Speaker 1: Hello and welcome to the CPA Australia podcast, your weekly source of business, leadership and public practice accounting information.

Georgina: Hello, my name is Georgina Switkowski of Nab Health and today it's my pleasure to be speaking with Andrew Davies of VMIA, and together we're going to be exploring the role of the insurer in better patient safety. Welcome Andrew.

Andrew: Thank you, Georgina.

Georgina: I'm wondering if to start with you can set the scene for us, Andrew, who are VMIA and what do you do?

Andrew: Thank you. VMIA, as one of my colleagues recently put it, is Victoria's best kept secret, at least that's how I like to think of ourselves. We're the government's captive insurer, but we do more than insurance. We're also the risk adviser to government as well. Our role is really to look after the risk transfer of government, providing all of their insurance arrangements, but also providing good solid risk management advice so that we can help them prepare for and prevent harm in the first place, or indeed, if they do get into help them recover rapidly.

Georgina: I think that's fascinating. One piece that I picked up from your website is that your organisational purpose is to build a confident, resilient Victoria through world leading harm prevention. That to me speaks far more than being a pure insurer, but actually adding something back to the organisations that you insure. Is that accurate?

Andrew: No, very accurate. I mean, in terms of confident and resilient Victoria, it's exactly where we think we should be as an insurer and a social insurance for the state, you know, to be confident and resilient, being that you know that your risks are transferred appropriately, you've got the appropriate insurance in place and therefore confidence in the face of risk. Then resilient - the ability to spring bound from any harm event because you've got world-leading claims management and recovery functions that sit there. The prevention and recovery elements of what we do is really though where we like to play as the social insurer. That's where we sit and we talk about, how do we use our privileged position, where we look across the state, understand the sort of risks that the state faces and then see how we can either mitigate harm from experiences we've had through claims and other areas, or indeed connect the state to world leading experts around harm prevention in the areas of interest.

Georgina: Oh, fantastic. When we look at the health sector in Victoria, I understand that the VMIA has three areas of focus that you look at, one being property, one being cyber, and the final being the piece that keeps our hospital execs up late at night, which is the medical indemnity side. I thought we might start by exploring property, given it's the easiest for lay people like myself to understand. I've got car insurance, I have a prang, the insurance company pays out. When we look at your role, can you give us an example of a recent incident where you've been able to use your data analytics or insights perhaps from your portfolio to add some value back in?

Andrew: Yeah, so property as your outline is, you know, for us, an insurance product not that dissimilar to whether it'd be your car but moreover probably your house or anyone who's got home and contents insurance, it works very similar in the commercial landscape. We insure all of the health services for their property and their equipment, and with that, we look at how do we make sure that the right level of risk is transferred to us when there is a big event or if some damage is occurring to a hospital, how do we make sure we get the repair work done really rapidly so that we can get up and running and we can protect the ability of those health services to provide the services - those critical services - to our Victorian community in that.

We look at things at VMIA is the social insurer end of things. We read all of our policies in the favour of our clients where we possibly can, and that works really well for property when you've got leaky pipes that might be impacting on the operability to have health service, but also works where we work with our clients, we use our claims information, we mine that - foreseeing themes in our claims, and with those themes, we then start to think about what preventative actions can we take. A small example of that as I was speaking about it at the conference or at the forum is around environmental stress cracking on equipment. We've seen with one particular health service where their equipment wasn't living out the life that it should, right. It was actually a bit deteriorating very rapidly and we identified that with that equipment, was something to do with their sterilisation techniques, they were actually impacting on that.

You take a look at that, so that's one health service. Now we've got 115 different hospitals under risk with VMIA. Our job really is to say, well, who else has got the same problem? What can we learn from that? How do we take that loss that we're seeing at one health service that is impacting on their ability really to maintain their equipment effectively, learn from that and apply any learnings to other health services. It's a really interesting space for us. What we know is that there's variability in practice.

Georgina: Okay, That makes a lot of sense.

Andrew: If there's variability in practice, our job is to think about how do we actually identify what is the best practice so that we can prevent the harm as it goes forward.

Georgina: Well, I guess in that example, it's a really interesting interplay in that infection control, sterilisation of medical equipment is a really clinically important aspect of running a safe hospital, but on the other side, you've got property that needs to be protected and preserved for the overall operating efficiency of the organisation. How do you manage that interplay of the clinician side versus the operational management of the hospital?

Andrew: Exactly, and I guess it's an important part of this where VMIA as the insurer, we're not the clinicians, we're not the infection control experts. What we actually see, because we look across the whole system is that one health service might be having a problem, others aren't. Our job really is to actually ask those questions, and if we can ask those questions around, well what's different, we might be able to identify, well, what are those small things that need to change to prevent harm, and in this circumstance, harm to equipment, but that equally could be harm in a clinical sense in terms of clinical

practice. We look to mirror that in our privileged position of looking across all of these health services to look for opportunity.

Georgina: Yeah, that's fascinating. I think we might move to cyber, the second pillar of your area of focus. I think my favourite quote from your presentation was that the beauty of being an insurer is that you can begin to catastrophise everything, which is a nice way of saying that sometimes when you're an insurer or indeed a banker, you need to consider what the worst case scenario might look like and mitigate that risk, or at least understand it. In cyber, and for many of us, technological advances, incredible improvements in the efficacy of criminals operating in that area really mean it, it is an unknown for many of us. It's not that difficult to catastrophise if only we knew what to look out for. From your perspective, why is health and why are services such a rich target for these types of criminal attacks?

Andrew: Again, why health services targets if you think about the sort of function that they perform and the sort of information that they hold about people, the value of the information in a medical record is almost 10 times that of what credit card records are worth, and as such, they become targets in that sense. You also look at it and say they are relatively easy targets, the sophistication that they have applied to the technology and the ability of a health service to maintain standards of technology quite different to the banking industry that has got much larger pockets to actually dip into, in that regard, the health sector really does work off of the sniff of an oily rag. Most of the dollars run to the provision of care and therefore things such as the technology can in some circumstances be left behind.

Now, as you say though, the criminal elements, those that want to be mischievous in a way are actually getting much more sophisticated, much more sophisticated in terms of how they might attack health services. To your point, it is a beautiful thing that you can actually dream up scenarios of the terrible that might happen, but beyond that, when you start to go back to the reality of where it actually is, where cyber is going, it's a great exercise in where you see the past not being the predictor of the future, right.

Georgina: Indeed.

Andrew: The idea of the internet of things where all of the connectivity is going to go to, it's not that hard to actually paint a scenario that could seem rather disastrous. Now then you have to step back from that and actually say what is more realistic in terms of what might happen, and what is the role that we can play as a small player within the scheme of things as the insurer, but what is the role that we can play as the insurer in risk advisor to what health services might want to be doing to protect themselves.

Now our cyber insurance policy, world leading policies in a regard around looking after breaches once they're identified, helping the recovery actions and everything that a health service might need to do, but moreover the work that the Victorian government is doing around the cybersecurity strategy, looking at how do we prevent where we possibly can. How do we make sure that we've got very robust business continuity planning in place so that we can maintain service even if we have had these breaches,

and what does disaster recovery planning look like? All of the good hallmarks of risk management, this is what we be advising our clients on in that regard.

Georgina: If my medical identity is potentially 10 to even 50 times more valuable than just my rural credit card data, what's driving that? What would someone want with my medical data? What could they do with it?

Andrew: It's really interesting, isn't it? You can't walk away from the medical identity, which is some of the reasons why it is much more valuable in a sense, right? You can walk away from your credit card data, you can actually get them cancelled, you can get new credit cards, et cetera, but you can't walk away from your medical identity, because of that's unique to you and it doesn't change.

Georgina: That makes a lot of sense.

Andrew: As such, you think about identity fraud, that's kind of where you're going to go if you want that sort of information. Now what would they do with it? Okay, if they make it public, there might be some recourse in terms of your public information or your private information being made public. From a VMIA perspective, that's interesting, and we'll indemnify our health services for that, for a breach of information. More over though, what might they do if you look at the recent Singaporean example, where the Prime Minister's medical record got hacked and what I read about that is that, they were particularly targeting the Prime Minister's prescriptions and what medications that he was on.

Georgina: There were repeated attempts weren't they? They really wanted that information.

Andrew: You start to ask that question, well, what do they want that for? What might they do with that information? What might they do to hack a dispensing system or a prescribing system to change the medications that are on or something like that in a future state, which is really interesting for us. Then think about, well how insurance respond to that, but moreover think about, well, what might health services need to do in the protections around these activities? How do you decouple some of that? How do you provide some level of protection that if your medical record is compromised, that the prescriptions that you're dispensed actually aren't.

Georgina: Of course.

Andrew: How do you actually think about that, and as we progress further and further into electronic medical records and other areas, this would be really interesting for the health sector.

Georgina: And increasingly implanted medical devices.

Andrew: Yes.

Georgina: Pacemakers and other bionic implants, the possibilities are endless really.

Andrew: Insurers globally are looking at these issues right now and working with health services about what that risk looks like, but then thinking about how do we step that back into what are the prevention measures that can happen, and what are the things that VMIA can do to advise our clients, and if we can't advise them, we see part of our role also is about navigating to worlds best practice.

Georgina: Yes.

Andrew: Who is doing this best in the world? Insurers are actually really well placed to think about that, because we have that common interest with our clients around that risk and the mitigation of that risk. We have typically got wonderful networks that we can leverage to bring all of the information about prevention back.

Georgina: Yes. Who is doing it best in the world, and how does Australia compare?

Andrew: Well it's really interesting, so if I quote our CEO, we're not leading, but we're not far behind.

Georgina: There we go.

Andrew: It's a really interesting space, because it's evolving very rapidly, right, and you'll see that through all of the media that you see, more and more penetrations occur around data, et cetera, and while we believe that Victoria is really well placed, I think the government's done a really bold thing in terms of the cybersecurity strategy, putting on the information security officer, and putting those roles in to make sure that we're setting ourselves up for these kinds of protections. We're doing a really good thing in Victoria.

Georgina: Oh this is fantastic. How long does it take us to pick up if someone has made an incursion into our systems? If people are the first line of defence, how do we go?

Andrew: It's a really good one, isn't it? Because people are the first line of defence, but also the first one that fails in a large way where, phishing is still the primary number one kind of issue in terms of how people breach systems. Targeted phishing these days is typically where it goes, but again, first line of defence in terms of detection, really good organisations will detect within minutes and hours, but the data that we see suggests that many organisations don't detect it for even up to years. A quote that I talk about quite often is that, on average it takes 283 days to detect a breach.

Georgina: Yes.

Andrew: I wonder what happens in 283 days. 283 days feels like a lifetime sometimes, and the amount of time that somebody could be interrogating my systems, identifying where my weaknesses are, looking at patient records or indeed other records, that's a virtually a lifetime in a long way in terms of playing around before it's detected. Then after detection, obviously you've got to then go about, well, how do I get my systems back? How do I get control back? How do I understand what's been compromised? Then, how

do I communicate with all of those who are potentially compromised. The insurance response to all of that, we would like to think that all of the business planning that the health services do and indeed all of our clients do actually will support them having really robust practices once they identify a breach, swing in the business continuity plan, think about how they address all of those issues.

Georgina: Wow. This is a nice segue to the next point talking about humans and our abilities to sometimes not quite do the right thing, which would be the medical indemnity final limb of your areas of focus. I know that this is something that keeps our health execs up at night, and it's a really important piece. It's also important because it's a key driver of their premium payable to VMIA. Are you able to talk us through what your book looks like, what the split of claims might be? Where you're tracking with premiums and how they're calculated and what they're looking for the years ahead?

Andrew: We'll let you in on all the trade secrets of an insurer. Look, so the medical indemnity, obviously an interesting space for us. Medical indemnity makes up over 50% of the premium that Victoria, so the Victorian public sector is charged from VMIA. Now, when you think of that, we are one of the larger insurers, probably one of the largest social insurers in the southern hemisphere in a large way. We have over $200 billion worth of state's assets under risk. We cover all of the public liability for the state, and with that medical indemnity, still peaks up at over 50% of the premium that we need to charge in that regard, and it's over 67% of the liabilities that sits on the VMIA balance sheet.

Now that's over $1.2 billion worth of liability sitting on the VMIA balance sheet for medical indemnity risks. Of that 35% is associated with maternity based activities, so obstetrics activities. That's a statistic that we have been working a lot on at VMIA, and working with our health services on a lot. We're looking at and have been really active in harm prevention in medical indemnity because it is such a large exposure for us, but also because it's the right thing, right. No citizen of Victoria wants to go to a health service and think that they're going to be harmed. The absolute common interest between us and health is about getting the medical indemnity down because that actually means fewer people harmed, unnecessarily harmed in health.

When you look at the statistics of 35% of our premium driven by maternity services, we've introduced over the last 10 years a series of different interventions to try and drive that down and two real strong intervention, so fetal surveillance monitoring is a piece of work that we did with RANZCOG, so the Royal Australian College of Obstetrics and Gynaecology, and with them the department of Health and Human Services, we introduced the foetal surveillance program back in 2003. In 2010 we introduced another program called the prompt program, which is a training program targeted at emergency training and scenario based training in the delivery suite.

Georgina: Understood.

Andrew: Where we have multidisciplinary teams trained in terms of how to look after patients that are deteriorating in a large way. When you come into the emergency department and you need an emergency Caesarean for some reason, the whole team knows exactly what they should be doing and they work together to get you to have a safe experience

in that. That program we introduced in 2010 and we actually have driven through all of the health services with their support picking it up. Now, our claims experience over that kind of time period over the last 10 years has declined by 65%.

Georgina: Which is amazing.

Andrew: It's a fantastic result for the hard work that Victorians do. Now we can't correlate it directly to these two initiatives, but we believe that it's actually really important that these initiatives continue, and as such, VMIA put in an incentive program this year, that incentive program is delivering money back to the health services if they maintain these systems.

Georgina: Okay, so a bit of a rating one driver scenario.

Andrew: Exactly, and a first for VMIA. Rating one driver, or we like to think of it as the same as dead locks on your house.

Georgina: Yes.

Andrew: You do these activities, there will be a rebate associated with these activities because we know your risk profile is less than what is predicted for it, our modelling, and were actually paying that forward. Our ability to start to say we will be confident that if you do these things that your claims experience will be lower than what we forecast, and we'll pay that forward so that you can have relief in terms of your budget. This training activity is not a burden to you, and in a large way, it's about aligning where our CFOs may be, the administration activities of a health service with the clinical activities and health service, and those two aligning really well under an incentive model, we think pulls all in the right direction, making it safer for mothers and babies.

Georgina: Okay. If we imagine past claims experience is something that will be different across each health service that will contribute to their total premium payable, what about the other factors that come into play in calculating their premium?

Andrew: It wouldn't be unusual for CFO to asks that question of me. That happens on a routine basis. The other things that come into calculating premium, we have an overall pool, right, so the way that we look at premium at VMIA, we're basically a not for profit. We run at the minimum in what we can do, what we have is external actuaries that look at our 10 year claims history, will take that into account and define what we need is an overall premium to account for all of the claims that might occur over the next 10 to 15 years associated with the year that we're applying that premium in. We then put that into a risk based model where we allocate out to health services. Now the risk based model accounts for the sort of work that you do, so obstetrics is riskier than surgery.

Georgina: Understood.

Andrew: Surgery has still got a risk profile, which is different to emergency or to general medicine.

Georgina: Indeed, okay.

Andrew: We put it into a model that says if you're doing, let's say 30% of the obstetrics work for the state, you would receive 30% of the obstetrics pool premium. Then we offset that by your experience, so if you've got a good claims experience, that'll be discounted, if you've got a poorer a claims experience and what we would normally see across the state, then that will actually end up with a premium implication for you. We work through this with each of the health services so they're clear about what their premium drivers are and the goal for us is really about making sure if they're clear on their premium drivers, they own the risk management activities that they can do, then they can make decisions about where they actually pull and pull levers for risk management and harm mitigation in their own areas to reduce their premium further.

What we want to do is to learn from that because then we want to take that out of one health service that has been able to pull a lever to reduce harm, and put that across the other 114 health services that we look after. That's why we think that VMIA as a social insurer has this harm prevention drive in what we actually do and talk about.

Georgina: I guess they are the known factors that the past performance or the past claims history, but how do you assess emerging risks and the unknown? How you assess what might be coming around the corner next and what proportion of the pool that might constitute?

Andrew: That's a really great question. The unknown unknowns in a large way, and if you think about risk, that's what it's all about, right. Otherwise we're actually dealing with an issue, but in terms of the unknowns, we see a role of an insurer is to stay connected with the emerging risks in the landscape. We will periodically commission research that tells us about what is seen as emerging risks. While we, you know, we have a fairly good intelligence in our claims about what's happening now, and we can have the analytics and insight running over that in terms of where we've been, where are we now, where the future is, is really getting into what are we seeing in research? What are we seeing in advancements in technology? What are we seeing in the changes to the way things are working within health, fly in, fly out as an example that comes about, how does that change the risk profile and what does that mean? 3D printing, as another example within health, how does that change the risk profile? What does that mean once a health service starts to become a manufacturer of product.

Georgina: If I'm a health service, what sort of questions should I be asking you?

Andrew: Great question. I think health services should be leveraging their insurers a lot more. We at VMIA, as we said, we've got that purpose around harm prevention and recovery. We want to make sure that we're providing the appropriate insights back to our health services about what drives claims. My encouragement to all health services will be to ask their insurers exactly that question, what drives their claims? What is something that they can learn from other's experiences? How do they learn from other's mistakes so they don't have to make them themselves to actually learn? I think as insurers, it's incumbent upon us to actually do that, to turn the insights that we have into intelligence to support our clients in harm prevention activities where we possibly can and leverage our networks.

God knows that there's enough premium that has to go out to insurers to protect for the activities. Leverage the network and the knowledge and skills that are actually in the insurers around what drives the claims. I think the other statement for insurers, don't think you're the clinicians, don't think you know the answers, right. We can only facilitate information flow and then have the clinical teams and the administrative teams at health services think about the solutions. Once a solution is there, a role for VMIA is about, well, how do we actually support taking that outside of one health service and making sure it actually transpires across many, so that we can all get the benefit of the ideas of the few.

Georgina: That's fantastic. Thank you Andrew. I think you've given us plenty of food for thought, particularly those of us entering into premium negotiations with our insurers. Have a great day and thank you so much.

Andrew: Thank you.

Speaker 1: Thank you for listening to the CPA Australia podcast. To download the transcript and to access the show notes for this episode, please visit www.cpaaustralia.com.au/podcast/95.