviously, to be able to do that, especially in a province like ours which isn't too big and also, I guess, from other jurisdictions it would be ideal if it could be from other jurisdictions, too.

Just to get a little bit of clarification on that - where are we with being able to do that, are we miles away from being able to do that, or are we approaching a time when it's not too far away?

MS. MCMAHON: I'm coming to the microphone before I even get acknowledged. I would say that we're getting very close to that reality. In fact, some days I could sit at Capital Health and I would joke and say I'm dizzy now. Within just our network we have it divided - now we use a Cisco network and for our clinical folks we have them set up so that all of the access that they have to clinical information would not interfere with what might be available to the public.

You mention about the prevalence . . .

MR. CHAIRMAN: Order, please. Unfortunately, Mr. Ramey's time has expired.

Ms. Regan, you have 14 minutes.

MS. REGAN: Thank you very much. There was something that someone said in response to - I think Mr. d'Entremont - about not being able to share information, computer information with family doctors yet.

MS. POWER: Just to clarify, our family physicians in the community, the vast majority of them have access to lab reports and to some of our scanned information but a

true electronic medical record, where we're sharing back and forth, so they're getting information from us but not vice versa. We want to have an integrated record that has everything about the patient on it, so we are a way away from there.

MS. REGAN: I thought I saw commercials that talked about electronic records, that Nova Scotia was moving to electronic records.

MS. POWER: We are moving towards.

MS. REGAN: But they are not available yet, is that correct?

MS. POWER: Yes.

MS. MCMAHON: I would describe it as we aren't 100 per cent electronic but as Marc and Ferne and others have suggested, for example there's an umbrella system called the share portal and the share portal, all of our family physicians and others have access to that. There is information that goes in - it's like a viewing umbrella application. They can go in and look at the medical reports that have been dictated. They can see the lab results, they can see the diagnostic imaging results.

The piece that we're now working on and I was alluding to before is what's called clinical documentation, where the care provider is actually typing in the system where now they're writing. So when I mentioned all the scanning we're doing, that's actually them writing all the information from the visit, it comes down into a department and we scan 34,000 sheets a day across our district alone - I'm not even speaking about the other eight districts or the IWK.

What we're trying to do is now get that particular piece in place over the next few years, that we would call it the EMR component. It would have that clinical documentation and it would have the order entry component to it. Once we have that and we can then feed that into the share portal, that should provide that access for everyone in the province, but that will be a few years.

We're also working on that, as Chris Power mentioned, we're having conversations as a result of the minister's meeting with our other Atlantic Provinces. We are all struggling right now in the same place with some applications, major applications for an EMR, and they are all very expensive. It wouldn't be unheard of to say in the $10 million to $20 million range to get those up to the level they need to be. So for small population base, we're now talking to those other provinces to see if there something that we can do.

MS. REGAN: Just to clarify, if I recall that commercial correctly, it shows someone coming into an ER and they are immediately accessing the person's records, but in fact, all that would be on there, at that point, would be records if they had previously

been in the hospital or had tests, not if they are just Joe or Josephine Average, who goes to the doctor and has had no problems. Is that correct?

MR. LEBLANC: There are a lot of electronic information systems out there that are related to health in the province and the commercial is probably related more to a personal health record being available. There is a pilot project right now in the province where we're looking at a personal health record and that would include your records from your doctor that you have access to, so that if you show up in an emergency room, you would be able to access not only records of the hospital, or the doctor would look up in the share portal the records in the hospital, you could yourself look up your own personal health information, or provide that information to look up to the doctor, and it would contain information from your own family physician or specialist you have visited who were participating in this program.

There is a pilot project right now to look at all of the nuances, because there are a lot of issues dealing with this and they are not technical in nature a lot of the time. They are all to do with sharing of information, privacy, confidentiality, and all those other things that we've been talking about. It's very complex and they are also not cheap to do, to give citizens access to their health information. That would answer Mr. d'Entremont's question as well, as being able to have access to your own personal health information and you choose who to share it with, at that time, because you have the access. Most likely in an ER you would want to share it but you may not want to share it with others in your health profession. There is that section of it, which I think is what you were alluding to, more than what the hospitals are doing.

MS. REGAN: So the pilot project is underway, where is it underway?

MR. LEBLANC: Right now it's in the Halifax area, there is in excess of, I think, it's somewhere around 30 physicians who have signed up and hundreds of patients of theirs that they have gone to who have signed up for this program and they are doing the pilot project now. I haven't got the exact numbers but I can get them.

MS. REGAN: Okay, so I'll have to go back and look at that commercial again because I thought that things - everything - it was proceeding, it wasn't a pilot project, and everybody's records were being putting on-line.

MR. LEBLANC: In a hospital the records are on-line, yes, and they would have that and our shared portal allows us, like I said, you come from Truro, come into Halifax, and your hospital information would be available, but we need to expand that. It's not there yet. It might have been an art-of-the-possible commercial, I don't know which one.

MS. REGAN: I'll have to get a hold of it. On to the IWK, according to the AG, Recommendation 3.12 requests that the IWK should better secure its system by increasing password and account controls, which include requiring users to use complex passwords,

preventing users from using previous passwords, and locking accounts after a number of failed login attempts. The IWK responded by stating they agreed with this recommendation, which would require additional funding. So I'm just wondering, how much additional funding has the IWK estimated this would cost and has the Department of Health and Wellness provided that required funding?

MS. MCGUIRE: We don't have specific information around the costing and the whole issue around passwords, although it might seem simple at first glance, it is really fairly complex and I'll have Ferne respond to all of that. We really have not formally asked for resources. We are working from our own internal resources and trying to reallocate those as is appropriate but I think Ferne can talk about the intricacies of passwords.

MS. MARDLIN-SMITH: What needs to be appreciated within a health care system is that there are numerous health information systems that our clinical care providers need to access, at any given point in time, in the provision and delivery of health care to our patients. In respecting that, we need to acknowledge that our clinicians would need to know - if we were to implement full, stronger passwords, which could be up to 12 characters, they could be alphanumeric, there would be a requirement in emergent urgent times when we would be looking at our physicians or clinicians to know how many different passwords, and what we want to do is ensure that those difficult passwords don't interrupt the provision of safe, quality patient care, so there is a delicate balance.

We are looking at our systems. We will be looking at those to see and assess them for where we could, maybe, increase our passwords but, where it may have a negative effect to patient care, we're not comfortable in going there.

When we made the comment regarding requiring additional resources, that was in terms of looking at something which is called a single sign-on, which is a solution that would enable the clinicians to have one password, therefore it could be complex, and knowing that one password would get them, immediately, into a number of the information systems, therefore decreasing the risk for not accessing information at a critical point in time, in delivery of patient care.

MS. REGAN: Just in terms of accessing patient records, are there different levels of accessibility? Let's say if you're an LPN and you log on, can you get anybody's records or is that restricted to a doctor? How does that work?

MS. MARDLIN-SMITH: Staff's access to patient information, within the systems, is driven by the need for them to have access to do the role into which they've been hired to do. If you happen to be a nurse and you need to provide nursing care, then you're going to have that access to all patients who could come through the door because to do their role in nursing, they need that access to that information.

MS. REGAN: Let's say you were a nurse on the neonatal unit, would you only have access to the patients who are on the neonatal unit or would you have access to patients in orthopaedic and all the various parts of the hospital?

MS. MARDLIN-SMITH: That will depend, at the IWK, on the role of that nursing position, if you will. We have some areas where we would have a float team, so if you're a float team and you're the nurse on that float team, then you would need access to wherever the expectations of that float team would go. It really depends, again, on that role and where and who that provider is.

MS. REGAN: So generally, if you're not on the float team, if you work in a certain unit, would you have access to only the records of the patients on that unit or would it go beyond?

MS. MARDLIN-SMITH: The access is given to the systems within the unit of the patients that they will see, and then it will depend on other types of nursing, if they have other roles that go beyond. So we do need to ensure that they have access, but again, when access is approved and given, there is a good understanding between the clinical care area and the manager who is approving access, before access is given.

MS. REGAN: Would that be the same case for Capital Health? Would nurses be restricted to their unit, unless they had a more generic role throughout the hospital?

MS. GAULTON: Realizing our patients move between units all the time, that would be very difficult to do. The concept of a nurse tied to a list of patient names is not a current capability and not easily achieved, simply because of that. So the nurse in emergency needs to know; the nurse in orthopaedics needs to know; if there's a critical orthopaedic patient and one needs to move to the medicine unit, then the medicine nurse needs to know. There is, as Ferne indicates, a huge level of understanding, at the front end, what it means to have access, and the principle of need-to-know - and that will go through everything - is what is fundamental to what you then actually access.

MS. REGAN: So just to make sure that I understand what you're saying - if you are a nurse at the Infirmary and you are on a unit, you have access to the records of all the patients at the hospital, is that correct?

MS. GAULTON: Yes.

MS. REGAN: Thank you.

MR. CHAIRMAN: Ms. McMahon.

MS. MCMAHON: I would like to add that as others have mentioned, in terms of need to know, we do have within the set-up of access, people do have to fill in a request

form. It is a user ID request form. It has to be signed by their most senior supervisor. We do, for example, for people who are direct care providers, they do get access to specific systems, and it is to all the patients, because they are moving all the time and the staff move as well; they get reassigned.

MR. CHAIRMAN: Order, please. Unfortunately Ms. Regan's time has expired.

Mr. Porter.

MR. CHUCK PORTER: Thank you, Mr. Chairman, and thanks to the witnesses today for being with us. I look forward to an opportunity to ask a few questions.

I want to focus a little on the backup stuff that Chris was talking about a while ago;. I guess he just touched on it a little bit. When I think about the backup systems, I think about where I used to work. I used to work in a provincial ambulance communication centre. Every day we would take 350 calls; today they're taking 450 to 500 calls or so and every day this system is backed up. It's all technology, it's all electronic and I think about how easy that was. It doesn't sound easy, but it's technical. It's a pretty simple process - the calls come in, they get recorded, everything is recorded. It wouldn't matter if it was a call or you were entering data, it's all there. It's all recorded. It would be backed up every night, once in 24 hours or twice, whatever the routine is, and then that would be stored.

It didn't seem like that big a deal and, I think I heard earlier, I gather that there were multiple backups - is that correct? I just want to clarify the points. If somebody wants to take that, that would be great.

MR. CHAIRMAN: Mr. LeBlanc.

MR. LEBLANC: Yes, there are multiple backups taken. Now the storage system itself does backups within the storage system, of itself, for preventing failure of electronic components within the storage. Then that data is replicated to the other data centre, in full, which then also copies that into sections of itself. So there are at least three, possibly four, copies. Then there are taped backups that are made as well of certain data. Data is well backed up and well protected.

MR. PORTER: Okay, and I want to be clear - I am not that technical. I understand the basics of that and I understand exactly what you have said. So it sounds like there are lots of copies of things, and I understand the tape backup that you are referring to as well, and it's stored safely and whatever - does it all end up in the same place, though? So all of these multiple backups that are coming from whatever the systems are - does it all end up in the same house, shall we say?

MR. LEBLANC: Not necessarily. Like I said, the Young Street data centre data, primary data for the MEDITECH system for 34 hospitals, is backed up at the CDHA

centre, so that data is there. Their data comes back, gets backed up to the Young Street, and so you've got two different systems right there. Then other off-sites are dependent on the hospital. I think Capital Health puts some in a secure storage area off-site, so we do it at different locations as well. It's not all ending up at one location; there are multiple copies that exist in multiple locations.

MR. PORTER: Is there a goal, somewhere along the way here, that there would be one house, if you will, for all of the data to end up from the IWK, or wherever the location of the hospital, and all of these other systems might be? It would seem a bit of a - I don't want to call it a scattered mess - a bit of a scattered plan that we currently have, and I realize you have multiple copies, which is somewhat concerning, probably at the same time, from an auditor's perspective, and just when I was trying to track it down. Does that mean that there are multiple places to go and access it as well?

MR. LEBLANC: No, the backup copies of the data are electronically done in such a way that they have to be accessed by the system that they were made for - you can't just go in and look at that data from any terminal or anything like that, it is meant to work with the system. So you have no concern about that.

Our ultimate goal is to have our secondary data site as a high availability data site, which means that you will have two data centres working in conjunction with each other and have access to the data on either site at any time. One site could completely disappear off the grid and you wouldn't even know it - you would still be able to do your work based on the secondary data centre. That's our ultimate goal to have, and in that way you are protected at all times. You would still do internal copies of the data in each site for the purposes of a disk drive going bad or a computer going bad, but it would give you replication of the data that you wanted.

MR. PORTER: Just a little bit more on the backup sites, while I'm on it - and, again, I'll use the example of where I came from and what we did. The backup site was not really close to where we were, it was a significant distance - and I won't state where that is for obvious reasons - but it sounds like the backup you're currently holding is relatively close to the actual location. That would be a concern, obviously, in and of itself. Is there a plan to move that and, if so, how far would you say is a reasonable distance?

MR. LEBLANC: There is a plan with our secondary data centre - what we're looking for is off the peninsula. Technology limits that now to sort of a 100-mile radius to be of high availability. If you want to do strictly data storage and you get it when you need it, you can store that anywhere in the world, but for high availability we're into the 100 miles, which puts it, I think, well within any kind of standard that's out there now for secondary sites.

MR. PORTER: I heard someone mention the number of pages a day - can somebody clarify what that was again? I'm just not sure that I heard that right, what we have going through in the system.

MS. MCMAHON: I think your point is interesting when you talk about your system. I think if I understand correctly, you would have one system running for all of the EMTs - is that correct?

MR. PORTER: Correct.

MS. MCMAHON: So when Marc and I are speaking, I mentioned at Capital Health, we have almost 300 applications, so when we're doing backup we're trying to make sure that we are storing and backing up based on how critical we need to recover. Right now, as Marc mentioned, because of the need to have the redundancy we do keep things in different places.

One application we have is called Horizon Patient Folder, and that has eliminated Capital Health from creating paper charts since around 2005, 2006. All the documents that are written on when you arrive for a visit, within any of our facilities, are sent to health information and get scanned and indexed to the patient's record, and then we no longer keep the paper. I mentioned we do 34,000 sheets a day, a million a month, so it's a lot of paper.

MR. PORTER: That's what I thought you said. I was actually going to ask - you sort of answered what I was going to ask you - what do you do with all that paper?

MS. MCMAHON: We keep it for a short period of time and then we do destroy it because we do back up the electronic information. So that's how we manage that.

MR. PORTER: Thank you and, as I said, I was just kind of curious as to - that's a lot of paper - how much storage area do we have around with all of this stuff in it, assuming that you probably did move to the scanning option and filing accordingly, which is great but . . .

MS. MCMAHON: I would remind folks that those papers coming down were being filed by hand, so the technology has really - and we would have a large number of people every night trying to file, and they couldn't get it on the chart fast enough because the charts weren't keeping up with the paper going. So now we scan those documents every day within 24 hours. They are done, uploaded and available to the care provider so it's pretty fast for their availability. We do store it with Iron Mountain and then we do have a confidential destruction policy with those.

MR. PORTER: Thank you for that.

I'm just curious as well, as the technical folks and as you work toward tomorrow and long after that, and with the leading edge of technology changing so quickly even in medicine as we know - is there a point where you ever see that you're off of paper, you know, the nurse is standing in the room and they go bang on that computer screen, it's already up there doing their thing, and I'm quite familiar with the setting that says I just did this or I just did that, I know where we're using it and I'll reference again, the paramedics in the streets are using their tablets. There was a reason for that and albeit you have 300 systems, we're dealing with one, so it may not be a great analysis, but it is similar in nature.

MS. MCMAHON: We are doing that now, we do have some pilots running where we have physicians using iPads and they're using wireless and we use a technology that they can access their clinical systems on those devices. Earlier we discussed that we are working on implementing the clinical documentation that would be done right at the point of care, so we would, hopefully - my dream would be to eliminate all that scanning and that paper.

MR. PORTER: Obviously there's a bit of a cost associated with that, that's one of the reasons, and when we're looking at tightening budgets and trying to reduce the figures, I would probably see that as one of those areas of consideration.

MS. MCMAHON: Yes, and we factor that into the business case. Even with the scanning we had a return on investment at Capital Health over three and a half years on that application. If my memory is correct, I think it was about $3 million, and by doing that work we eliminate all the paper charts that you would have, and over time we reduced the staff, obviously, because we can do it much faster.

MR. PORTER: Thank you for that. Now I want to talk a bit about the data in general. In the past we've had folks before us here in this committee - maybe the deputy at the time was talking about the issues of access and passwords. There were a lot of problems for a while there about who could access patient information and things like that. I know in my area there were a couple of calls from families who were involved in that, and to say they felt violated was putting it quite mildly. You may recall some of that.

What's been done since then to try to tighten the system up? I know that if you were a ward clerk - and I'll just use some examples here - you couldn't access patients' records, or if you were a clerk you could only go so far and then it was the next step, and perhaps the doctor had all the authority. Where is this right now? How is this working? Have there been changes made to the way this works?

MS. GAULTON: It's an interesting division between what you can achieve electronically in that situation versus what is a matter of trust in accessing records. In these instances, we need health care providers to have huge access to patient information. We need it for quality care, we need it for safe care, and so as folks have indicated, at the front end we're very careful about who gets access to what. But sometimes, even in situations

where people are allowed access - they need it to do their jobs - you can have situations, of course, and they're very rare, where that is not that case, where we've seen some problems arise.

On that front, we absolutely look at what we can do from an auditing perspective to both reactively audit as we get complaints and proactively audit to identify that. Those are huge ways to be teaching our people about how important it is, and we work all the time around increasing education on this front. There are loads of things, but one of the things at Capital Health now is a mandatory re-education program on the fundamental importance of confidentiality, and in fact, re-signaturing - if that's a word; it's not - off the confidentiality pledge. That pledge is very front and centre.

PHIA and its introduction actually provide us with a great platform. We have to educate on it, in any event, and really start to hammer home the confidentiality. As such a fundamental issue, it provides us with that additional forum to have those discussions.

MR. PORTER: How much time do I have left, Mr. Chairman?

MR. CHAIRMAN: You have two minutes.

MR. PORTER: Two minutes, thanks. I don't have a lot of time, but I'll just say thank you for that. I was kind of curious. The auditing piece is one thing, and I think we have to constantly be doing that. I also understand sometimes you just can't control what people do, either, but I was curious about - how can I break it down? - maybe the access piece. You know, front page and you can have access if you're this, two or three pages and you can have access if you're that. There are different levels. I think that was what everyday people understand.

How do you get to a certain thing, especially when you're passworded? It's technology - I mean, it's a matter of writing a program, I assume. Again, I'm not technical by any means, but people wonder how you get that deep into it and how they could possibly know so much or go so deep into something whereby certain levels of people just shouldn't have that access. That was a pretty serious issue, and I guess I can't stress that enough. I'm sure people are still wondering what's been done, and I think that to your point, that's good that we're doing more, and I think there's always more we can do by way of education and everything else to go along with that.

I don't know if anyone else wanted to comment - I know we're running down on time - but I'll finish. Thank you, Mr. Chairman.

MR. CHAIRMAN: Ms. McMahon. You only have about 40 seconds.

MS. MCMAHON: I will make a comment, and this relates to when I was cut off with Ms. Regan. We don't give carte blanche access for everyone. We do have tiers, so if

you are in the direct care you would be rated as Tier 1, and you would get broader access. So your clerks - we actually segregate the types of documents they can look at. It's not across the board - we have a general approach to that. There are some cases where, because of the work that someone is doing, they may have broader - but we can segregate the documents they look at. If someone is approved for research, they come in and we actually will - there is quite a process they go through for ethics . . .

MR. CHAIRMAN: Order, please. Unfortunately, you've run out of time.

Mr. Epstein.

MR. HOWARD EPSTEIN: Thank you very much, Mr. Chairman, and thank you all for being here, this has been quite interesting. I just want to ask a few odds and ends of questions. I'd like to start, actually, with something about the extent to which the records are now electronic. I think we heard that there's a lot of generation of records electronically and then, I assume, a form of conversion or scanning that would take place.

The first thing I wondered was whether there are some documents that are not suitable for conversion to an electronic basis. I wonder, for example, about handwritten notes or are there certain kinds of X-rays or other forms of diagnostic imaging that might not be electronic? I'm not sure and I'm wondering if you can tell us about that first.

MS. MCMAHON: I'll finish up with that very quickly. We have our diagnostic imaging and lab. That information is - I talked before about interfaces - that information actually gets sent electronically to that Horizon Patient Folder, so it all gets archived as the complete record in that system. All the documents that are handwritten are scanned so that's why we have 34,000 a day. Everything is scanned and put into what we call Horizon Patient Folder. That's basically the same as the old paper chart you had years ago, it's all in that system now, so all available to view.

MR. EPSTEIN: Thank you. When did the system at Capital Health become all electronic?

MS. MCMAHON: That system went in in 2005 and it took us a couple of years to pull it across the district. Again the lab system, those were in place beforehand, diagnostic imaging was in place beforehand, as was our pharmacy system, but they do interface with that HPF and created a complete chart.

MR. EPSTEIN: And what's the situation with old records, pre-2005 records?

MS. MCMAHON: Oh, that opens up a good topic. It's one of the bees in my bonnet. In the Act that we have here in Nova Scotia, we keep medical records for 25 years. It was 20 for a while then it went to 25 because of the food and drug, and requirements when it was a research record.

I would add that many provinces have gone to a 10- or 15-year retention because it's very costly. I did a survey around international bases and 10 to 15 years is kind of the norm. At one point, before my job changed, it was one of the things that I had hoped we might talk about as a province - our retention period. Right now it's 25 years and that's in the - I think it's 20 years in the Health Act, 25 years at Capital Health because of the research component.

MR. EPSTEIN: So there has been no attempt to go back and make the pre-2005 records electronic, except those that already were.

MS. MCMAHON: We have almost two million charts. You can't make them electronic because electronic works, the form, you have to bar code it all and that bar code is read in the scanner and that's what indexes it to the right person's chart. There are actually two codes on it: one bar code is the patient's when they come in, the bottom one says that's a nursing progress note, and that's how it gets indexed. So if I was to pull up a chart, I would be able to see there are 70 document types, so as a clinician, I can go and say I want to look at the progress note for the last visit, I want to go see the ambulatory care visit, I want to go see this and that is how they would find it quickly.

MR. EPSTEIN: Are these records searchable? By which I mean, we've talked a lot about the security aspect but if, for statistical purposes, you needed to pull out information, are they all searchable? I see, for example, just to focus on the IWK stats from time to time about numbers of children who are injured in certain kinds of accidents, these stats must come from somewhere, and I'm assuming that unless someone is just keeping an eye on them as they float by, that they're probably searchable. Is that the case?

MS. MARDLIN-SMITH: That data that you're referring to is actually coded and abstracted, if you will, from another department and that department uses the International Classification of Diseases, well-known as ICD-10. Coding and abstracting has been going on across the country for 25-plus years, so those statistics that we're able to mine for data and provide that is available through another means.

The scanning and archiving component, which Capital District Health Authority had implemented several years ago, is also now a provincial initiative for the IWK and the other district health authorities. The IWK has just, since about February, has moved forward with actually scanning our paper documents into our electronic medical record. It's a different system than Capital Health, but again, that is where our files are able to be scanned so that they are then accessible to clinical care providers who have been previously authorized to have such access.

MR. EPSTEIN: Can I ask something about the share portal? As I understood it, this is something that would allow family physicians to have some access to the hospital records. Did I also understand that the hope would be that there would be some mutual

sharing so that the hospital might also have access to family physician records? Is that the basic idea?

MR. LEBLANC: Right now, you're correct in that. Physicians who sign up to view the share portal have access to certain data that's from the hospital information system: lab data, DI data and some electronic reports. Eventually we would like to have the general practitioner and specialist data to be able to be accessed as well, but right now it is not.

MR. EPSTEIN: I know our focus is on the hospitals, and I heard you mention earlier that there are some pilot projects underway; can you just tell us to what extent family physicians in Nova Scotia actually are using electronic records right now in their own offices?

MR. LEBLANC: Greater than 50 per cent are using electronic records. I haven't got the exact numbers, but I can get them, but greater than 50 per cent of family physicians and specialists are using electronic medical records in their own practices.

MR. EPSTEIN: I think I cut you off a moment ago. Did you want to finish on your point about the sharing?

MR. LEBLANC: No, just that we hope that we will get there someday that we have it all available.

MR. EPSTEIN: Thank you - I was just conscious of time. Can I ask something about the nature of the breaches of security that might have taken place over the last number of years? I know people are, naturally enough, very sensitive about their own personal information getting out there and yet at the same time - so far as I'm aware - most of the instances that I can recall having ever heard of, sounded as if they were more along the lines of people being nosey about their friends, neighbours, and relatives, or maybe curious about a celebrity if someone showed up who is well known.

Is that really the nature of the breaches or has there been something else? I ask because of this: we've had a very famous case, in Halifax, of a breach of military security where we now have a Mr. Delisle serving time in jail for selling secrets to a foreign power. Is there something marketable? I assume there is something marketable in the health information, but have we run into this or have other jurisdictions in Canada, or is it mostly of the nature of personal nosiness?

MS. GAULTON: In fact, the notorious cases that we hear about are not electronic access and those beg - someone who is tapping into the records electronically from their computer at home or any of those types of things. As we indicated, we monitor for that risk, but it's not the breach that you hear about in health care.

It's interesting - I'm a lawyer - but if you participate in things that deal with the confidentiality of health information these days, they actually do start to discuss that as a significant risk and yet we don't see it as having materialized because of the systems we have in place. We are largely looking at situations where someone appropriately has access and then there is a use of that that was not on a need-to-know basis.

MR. EPSTEIN: But that gets back to my question. In terms of incidents that have actually occurred in Nova Scotia, has it essentially been hospital personnel satisfying their personal curiosity about someone else? Is that really what we're looking at?

MS. GAULTON: I won't speak to the motivation of people on that front, but those are the ones we hear about, instances where there has been a person who is accessing as opposed to an electronic failure of security.

MR. EPSTEIN: Have there been larger breaches of security or attempts that have been rebuffed?

MS. MCMAHON: I think in your kit we provided you - from Capital Health's perspective, we use a multi-layered approached for security for the IT systems. That would start with HITS as the umbrella. It's a private network so they have their firewall and they have security in place. At Capital Health we also contract with an external company, and they just sit and run a program on our system, constantly, to tell us what threats are happening.

In one 12-month period we had 1 million attempts of those over that year, 20 were escalated, none breached the system, but they were escalated to the point where our security went in and actually did some work to make sure that they didn't get any further. So we have a multi-layered approach. We also have encryption on our laptops. We also have a system called – we've referred to it as NAK - and basically what that is is if someone comes in with a home-router, or something that is not authorized, and plugs it into our system, it blocks it and shuts it down. It actually tells us right where they are. So Catherine was speaking about people who have access legitimately, and then, perhaps extend what they believe that access granted them.

MR. EPSTEIN: And that was really what seems to me to be the typical case, but you're not telling us about possible attempts from some external actor to access the system generally. Do we know anything about why any entity would do that?

MS. MCMAHON: I would say any company today that has technology has that happening all the time. Hackers just sit there and try to fish through. Banks would have the same setup, hospitals all have it; your departments here have it, and I'm sure the Auditor General has it.

MR. EPSTEIN: So the target, I assume, would not, probably, be so much the health information as things like names, address, date of birth, and maybe telephone number, or something like that, that is marketable?

MS. MCMAHON: Some of them are just fishing to see what they'd hit. Who knows? So we target that. I would speak in terms of my previous role, when I managed Health Information Services. I know over a - I think it was, six- or seven-year period - I had one employee breach that I investigated. So I would suggest, based on the volume that we have - 12,000 employees - the amount is very infrequent, and I would say our care providers take their work very seriously. I have even had calls from care providers who said, I think I hit something incorrectly and I don't want anyone to audit me and I'm really sorry and this is what I did. So it would be very unusual. And I think, when we refer to some of those media stories, they get that attention because it doesn't happen that often.

MR. EPSTEIN: I agree. And thank you very much, that's a big help. Thanks for your presentation today.

MR. CHAIRMAN: Thank you, Mr. Epstein. I will now give the two organizations a chance to wrap up, and I'll start with Ms. McGuire.

MS. MCGUIRE: Thank you very much, Mr. Chairman. I think as you can see by all of the comments, questions, and answers today, our commitment to protecting personal health information of each and every patient at the IWK is a very strong one, and we take our role as custodians of this information very, very seriously. We do look forward to enhancing our existing security protocols, as we make continued progress on implementation of the Auditor General's recommendations. We look forward to harnessing opportunities for system-wide enhancements through initiatives like Merged Services Nova Scotia and PHIA. And patients and families, in particular, should be assured that their information is securely managed by the IWK. We'd like to thank all of you for the opportunity to discuss this very important topic with you today. Thank you.

MS. POWER: Thank you. I, too, would like to thank all of you. We always welcome an opportunity to be able to talk about what we're doing at Capital Health, and hold ourselves highly accountable to each other, but particularly to you and to the citizens we serve. So when there are any indications that we're not living up to the standard that we hold ourselves to, we always welcome an opportunity to see that, to do better, and to speak to you about that. So thank you for the opportunity. This is a hugely important area for us, and I know that it's a hugely important area to our citizens, to know that we hold their information very closely to our chest and use it only in times when we need to, to provide care to them. So thanks very much.

MR. CHAIRMAN: I'd like to thank you very much for coming today. It was very interesting and very informative, and you do have a difficult job on your hands. There were a couple of requests through the system. Ms. Kelly had asked for pilot project numbers, and

the clerk will send detailed information, and Mr. Epstein also asked about the number of physicians using electronic data in their office, so if you could provide that, it would be great.

Again, I'd like to thank you for coming today. I look forward to many improved things from the department as you move forward with this very complex issue.

That concludes our meeting for today. We will have our next meeting next week - it will be the Public Trustee Office. And just after we adjourn we're going to have a presentation by the Auditor General, for the committee members only.

So, again, I would like to thank you for coming.

A motion to adjourn would be in order.

MR. CLARRIE MACKINNON: So moved.

MR. CHAIRMAN: Thank you very much.

We stand adjourned.

[The committee adjourned at 10:55 a.m.]