Health: Protecting Healthcare Data

Speaker:
Mary Jane Dykeman, Partner & Co-Founder, INQ Data Law

Moderator:
Lauren Eikerman, Rogers Cybersecure Catalyst Team, Ryerson University

Lauren: Welcome everyone to our workshop session for the health care sector called Protecting Health Data.

We're very excited to have all of you here today.

My name is Lauren Eikerman and I am a member of the team at the Rogers Cybersecure Catalyst at Ryerson University and I'll be pleased to act as your moderator for today's session.

And we are honoured to have Mary Jane Dykeman with us here today to lead today's workshop.

Mary Jane is a partner and co-founder of INQ Data Law.

Her practice focuses on privacy, data governance, cyber security and artificial intelligence, helping organize innovate with trust.

And she's a longstanding health lawyer and helped developed Ontario's health privacy legislation.

Mary Jane is a chair of the board of the Alzheimer's Society of Toronto and Deputy Chair of the Research Ethics Board at Canadian Blood Services.

She also teaches Mental Health Law at the Osgoode Health Law Program.

Welcome Mary Jane.

Mary Jane: Thanks very much, Lauren.

Oh sorry, I didn't mean to interrupt you.

Lauren: Oh, no worries.

Just a few quick housekeeping items before we get started today.

So, the hopes of today's workshop this afternoon is to generate good discussion and good questions.

So, as Mary Jane gives her presentation, please type your questions in the question box on the lower right hand section of your screen and you'll notice two little icons, a chat box and a question mark.

If you click on the question mark before you pose your question it will filter it as a question for me and it would be helpful to filter them at the end.

And the questions will come directly to me, so I'll post them after Mary Jane starts her presentation.

So, this will be a large workshop group and I may not be able to pose all of your questions to Mary Jane, but I will certainly try my best to identify repeated questions or emerging themes.

So, without further delay, Mary Jane, over to you.

Lauren: Perfect, thank you Lauren and thank you to the Catalyst as well, and then of course, all the attendees who are here through the day today.

I think you met my INQ Data Law partner, Carole Piovesan this morning on the panel and I wanted to come in to talk a little bit about health.

So, I was very pleased to have that invitation.

As Lauren said, I've been working in the health system for a very long time.

I came into the Ministry of Health and long term care legal services branch in the summer of '95 as a summer student.

File number one PHIPA and the fact that we were looking to create health privacy legislation and as many of you know, it came into force November 1, 2004.

So, it took some time, it went back and forth to a different part of the ministry, the then Ministry of Business and consumer services and came back ultimately and this has been the focus.

So, when we talk today about cyber, VPS, what's happening around the world frankly, we talk about cybersecurity and yet back in the day, PHIPA was not necessarily about all of the electronic systems, we did not draft into it specific protections, we said you must safeguard no matter what the form, no matter what personal health information or PHI it is, no distinguishing as to sensitivity of one piece versus another.

But here we are in 2020, we have many, many shared systems, we have electronic health records, we have lots of ambition frankly around what we do with this enormous amount of data that we have access to and what are those points of access.

We have questions about data governance, questions about methods of the identification, how can we harness data.

And we often say how can we do it responsibly so that we can innovate as well.

Healthcare in particular, and of course that's my bent, and if you're here today it's because it's what you're interested in.

And I do think that health care data is special, we're gonna talk a little bit about that as well.

So, I'm going to run the controls on this, I am going to ask the question right up front, is health care a snowflake? And by snowflake I don't mean that it is so precious, but I do think of it as special.

And if you were to put it out to the public, they would likely have the same expectation.

In fact, I think they do have that expectation.

And they may be slightly more jaded now because pretty much every single day there is something on the front page of the paper and across social media about a cyber breach, it was not hard to go and look for health care examples or other examples of sensitive data falling into the wrong hands, whether that's something that happens internally, whether it's something that happens maliciously or inadvertently or by cyber criminals somewhere else.

We think of healthcare information as being special.

We know that it has protections that apply to it and obviously PHIPA will be modernized and has been modernized in some ways.

We know that (UNKNOWN) is also under consideration to be modernized as our trade partners go forth and make key changes.

We've watched GDPR, we've watched the California legislation CCPA also create standards as well.

And I was invited to a conference with one of the attorney generals in Connecticut in the spring, not surprisingly it got parked to fall, then it got moved to spring again, if we're lucky it will go forward in May.

But as I was doing that research, I was looking at one state to another and how they handle specifications around cybersecurity.

There's always a question about what should those standards be, should they be legislated, what is the direction that either government will take or other industry partners will take to do things like the identification or to adopt certain standards in the time as we await something legislative.

We look at that at INQ as well because we do a lot of work in artificial intelligence and, obviously, machine learning, these large treasure troves of data, but the legislative rules are a problem.

(BACKGROUND CHATTER) We're talking about artificial intelligence and the fact that there is no specific legislation.

So, we talk about what are those guardrails that we can create in the meantime.

And I would say cyber is the same thing, but the imperative in Ontario in PHIPA is, of course, that it says there is a duty to provide safeguards, administratively technical safeguards.

It's a matter of what do we do with that and we have a changing landscape which we'll talk about.

I think I've covered a little bit about this and then all of a sudden we have cyber literally knocking on the door.

Just a backdrop, again, as you know and many of you may be in it daily, the reminder all of the different consultations going on, it actually is not just PHIPA and it's not just within health, but in government generally.

We've just come through the data interoperability submissions and consultation and the consultation paper that was released and it posed a few questions that I don't need to go into in detail here.

I think this is an excellent opportunity, I know industry was pleased to see it, the hospitals were pleased to see it and to be part of the conversation because we do need to crowdsource at a certain point.

We need to not necessarily reinvent the wheel or make it all about us or one player, but to come together to have an implementable solution.

And when we were working on PHIPA, and again that's a long time ago, it was very much a how do we make it work at the front line.

And we can go back and forth about what is good and right about it, what could be changed and modernized, particularly where we were not dealing with electronic health records, what about the definition of the identifying, what is it that we do with that.

But I just thought it was an exceptional opportunity to work through some of this and to have some input into any kind of specifications, including around cyber requirements and standards to.

As long as they are nimble and could be updated because the technology is moving so quickly.

One of the other things I can say is that working with health sector clients and health sector providers obviously this is very much on their mind.

People are aware of PHIPA and the requirements, but in particular we're spending a lot more time on the potential of a threat.

So, for many years we were talking about unencrypted devices, we still talk about that obviously, and the IT people are continually pushing us, let's get those standards in place.

There's always this question of where is your greatest risk, is it from an external threat or is it the people in.

Do they know what to do? Are they well equipped, are they well trained and how do we keep up, because obviously threats are changing.

In any case, we are looking to see what may come of the specifications that arose from the data interoperability consultation and I think the timing originally was to be today, October 1, I am sure it will come because there are many of these health data and broader data questions and conversations and consultations and some action coming.

And yet, these other questions and topics are on the move as we speak.

I've just posed a question in passing, what does it mean for procurement? Let's assume that we get to a point that we have the standards that are generally adopted, either imposed by law or on some sort of consensus, and what does it mean for procurement.

Our firm, especially on the DDO health law side, does a lot of procurement work and a lot of shared systems work.

And if you draft our FPs and if you are in-house creating those reviews and systems and assessments, where is the expertise then because for anything that's procured you're going to have a technical group that can take a look at what a proponent is putting forward and weigh it against whatever the criteria happens to be.

And so, how is it that we do that? And we know that some time ago it was about audit functionality and even the information and privacy commissioner of Ontario was saying at the time, coming out of some very bad breaches where audit functionality was front and centre, where did the person go in the system, what did they look at, how long were they there, what did they do with that information.

Now, we're at the point where PHIPA has been amended, I believe it may not be enforced yet as to that clause, but that requirement is now being baked in.

And so, we can anticipate that as we start to move towards cyber standards, again, they will either be legislative or there will be this, I don't wanna say rising up, that sounds rather dramatic, but there will be this opportunity to create a standard so that there is some guidance and harmonization.

And, again, you don't want to start over.

My law partner, Kathy O'Brien, often says, 'I weep for the taxpayer.

And what she means by that is if every group starts over and does it in-house, then that is time and energy and money taken away from the core group that organizations want to serve, being the patient, the resident, the client and the system.

And, of course, we looked at other jurisdictions also.

I don't need to go into detail again here, other things that are on the move and being put forward and have had consultation as well.

I just draw your attention to the one at the end.

I believe it was October 1 initially, but has been extended.

Now, that's not health, that is a broader government consultation on private sector, privacy legislation for Ontario, question mark mainly because it would be a mini (UNKNOWN).

We need to sort, does it make sense to have it made an Ontario statute in that manner, will (UNKNOWN) be modernized to meet some of those issues.

But the fascinating thing about that consultation paper, which is still up and open, is that government attached to it a series of other questions, really important questions, about transparency and consent and the identification and the like.

So, all of this is very much on the move and then let's just come back to.

I don't need to give you a definition of cyber security as well, I've already posed the question.

Carole and I paired together fairly recently to write the cyber chapter for Mondaq, which puts out a lot of legal resources.

And there's some case law and we draw on some case law to inform the cyber narrative.

Just probably brought a few of those.

So, what do lawyers do? They go to, well what would be the offence, if someone did something, mischief, hacking, identity theft, knowingly intercepting private communication, wilful is in quotes, fraud.

So, these are all conscious activities of someone to step in and create this harm, defrauding people.

I suspect in due course they will amend the Criminal Code and possibly add other elements as well as to the scope of cyber infringement and offences.

Can due diligence help you? We take you back.

This is not a health case, but it is a cyber case.

And I only raise it because it points to what made an organization do, even if it did its best to protect against that threat, which is ideally where we want people to be.

We want them to be as up to date as possible and as ready as possible.

And then as you know with cyber, there can always be a twist, but I just raised this one because the judge in that case ultimately said Home Depot actually was shown in a good light in terms of the timing of the response, they were responsible, they did what they should do, the liability in quotations is negligible to remote.

Now it's interesting, over time as we learn more and there are more of these attacks, I wonder if someone could actually take a look at this and then say, well maybe the climate has changed.

We don't know whether even in these four short years that a case such as this would be decided in the same way.

But the due diligence piece I thought was good.

And then contrast, Equifax, of course, as you're aware was not a cyber case, but really more about the diligence upfront and the responsiveness in the aftermath can make a difference.

And we've thought about that throughout the course of various PHIPA breaches, what could someone have done when we start to talk about ransomware, for example, and we'll come back to it.

When we think of ransom where we sometimes talk about keeping up to date, and I've got a couple of cases where we're working together and pointing to what might make a difference, wow can you be diligent upfront.

And then, if it happens to you, it's also in the way you respond to it.

I added one more case again just in terms of a case that set out in some detail well, what are the technical things.

And I'm not a technical person, per say.

I've been hanging around the IT groups for a very long time, almost as the bridge sometimes between getting something to either legislation or policy or privacy response, and privacy and security go hand in hand.

We can talk cyber while we're talking privacy potentially.

So, in any case here are just a few things that in that case it was pointed to the fact that you need to be technically on top of it, in fact you need to be ahead of it.

And I think it was probably last fall, I had an opportunity to be in New York with the CEO of Splunk, a cyber company.

And I was just amazed because so often over the years we would be bringing security experts in if there were a breach and sometimes the work was quite agonizing, they were experts, make no mistake, they were forensic experts combing through the system, but it was almost like putting a puzzle together, putting the pieces back together.

And what interested me, and I don't have any particular affiliation with Splunk, but listening to the CEO and seeing a demo of what they do I think things have shifted, they've probably shifted some time ago, you'll tell me, where we can watch in real time the threats on the system and the visuals are better and we can show we averted X number of attempted attacks.

So, I wear my hat as a former in-house counsel to a couple of the teaching hospitals and I think of our clients today and I think of how different board members have sat up very straight.

Usually when they're sitting on a board they're sitting in other positions.

And coming into the board and taking very seriously some years back we talked about privacy for a long time, all of a sudden we're also talking about security and it makes it very real when this is the kind of impact that can be had because it's electronic information with a few keystrokes or ransomware that is embedded and could be sitting there for some time and then dispatched, it's absolutely possible and likely that you can have many, many people affected.

And it's that swift and relatively easy and the fact that in many health care organizations we have lots of systems, we may have our key systems, whether it's a (UNKNOWN), we have lots of legacy systems as well.

And it is, I'm sure, daunting in many ways to consolidate to be able to stay ahead technically.

And then, we're gonna talk a little bit about third party vendors as well.

I leave this with you because, as I said, I can say the words, it's like all of the health records that I've looked through over the years as a health lawyer and I'm familiar on a lot of counts, but I'm not the clinical person.

I'm also not the technical person and for some of you this is going to be.

You may have a different list that you would add to or take away.

Internet of Things, of course, is a worry.

We see lots of media attention to vulnerabilities in terms of third party components, third party vendors, but connected devices, need not be a third party vendor and we are living it through the course of COVID since March.

Obviously everyone's aware, so many people have quickly moved to work at home, for example.

And maybe we got them home quickly and we're glad that we could keep them up and running and keep our programs and services seamless.

Obviously in health care there are some groups that need to be on site if you're running a residential facility or an ambulatory clinic or a place where people need to be, but there are many programs and services that wrap around the client, the resident, the patient where we could have people at home.

And the scramble, and I'm sure for many of you, there was a scramble to try to figure out really quickly, what about the data, what about the device, what about the protections for it, what about the fact that people are on their own phones, what about their own laptops, maybe it's a shared family laptop, maybe it is not secure.

And ultimately I don't know what the legal concept would be, but it's sort of like a forced measure of we need to do what we can in the moment because the most important thing is to keep everybody safe from a health point of view and to not disrupt the business.

We can talk about business disruption all we want and we may have the technical backup and the data is in the cloud and everything else.

But even to access that data.

And I was getting calls saying we need to pull out the work at home policy and actually let's park that for a moment, let's get back to can we continue to deliver the services that we need to, how do we make it seamless, how do we make it safe.

And then, of course, the next component is the fact.

And it's probably not right there on the slide.

I'm gonna come back to the work arounds 'cause that's important, but just the fact that there's so much data, there is so much new data even related to COVID and it is a pressing.

Mary Jane: Problem for society, we need to use the data that's been created to try to figure out how do we go forward? We saw that in SaaS 17 years ago, and I was working in the healthcare system at the time.

And there are lots of questions then how quickly can we do research? I sit on the board of the Research Ethics Board at Canadian Blood Services, different studies coming in, we wanted to make sure that as we were agreeing to data going for blood products, for that matter, that we had the rigour, but we had to move swiftly because this is literally, and not to be dramatic, but it's a life and death scenario to see some of this research go forward.

I wanna come back for a moment, though, to the workaround issue.

And what I've said is we need some arrangements likely across all kinds of work settings to keep programs and services running, and not see anyone fall into the gap.

The workarounds, as I said, might have included using your own phone, laptops, connections that are not secure.

And my question is, did we go back? And we do it quite often in healthcare, we do a work around when there's a crisis, and we're in the huddle, and we troubleshoot really quickly, and what could we do? And maybe stop that flow of data, or we shut down that system and we're always trying to think through OK, let's just pause it for a moment.

Let's just think if we do that, what is that downstream effect and impact? OK, we looked at it, we weighed it.

We somebody documented it to show, we turned our mind to it, someone may come back later and say, well, that turned out not to be such a great idea.

Well, we had to make a decision in the moment and we wanted to be thoughtful, same thing with these workarounds.

And has there been enough pause between the first wave and the second wave to revisit who's still sitting using their own phone? Who is still logging in in a different way or not logging in what are they doing with the data? What about the.

I mean, clearly, we're here to talk about cyber and what threat that created the Internet of Things itself, even in a pre-COVID day, has had its impact already, anything that gets connected to your system can be that conduit in and what do we do in terms of both setting the policy and then ensuring that it's followed as to how people use your Internet resources and what they plug in or whether they technically people will find workarounds all the time, if you say oh, no, use a VPN, and you won't be able to print from the VPN.

And then they say, well, I sent it to my son's Yahoo address.

You think oh, OK, that's not quite what we hoped for ultimately, but I just it's a caution to go back to the to the workaround issue.

So let's just see, just a couple of quick comments, I'm gonna do a little time check.

Medical devices and third party vendors, medical devices I've been thinking about for a little while, just really taking a look at how much data is collected within certain medical devices? So this is not on Epic or Meditech or whatever point click care system in healthcare, it's on a likely third party vendor device and years ago, everyone was panicking because even photocopiers, the technology was getting better.

Photocopiers would then store the data, I pretty sure that your kitchen appliances store data, your car stores data.

So I was wanna know a bit more about the data that is stored there.

What was probably much more terrifying was reading about the Ripple20 cyber attack very recently, hundreds of millions of gadgets affected.

But when I think gadget, I think of a little gadget, I'm not thinking medical devices, some type of pump, for example.

And the backdrop and some of you will have seen this 19 hackable bugs in the code that was provided by this company Treck, the impact on health care.

So health care was just one group that was affected, but it caught my attention.

It will catch your attention in terms of you know, to the extent that someone could step in from away and tinker, tinker sounds not as serious as it is with a medical device such as an infusion pump.

You know, this is the stuff that movies are made of.

And I do go back and I know I've said it before, but it was reading a few months back the book Sandworm and its geopolitical cyber attacks and everything else not specifically healthcare.

But toward the end, there's a comment from Brad Smith, the President of Microsoft, I think speaking at the UN, and he basically was speaking about health care, attacks and breaches and said, he cited one group whose philosophy is listen, "if you get attacked, just go find someone older than you who knows how to do it manually".

And that just gave me pause because when you read daily about the various cyber attacks and whether or not we're properly patched, do we have a backup? Do we pay a ransom, et cetera? If our systems go down in healthcare, the outcomes could be very poor.

And what do we know about those manual ways that we use to do things? We don't wanna return there forever.

But let's talk about workarounds.

Would people even be prepared to do a workaround? Do they know what to do? But anyway, that book itself is worth a read the remote code execution is again, the one that's terrifying.

Someone can hack in from a way and change something it's worrisome if it were transportation, it's worrisome in a financial setting, it's very worrisome, of course, in a healthcare setting.

OK, I think I must be almost done.

Just a bit more information about Trek itself.

And as I said, legacy systems, need for patches, some other technical stuff that could be important to you.

Even VPNs are only as secure I board chair one time, said when I was walking through privacy and cyber, and I think there must have been yet another unencrypted USB key case.

And he said, 'could it happen to us?' And the CEO sort of caught my eye.

And I thought, was that a signal to say, no, we've got it all under control.

And I said, but here all the things that we're doing, I've always thought we're only as good as the next unencrypted device that goes out.

And now today with some of the cyber situations, it holds true.

We've already talked about procurement, the someone's has asked just cut it out of the corner of my eye.

The book is Sandworm.

And I it was the first time I listened to an audible book, and it was on audible and again, terrifying and dramatic to be listening to it late at night in the dark as they tell the story of the Ukraine, essentially shutting down as a result of cyber.

So just to close I thought well, she put up a recent example, as I said, we see this every day at INQ scan, and look every day to see what is happening around the world, whether it's a privacy development, whether it's Internet of Things, and including cyber and major hospital chain in the US, Puerto Rico was hit by a ransomware attack I've had a couple in the past week, it's happening all over.

There was media today about TELUS Health, having been hit in two of its companies and having paid a ransom and we don't need to get into the pain versus not situation.

But in case in this particular case, Universal Health Services also was hit and had to be redirecting people I did read of one case, it wasn't necessarily Universal Health Services, though.

One case where someone had a very bad outcome, critical incident based on surgery being delayed by virtue of redirection and I read someone speculating maybe that's one of the first demonstrable cases where someone has really suffered terribly as a result of ransomware.

And with that, again reportable to IPC, yes, Blackbaud breach I raise only because, it affected health charities, foundations, schools, and the like, and there's no legislation that applies.

So there was a big scramble to sort out, do we have to report to a commissioner? No, we don't well, we should write letter and give notice, what's the letter going to s ay Blackbaud paid the ransom, staff need to know what to do quickly.

And then obviously, ideally, you have systems to detect or to find it once it's there, in that you have backup, of course.

And then I close with a Noble declaration from some of the cyber criminals at the outset of code.

Remember, everybody put up a COVID statement.

You know, safety is our priority.

There's a certain theme to them, and I'm not making light of it.

Cyber criminals did the same thing.

We endeavour not to attack healthcare organizations during this terrible global crisis.

Of course, that did not last long, maybe some of them held by it, but others went full tilt and in fact, use cyber use COVID as the entry in.

So I think I will leave it there, I'm surely finished.

So I say thank you and thank you for attending today.

I think Lauren will be coming back to us, let me just start reading again.

Lauren: Hi Mary Jane.

Mary Jane: Hi there.

Lauren: Thank you so much.

For all your insights that was really excellent presentation and very informative.

Mary Jane: Got did a book recommendations.

I see countdown (CROSSTALK). I may have to photograph that or ask you to remind me later.

So Sandworm (CROSSTALK)

Lauren: Write it down for you.

(LAUGHS) Yes, thank you so much.

Yeah, everyone, please keep your questions coming in.

And we can continue the discussion.

But one question that came in so far is that the Intentive Data Privacy is to establish data collection rules, information disclosure, data act and data access rights, do you think policies written thus far, are effective? And with the following pattern in mind so results, output and intent?

Mary Jane: Well, it's a great question, could we do better? I think we could do much better.

And I remember the Federal Commissioner made a comment, probably at least a year, it might be longer year and a half ago, really slamming the 6000 word, policy or consent.

And, we know for a fact, we may have done it ourselves, I'm not gonna ask for a show of hands where you get into the Internet, and you want the service and you'll trade your data.

And you get to the piece where you just scroll down and you're looking for the bar on the right-hand side that gets you to the bottom.

I tend to read those things.

But you know, just you may have kids or yourself be purchasing and just literally scrolling down and clicking.

I agree and legally binding.

But what did that thing, say every now and then I come across really great Terms of Use, and great privacy policies, and some of the legalese is gone.

And that really was the call, even in this paper, a consultation that's on now, in terms of, again, I've called it the mini PIPEDA I don't know if government would call it that, to the extent that Ontario proceeds with made in Ontario private-sector privacy legislation, including by the way I didn't mention, because they wish to cover those groups, the non-profit's charities and others that I mentioned in the Blackbaud case are not covered.

I don't think we do enough good work, or we're trying to do the good work.

But ultimately, it's not successful yet it is not playing enough and I could spend another day talking about what is it that the public expects, they put trust in us it's a privilege to hold their data even back in the

McInerney and McDonald case that established access rights to your own data.

That was in the 90s Court of Appeal out of New Brunswick, it's embedded in PHIPAA, and it said, "you healthcare organization, hold the data in fiduciary trust, you own the system, they own the information.

So when I look at that question, I just think, have we done enough and there's a lot of cut and paste probably of policies and or people trying to regurgitate the statute, the full statute into a privacy policy because they're worried they're doing more than they should and it needs to just come down to something much more transparent.

And that was also in the mini PIPEDA consultation paper.

Lauren: Thanks so much.

Another question.

Our doctors are now using email to communicate with their patients.

How good of an idea is this? Can current laws and regulations be used to manage these types of communications?

Mary Jane: Well, when we look at PHIPAA, I think it's a great question.

We look at PHIPAA, we chose not to draft it in specifically I try and I think of how much email we were using in 95 to 2004 would have been some so we did not make a rule around that.

And it got to be frustrating for people, and ultimately, the Canadian Medical Protective Association CMPA, which covers doctors put out some rules in the absence of legislation, the body that provides coverage to physicians across Canada said, "listen, here's our standard.

Here's what you have to have in place you have to get consent, et cetera," there's a document, if you Google it, you'll find it or reach out to me, and I'll get it.

And then sometime after that, and much more recently, the Information Privacy Commissioner of Ontario also then circulated its own guidance document as to when you can move to email.

And what they said in a nutshell was it has to, you know, it should be encrypted, you get consent, and it should be encrypted.

I mean, if it's encrypted, arguably, it's not at PHIPAA.

But ultimately, you have to turn your mind to whether or not it's feasible, because many healthcare organizations said, listen, we don't have one mail we are, even if we have one mail, the people we're talking about sending it to, are not going to have one mail that might be a substitute decision maker of a patient.

So they said, you have to turn your mind to whether it's feasible not to encrypt it, but it is not secure And I think the bigger issue is also texting.

This people we don't have great guidance on texting, either.

I don't know how secure texting is people say, oh, I just bundled everything from the text, and made my own note or I don't know where you download it and print it.

Or some people said, oh, I just didn't consider that to be part of a health record in any way.

And it you know, sometimes it's a boundary issue, we're having more issues now, because people started giving out their personal cell phones through the cause of COVID.

Lauren: And one person just said, SMS is not secure.

Mary Jane: Yeah, that's the issue and so we've got some work to do.

Lauren: Yeah, another question that how would you recommend to IT members of small organization and are or not-for-profit organizations? We're providing care for clients sometimes could trump security recommendations? Is the way is the right way,

Mary Jane: I think this is true.

You've got to get into a network or group again, you cannot, you cannot do it alone, you cannot reinvent the wheel at every time, you cannot have a made in-house solution.

I think this is really critical it, one time years ago, I did a hearing.

And I remember the person said as we were leaving the hearing, well, you know, we can pay you or we could buy some new beds.

And I'm thinking, oh, my gosh, but that your comment is we want to we don't we're not saying that privacy and security is distracting.

But it's some of it is expensive.

And so we've got to get, you know, we're doing some work on some tools to try to, again, crowdsource and best practice, and what can help and what could assist your peer because I agree, it would be very hard, I would say for that person, please do stay in touch because we're starting to build out not just the privacy side, but also the cyber side as well.

It's would be very difficult and again, if TELUS Health got hit today, Lauren, and I were just saying ahead of their an impeccable organization on many fronts in terms of standards, it can happen to anyone, when you read Sandworm, you'll see that everything that happened in Sandworm, came in through a very small shop, and they said something to the effect of we just didn't think it could happen to us.

And it no, it was really quite something.

Lauren: Yeah, same that it can happen and have, you know, policies in place and the plan?

Mary Jane: Yeah, but the crowds, we're gonna have to get together as a sector, I think to, again, not just create standards, but to make it more workable.

You know cyber criminals don't care if they come in through a big organization.

In fact, they I don't say weak link.

I think there's some amazing people working extremely hard.

It's just it's almost impossible, and it's already out ahead.

And, you know, IT gets its moment in the sun.

At this point, you know, you're not relegated, but yet the question is, are you resourced? 'Cause the issue is gonna be on you at some point.

And all eyes are on you and then it's well what did we do well, did we get the resources we need and then we can collectively figure out what do we need what would be the appropriate thing? Because it's a anyway, I don't wanna end on anything negative at all.

I'm just glad there's so much attention to it now because the threats just keep coming.

And we've got the human component of the shiny link, and we can tell people don't click on the shiny link we can put the footer on the email that says watch out for shiny links and I you know.

Lauren: (INAUDIBLE) This is very important.

Mary Jane: Exactly.

Lauren: Thank you so much, Mary Jane I really appreciate all your insight here.

We are coming to an end here so I should wrap this up.

And I know there's there'll be more questions and I wanna assure you that this discussion will continue in many different forums.

I want to thank all of you for your questions and your engagement on this critical topic.

And most of all, thank you so much, Mary Jane, for your presentation and our discussion here.

They were really helpful, and we appreciate your insights and all the expertise you've shared.

Mary Jane: Great, I'm really, really fast to see oh, extra regulation and standard to be developed to protect PHIPAA I mean I do if we can get there and if it doesn't come legislatively, then I think as an industry, basically, as professionals, we've just gotta come to something.

Because that's, you know, as lawyers, and I don't do the litigation.

If you saw Carol Crawford son, my lawyer partner this morning, she's a former litigator, and that will come through, but I'm all about the diligence also.

And what would we pull out to say, listen, we all attended this.

We all were part of x, we all came to the end, and if someone says later, that wasn't quite the right standard.

And we say at least we were diligent you know, there it is.

Lauren: OK, thank you so much.

I think that's gonna be it for today, I just want to give one more announcement, which I'm sure all of you may have heard through other sessions today.

But the cybersecurity centre of excellence at the government of Ontario has created a new set of cybersecurity training modules designed for organizations across the broader public sector.

And they are available on the Cyber Security Ontario Learning Portal.

Excellent yeah, there's a link in the lobby on the lobby page in this on this platform that you can go to, but these are free learning modules, and they will be released at regular intervals over the coming months and the first two modules, concerning breach procedures and Business Continuity Planning, are available today at cybersecurity ontario.ca.

So these modules have been created specifically for you at the broader public sector at the cybersecurity centre of excellence at the government of Ontario, and I urge you to go explore these training sessions with your organization.

Mary Jane: I urge you as well, because, again, if something were to happen down the road, I don't mean we're diverting it to point it to government, I'm literally saying there is a good resource available that is vetted and endorsed.

And we need to hang our hat to something so absolutely I'm gonna go check them out and watch for the next ones that are coming, that that's what we will pull out to say we were in this group, we went and looked at those we started to work our way through them, we adopted them.

And you know, then we have something to point out.

Lauren: Exactly, exactly.

Thank you so much we really appreciate I think I've said again.

Mary Jane: No problem.

Lauren: Everyone I'm going to put you back into the lobby, we'll have a 15 minute networking break and then the second work for the afternoon begins at 2:30pm.

So I will see you there thank you so much again, Mary Jane and everyone who attended.

Mary Jane: Thanks everyone for that.

Have a great day bye, bye.