Transcript

Risks of My Health Record

Webinar, 6 September 2018

Watch the webinar here: https://www.youtube.com/watch?v=M59yAJt_njM

Find out more about the webinar: https://chf.org.au/introduction-my-health-record-webinar-series/webinar-4-risks-my-health-record

Section 1 of 3 [00:00:00 - 00:20:04]

Mark Metherell: Good afternoon and welcome to this, the fourth in our series of webinars
on the My Health Record, which we at the Consumer's Health forum are
presenting. This session is to focus on the risks in MHR, or My Health
Record, and we welcome questions and comments from you, the online
audience. Thank you. I'm Mark Metherell, I'm communications director
[00:00:30] with the Consumer's Health Forum and I'll be facilitating today once again
in this series. We have an impressive group of panelists who bring a nice
variety of expert perspectives on this issue of the risks that my company,
My Health Record. If I can introduce our panelists, we have Tony
[00:01:00] Kitzelmann who's chief information security officer and general manager
at the Australian Digital Health Agency, which administers My Health
Record. Tony was previously senior cyber security executive and general,
and chief information security officer at Lockheed Martin, and had been
involved in cybersecurity management with both the Australian Taxation
Office and the Department of Defense.

We have Dean Martin, who's a consumer advocate and a member of the
[00:01:30] Australian Digital Health Agency Consumer Advisory Committee. He's a
consumer representative from the southeast Sydney local health district
consumer and community council, and his day job is a research manager
at the Black Dog Institute. We have Dr. David Hansen, who's CEO of the
[00:02:00] Australian E-Health Research Centre at the CSIRO. David leads a research
program of nearly 100 scientists and engineers developing information
and communication technologies for the healthcare system. And at the
end here, Aaron Cogle, who's executive director, for National Association
of People with HIV Australia. Aaron has previously spent 12 years working
with the British National Health Service as an HIV program leader. And
[00:02:30] before that, was with the Aids Council of New South Wales. The
Consumer's Health Forum has designed and directed this webinar series
with funding support from the Australian Digital Health Agency. I should
make clear that while we're fortunate to have on the panel highly expert
people, the object of this exercise is to respond to the questions of an
interested consumer audience.

There has been some social media a discussion this morning about the
[00:03:00] fact that this particular panel is men only. I can say that all previous
panels, uh, our series have had a strong representation from women. In
this particular case, we weren't able to arrange it. It's also worth recalling
that the first webinar of the series also focused on privacy and security. So
we're seeking to also look at other complexities and risks with the MHR.
[00:03:30] So let's start by asking each of our panelists what they see as the major
risks with MHR, and if I can start with Tony.

Tony Kitzelmann: Thank you. First of all, good afternoon, and the opportunity to come and
talk about this as a really important because it's bringing light to the
commitment the Australian digital health agency has brought in regards to
securing the product. The My Health Record system, as you can
appreciate, is a large national piece of infrastructure that's going to
revolutionize the way that we deal with electronic health material in
Australia, and make it available to our consumers and healthcare
[00:04:00] providers. For my role as the CISO, it's important for me to understand
what those risks are that are exposed to such a complex and substantial
piece of our national infrastructure and provide the security that is robust
and fit for purpose to ensure that we actually have something that meets
our ongoing requirements. So for me, my risk based focus is I'm an ex-
copper, so I share and only trust facts.

So for me it's about understanding what are the risks here, the cyber crime
[00:04:30] that may potentially be targeted towards this platform, and how, as a cyber
security specialist and a leader in a space with a very smart group of
engineers, we build a solution that is robust and tested and resilient to a
manner that protects this critical piece of infrastructure for the agency.
Our response to that has been check, check, and check again. So we've
undertaken a very comprehensive approach in regards to designing the
solution, testing every component of the solution to make sure it is cyber
[00:05:00] resilient, and actually making sure that everything that we do is
independently qualified so that we can measure the risk, and understand
that our investment and our commitment has been actually effective to
secure the solution.

Mark Metherell: Thanks, Tony. David, can I ask, what do you see as the risks?

David Hansen: Oh, so thanks for that. And also, I appreciate your opening comments
around risks beyond privacy and security because I think the risks are
certainly beyond privacy and security around My Health Record, but then
[00:05:30] so are the opportunities and risks are often related to the opportunities
that we can add to certain things. So in terms of My Health Record, I think
there's a range of risks and opportunities that the system has. I think we
need to be really open that My Health Record is only one part of the digital
health ecosystem which is emerging in Australia, and so we have a
number of services that support My Health Record in terms of individual
[00:06:00] health care, identifying it as terminology interoperability. These are all

things that the agency is bringing to the standards and services which enable our hospitals and our GPs to connect with the data and make it available.

So data quality is a big issue. So the data which goes into My Health
Record comes from a number of different sources, and so coming from
hospitals, coming from the GP clinics, pathology results, and so it's going
[00:06:30] to be really important for the users of the system to be actually checking
their record, looking at the data that's there, and comfortable that it is
representing their health and the sort of conditions and allergies and other
things which do apply to them. So there's a risk where I think we need
consumers to be really ready to log on, check the information. Clinicians
[00:07:00] will generally check, will always check. Anyone who's been to a hospital or
a GP knows that they'll get asked by the clinician a number of questions,
they'll check the data that they are looking at is correct. But as has
happened in the rest of our busy lifestyle, more and more of technology
uses the data which is in those systems to provide the services and things
like that.

So to get the most out of the My Health Record system, making sure that that data is correct and up to date is going to be really important, as an example of one of the other risks.

[00:07:30]
Mark Metherell: Thanks David. Dean, what's your perspective on risks?

Dean Martin: I'd certainly echo what David has said, it has risks and there are benefits,
and I think from a consumer point of view, currently one of the risks is that
that consumers don't necessarily understand what the potential benefits
of the system might be, and they may not feel comfortable about having
[00:08:00] their information in one place like is going to be the case with My Health
Record. They might prefer to have other ways managing their health
information, or not managing it. It's a case maybe.

Mark Metherell: Right. And Aaron, from your point of view, how do you see the risks of MHR?

Aaron Cogle: So there's always as has been mentioned, a risk of data breach and things
like that. And for HIV positive people, that can have particularly bad effects
[00:08:30] on their life, which no doubt we'll come onto a little bit later on, but I think
some of the more bigger risks that the system poses is that trust in one's
doctor in the ability to be able to honestly talk to one's doctor is really
important to secure the best health outcomes. And that might be talking
about things which might not be, perhaps always legal, like drug use and
[00:09:00] things like that. And so the problem that I think, the risk that I think My
Health Record poses is the possibility that people won't be able to be open
and frank with their doctors because there is, in the back of their mind, a
fear of that information won't stay between them and their doctor, ad that

there could be issues around criminalization or indeed any use that is not for a specifically health related issue will curtail people's ability to speak open and frankly to their doctors.

[00:09:30] And then there's one final macro issue that I think is possibly posed, and that is the involvement of data is always often followed by the idea of selling data and money. And so when money comes into a system like that, I think the the idea of, of health information being collected just for health purposes can sometimes be a bit skewed, and it starts to be a collected for profitable health purposes. And so those are the risks that I think we need to monitor as the system rolls out to make sure that we've got it right.

[00:10:00]
Mark Metherell: Tony, there's a matter of risk and who owns it. Do you think, is there a place for private industry, the private sector to be involved in the data collection or storage, or should we only leave it to governments? Do you have a view on this?

Tony Kitzelmann: The profit sector are already involved in the collection of the data, so we see those clinical information system providers out that provide those services to the healthcare practices. So they're already part of the integrated digital ecosystem that we actually deal with in the real world.

[00:10:30]
Mark Metherell: You're talking, if I may just interrupt, about the sorts of systems that GP might have that he or she refers to.

Tony Kitzelmann: That's correct, yes.

Mark Metherell: That sort of thing?

Tony Kitzelmann: Yep. So that exists already in this place. And we also see, as you know, they are mobile applications out there that are provided by third party vendor. Of course, people in the community have said, "Well, I want this on a mobile app and I want to be able to interact with my data in a way that's appropriate for them as an individual." So I think there is always the balance between how we, as government partner with private industry to bring innovation and bring a new, fresh look at the way that we can make
[00:11:00] data available, but always remember that it's not our data, it's the data of citizens and that whatever we do, we need to make sure that those protections are always considered as the first and only consideration when we make those decisions about bringing it in.

Mark Metherell: Dean, from the consumer's perspective, as Tony's mentioned, there's already a lot of private sector involvement in collection of health data one
[00:11:30] way or t'other. What's the feeling, do you think that consumers are well

protected or go and have their health information sold off to the hospital, that sort of thing?

Dean Martin: I suspect there are some people who would believe that, but it's clear that that's not the case, and you only have to look at what the College of GPs have put out about My Health Record which, while it's quite complex, does [00:12:00] explain quite clearly how the system works, and there's a lot of work that's been done by the Australian Digital Health Agency as well to explain what the system is, how to do various things with the system. So I think that overall, the risk of the data being sold is minimal if nonexistent.

Mark Metherell: Would that, would you agree with that?

[00:12:30]
David Hansen: I think this goes into a whole range of issues around secondary use of data, not just in My Health Record, but across our healthcare system. And it's important to realize that there's a significant number of safeguards in place around that secondary use and its appropriateness. Certainly, health data collected in our health system and in GP clinics are used to, for a [00:13:00] number of purposes, quality control, we want to make sure that the healthcare that people are getting is of high quality. So that quality assessment is a big use of secondary use data. Medical research is certainly part of that, and so we have human research ethics committees which review access to data and, and those sorts of things. So there's a [00:13:30] range of secondary uses of data which we may get onto later as well. And so the sale of that data, or access to that data through commercial purposes should be governed, and is governed in the majority by those sort of processes that we have in place, and as well as the consent process.

And so the consenting use of data, I think My Health Record actually gives potential, and we should realize that My Health Record probably won't stay exactly the same as it is now. It will change and evolve as technology [00:14:00] changes and our lifestyle changes. Tony mentioned that we all want the data on our phone. 10 years ago, that wasn't the case. So I think there'll be a range of new technologies that come out. It's another risk for My Health Record. We don't know the potential for it to be superseded by new technologies which come out that will need continued investment. And we're seeing exciting things happening around the world in terms of [00:14:30] interoperability with the health systems which provide a more federated type model to sharing data or to having your data come together on the phone rather than in a central place. So there's a range of risks there that we need to be cognizant of as a nation as we evolve our technology.

Mark Metherell: Can you just expand a little more about these sorts of federated?

David Hansen: [00:15:00] As I think Dean mentioned, and Tony, that we've got My Health Record as a single data store with all that, which contains summary Health data from

GP clinics, our pathology tests, all those sorts of things. We're now seeing in the US, Apple for instance, offer through their healthkit access directly to your electronic health record at a clinic or a hospital using some new technologies, SMART on FHIR. And so there, the only place that the data [00:15:30] comes together is actually on your phone rather than in a central repository. So there'll be a range of things which happen over the next 10 years, this technology.

Mark Metherell: So nobody else, no other organization can see all of your ..

David Hansen: Potentially. That's another model which can, and look, I'm not saying that that's what we need to do. I'm saying there's different models, we need to make sure that we evolve with that as those technologies become available,

Mark Metherell: Tony, can you see, I mean obviously this is a fast changing area. We [00:16:00] wouldn't have thought 20 years ago that we'd be able to look up our health details on our phone. Is it the case that the developments are likely to leave us in 10, 20 years with some entirely different technology or way of storing and distributing our health information?

Tony Kitzelmann: Without a doubt. Technology evolves so rapidly. Everyday, I come to work, I learn something new, and that idea of federation is a great example where the data may be stored in many locations around different parts of [00:16:30] the environment, genomics, imaging data, and it may be appropriate that the data is simply just referred to from the My Health Record system, so it goes and fetches it for you when you need it, but it's creating that index, or that catalog of information that is yours as a citizen, and making sure that when you need it, it's facilitated and available. That federated architecture models been around for a long time, and it does leverage a lot of the reuse of information and data. It makes it available when needed, and doesn't necessarily mean it has to all come to one location. It's about having [00:17:00] something that's fit for purpose and appropriate. In 10 years time, who knows where we're going to be, what technology will change me. My daughter keeps saying to me, why is my Fitbit hooked up there, and why I can't all this data in there.

It's alright, it's going to change. We're going to have increasing demands as the citizens say, "Well, what about this? What about my diabetic starter that I want to have on board?", And those key pieces of information that will evolve as society changes.

Mark Metherell: So have we got clear principles that endure and still protect us as we get this changing technology?

[00:17:30] Tony Kitzelmann:

I think we do, and my view as a cyber security nerd, and I sit back and I say that respectfully to myself is that we do because the principal that we take here is that we don't own the data, we're simply custodians entrusted to-

Mark Metherell: When you say we ..

Tony Kitzelmann: As in the Australian Digital Health Agency, don't own the data, we're entrusted on behalf of you're citizens to make it available if they decide to be in the system and be actively involved in the digital health management. So the ability for us as a cornerstone is it's not our data as an agency, it belongs to our citizens. We follow the wheels, and we always [00:18:00] go to the full most of our requirement and protect the integrity of their rights as the owner of the data.

Mark Metherell: Sorry, go on.

Aaron Cogle: Tony hit on a point there about individual sovereignty over their own data, and I just wanted to point out that with all this technology in future as it evolves, we may not be able to entirely protect it in technologies that we [00:18:30] don't even know what they would look like yet. But if we had a principle which was the the individual, this is absolutely sovereign over what is done with their data, and then that individual, there seems to be an assumption here that either the private industry or the government has to hold that data but indeed, if individuals were sovereign over their own data and they could choose to share it with government or a private industry depending on what the benefits to them were, then I think that sets up a situation where people can have a lot more control and faith in what's going on, [00:19:00] because essentially, they have to be provided with a really good service before they can share that or get a good health benefit.

Mark Metherell: We've had a question come in online from George who asks "Will the service hosting data be located physically within Australian mainland borders?" I'll ask you, Tony to ..

Tony Kitzelmann: A simple answer. 100 percent yes, guaranteed. It's in Australian government certified data centers, and is only hosted in Australia with very strict controls about the use, and how that data can travel within our ecosystem.

[00:19:30]

Mark Metherell: So it's not up on a cloud that somebody in California that can ..

Tony Kitzelmann: 100 present sits on Australian infrastructure, measured to Australian government security requirements and protected. I've visited the data centres. I know where they live and how well they're protected.

Mark Metherell: Right. Okay. Well, you'll answer George. If I could ask Aaron, do you think there's enough being done to inform people as to why or when they should sit security and access controls to the MHR?

[00:20:00]
Aaron Cogle: Yeah, I think there are some concerns there in that-

Section 1 of 3 [00:00:00 - 00:20:04]
Section 2 of 3 [00:20:00 - 00:40:04]

Aaron Cogle: There are some concerns there, in that in order to properly set a security control over a piece of information that's on My Health Record, you have to first be able to understand what that document is telling you, and there might be some medical or scientific information on there. And then you have to make a determination about who you want to see that and what level of access people should get through My Health Record. And then you [00:20:30] have to be able to work the security system on the the My Health Record system in order to be able to do that.

Now, when you have a chronic condition, such as HIV, every document, it can quickly add up to tens of thousands of documents. And so anyone who's got even a very small limit on their time, so anyone who has a job, for example, is going to really struggle to be able to go through every single document on their My Health Record and determine who they want to see it and then to be able to set the appropriate security mechanisms.

[00:21:00] So we do have some concerns that unnecessary disclosures, which are not illegal disclosures, but just unnecessary disclosures, will be happening because people will be overwhelmed by the amount of info that's on the system.

Mark Metherell: What do you think about that, Tony?

Tony Kitzelmann: And i`t's a valid point, and I suppose that's why we implemented the record access control in a modular type of approach so that, as a consumer ... Now, my personal settings? I've set it up so I just get notified when somebody accesses my record. I walk out of the doctor's surgery and I get [00:21:30] an SMS notification. I'm going, "Sweet. I know who's been on there," and I've got that audit log. But you also have the ability under My Health Record to go in and actually apply your particular record restriction, in this example, so that when you go to see your health care provider, you can actually provide them a number on the system so that they can then access your record and get it.

And you also have the ability, as we talked about, as to be able to make those records hidden in the individual ... at the file level. And I completely agree, when there's a lot of them, and that challenge is there, but you have [00:22:00] that ability to say, if you want a health care provider to access your record, here's the appropriate access code so that they can go in and get it. And that is for their particular service. It gives you that control, and it gives it at a one-to-one relationship between your health care provider and you as a patient.

Mark Metherell: Well, Dean, Tony's made that sound all pretty straightforward. What's your view? Is it going to be easy for the average consumer to set things up to suit their needs?

[00:22:30]
Dean Martin: I suspect that, excuse me, the average consumer will not have a problem. It's where there is either complexity or stigma, or where there is somebody with less health literacy that may not be able to do that for themselves. And I think that's where the point I made initially about the risk being the complexity of the system and how they will perceive that and how [00:23:00] comfortable they feel about using the system will play a part in how My Health Record develops in the future.

Mark Metherell: David, you're into health and phonetics. I mean, you're the sort of the person who'd be on top of the technological aspects of this. Is there a risk here that the technologists have produced something which the average person's going to have challenges manipulating properly?

[00:23:30]
David Hansen: Sure. Well, digital literacy in our society is definitely an issue. So I think we've got large numbers of those average consumers that you might have mentioned who these days are pretty digital literate. They can use technology fairly easily. But we do have challenges for those people who aren't so used to digital literacy. It's part of, I'm sure, what the agency's been doing out in testing the access and use of the technology. But it's [00:24:00] also something that we will see evolve over the next little while as more and more people use the information. So I'm sure the agency will continue to invest to make that easier.

If we all think about ... The example I like to give is the first time I used my mobile phone to check into my flight. It involved about 10 clicks, and eventually I got a boarding pass. And now, both Qantas and Virgin, it's really a one click thing and you've got a boarding pass. And so as the [00:24:30] technologies evolve and continue to be invested in, it'll become easier for all of us, and including those people who aren't quite as digital literate to use.

And so some of the access controls, some great points from Aaron before. While I'm sure the agency's already looked at those, I think there'll be easier ways to be able to say, "I actually want to apply this to all of my documents" in the future. There's things that the system will improve as we continue to invest in it.

[00:25:00]

Mark Metherell: On that point, Tony, in a blog posted on digitalhealth.gov, you are reported as saying that the Cyber Security Centre recommends setting an access code that is given only to health care providers you want to access your record and setting up automatic notifications via SMS or email to let the consumer know when their record has been accessed. If that's the recommendation, why isn't that the default for everyone?

Tony Kitzelmann: [00:25:30] Because it's a consumer's record. And I'm a great example of that. I actually don't want a record access control on my record. I want it to be available for my health care practitioners. And as a consumer we ... As an agency, we acknowledge that it's not our right to set what people should and shouldn't do with it. We provide guidance, because it's their data. And we provide that so that we can make people ... allow them to make informed decisions on how they want to manage it.

Like I said, I personally, I'm happy for my health care practitioners out
there, because these people are out looking after us and doing good
[00:26:00] things to make sure that we're cared for, and I don't want there to be a
restriction for them to provide service. But that's for me. For other people,
there may be a requirement that they want something different, and we
need to be respectful of that, and we acknowledged as an agency that
we'll provide the guidance needed and allow people to choose what they
want to do with their record.

Mark Metherell: You hear these stores of up to 900,000 health care professionals, nurses, physios, whoever, being able to access your data. What do you say to that?

Tony Kitzelmann: [00:26:30] I hear this one quite regularly. People say it's just a big database and the doctor can jump on or the health care provider can jump on and just browse the database. It's actually not correct. To be able to actually access the database, they need to conduct a conformance search, they need to have a software, they need to registered with us. And we audit all of that. We also, as part of our commitment ... and this an evolving capability that we've got going on as part of our enduring service, is to provide user behavior analytics so that we can actually look at what normal is and how health records are interacted with as part of a normal consumption.

[00:27:00] And if we take an example of a health care provider in a small, rural
location, how do they measure up against in performance and access to
the record compared to their cohort so that we can actually be smart and
aware of what' going on? This is evolving every day. And we see, for
example, many situations where people are coming back and saying ...
The agency gets inquiries quite regularly about, well, when this access
occurred, what was the reason behind it? And we're using a governance
framework that's been built and made available to ensure that's
[00:27:30] appropriate. And we write to the health care provider organizations and

ask them to validate and justify it. At the same time, the consumer has the ability to go in and verify that that information was appropriate.

But factually, it's not a database that can be just browsed. It's something that needs to be done, it need to be a conformance search, and it needs to be done in a way that is appropriate.

Mark Metherell: For me, you said ... I mean, do you have to deal very often with attempts by people to hack into the health information? Are you aware of it? Do you have to deal with attempted intrusions like that?

[00:28:00]
Tony Kitzelmann: My data is ... My thoughts have always been I have to build and prepare for
the fact that one day somebody will try and attempt to get in. And that's
why we've invested so heavily in protecting the system. It's hard to
describe in an open forum. And we don't talk about what we see, because
we do stuff against our environment infrastructure where people are
trying, but they're not successful because we've built it resilient. Now, we
do observe ... We actually profile what goes on in the broader Internet and
across all the different cyber-crime environments to understand what the
risk is for Australia. We work with our colleagues as part of the Global
[00:28:30] Digital Health Partnership to understand what the risk to Australia health
care is compared to the NHS digital to the US, the UK, China, Singapore,
and understand how this evolving threat landscape changes, and then take
that into the context of the My Health Record system to make sure we are
defending it appropriately.

As a former copper, I trust no one. And mine is all about prove to me,
prove to me, prove to me. My engineers test it. We PIN test it. We actually
pay people to validate that the security can't be broken into so that we get
[00:29:00] that level of rigor around it. Because we're always looking for new
opportunities to better at what we're doing.

Mark Metherell: So you're inviting people to try and break into the system?

Tony Kitzelmann: Oh, I'd never say that. We actually engage with highly specialist technology
companies who work under very strict rules of engagement to test the
security of the My Health Record product. And we work with the Australian
government as well to ensure that we bring the very best and smartest
minds to protecting and validating the security. I trust my engineers.
They're smart, smart people. But I also trust somebody else that's actually
walked the walked and proved that the product is as secure as they tell me
[00:29:30] it is.

Mark Metherell: And how does our system compare and contrast with these other systems overseas? Are there different features in terms of security?

Tony Kitzelmann: As a rule, no. The security that you would apply to something, a large ... an
effectively industrial digital health ecosystem like ours, are very
consistent. We obviously have perimeter-based security. We have
intrusion detection monitoring systems. I have a security operation center
[00:30:00] with analysts, watch all the traffic that moves across the network. And for
example, all of our data, when it flows through the network, is fully
encrypted and protected. So if somebody wants to try and intercept the
payload, they would get nothing. When the data's sitting in a server, it's
protected.

Always say to people ... somebody once said to me, they said, "Well, Tony,
what happens if somebody just breaks into the data center and gets
through those five layers of defenses, gets past the security guard and
walks out with the server?" Well, it doesn't matter, because, see, data's
[00:30:30] encrypted on the server. They take it out of our system, it's never available.
And they're the sort of things that we go the extra mile on.

We spend a lot of money and a lot of time investing in this because it's so important to get it right. If I get my job wrong, people will lose confidence in the My Health Record system, and then we miss this great opportunity for the country.

Mark Metherell: Yeah, yeah. David, what's your response to what Tony's just said? Are you convinced that everything's watertight?

[00:31:00]

David Hansen: Look, I think Tony and the agency has done a lot to make sure that the
data is watertight, and so I think that's less of a concern. We continually
hear from cyber security experts that the greatest point of failure is
everyone's use of passwords, as an example. So we all have ... Access to
My Health Record is governed through two factors: authentication, you
[00:31:30] need both your password, and then an SMS sends you a code, so people
who have logged on. And in the professionals, we need to make sure
health care providers are doing the right thing in terms of providing the
security to their health systems.

So while we can be thinking about getting hacked in and doing all the kind of high-end things, we need to be sure that people are changing their passwords, have a good, strong, secure password and all those sort of things as well.

[00:32:00]

Mark Metherell: Dean, from a consumer perspective, are you reassured by what you've heard?

Dean Martin: I personally don't have issues about the security of the system. I think it's being built to very high standards. And in my experience, most security

breaches are actually because of people rather than because of systems.
And it's actually getting that part right.

Mark Metherell: Yeah. Aaron, what about you?

[00:32:30]
Aaron Cogle: I think we can make a balanced judgment on whether or not we're willing
to risk the idea of a data breach because of the benefits that something
like My Health Record can bring. And indeed, the security protections do
sound really impressive. I think that for positive people, the impact of a
[00:33:00] disclosure ... So a security breach would mean that an HIV-positive
diagnosis, for example, might get out there into the public, and that visits
incredibly damaging things on the individual, and not just people with HIV
but other stigmatized groups as well, if information got out there.

The thing I'm more concerned about, I think, is the authorized sharing of
that data within the system. So I would argue, contrary to Tony, that we
[00:33:30] should start with closed settings to restrict the amount of sharing that
happens and then move to broader, open sharings after that. And the
reason for that is because people with HIV, for example, if health
professionals find out that somebody is HIV-positive without their wanting
their status disclosed, then that can visit all sorts of consequences upon
[00:34:00] them. And not just out there in public, either. People can lose jobs. It can
ruin relationships. And indeed, they can get poorer health services
because of it. So we know of examples where, once someone's HIV-positive
status has been discovered, then they've put at the bottom of
waiting lists, etc., for no valid reason.

So what I would be questioning is why someone's physiotherapist, for
example, needs to know their HIV-positive status. And so if we start with a
really small group of people that can see that information with appropriate
[00:34:30] security concerns, and then people can share it broader as they get more
comfortable with the system, that would be my preference.

Mark Metherell: It sounds like we do still need more information and education. Dean, who's responsibility should it be, do you think, to ensure that the community at large, individuals, are educated as well as they can be about the benefits and risks of My Health Record?

[00:35:00]
Dean Martin: I think this is a macro-level answer to that, which is that everybody has a
responsibility to educate themselves as much as possible about My
Health Record, what its benefits are and what the risks are, and to make
an informed decision. And there's a micro-level issue, which is about
capacity to actually do that for individuals and how they actually perceive
[00:35:30] the system and what issues they might imagine or actually might be
correct in thinking, issues that would prevent them from using the system.

Mark Metherell: We've had a question from a consumer who's asked, how easy will it be for an acquaintance of a person motivated by curiosity and working as a health professional in hospital to gain access to a person's health record? If I could ask you, Tony.

Tony Kitzelmann: [00:36:00] So if that health care provider decided to do something wrong, and they're trusted inside a sort of scenario, something that we're very cognizant of, in that they had that relevant information and they decided to do that, that possibility does exist, and because they would have authorized access and they would do something that contravenes the legislation, which comes with criminal penalties or financial penalties associated with it. That possibility always exists, and that's the importance of citizens taking control of their record and actually engaging with that health record and the audit trail to make sure that they're across that.

[00:36:30] It is a criminal breach, and we've seen examples in society where fraud occurs and people do similar types of crime types that you would just look at and go, "Why would a reasonable person do that?" Our plan is to always make sure that we inform the owner of the data of the audit and the ability for them to set those controls.

Now, if they have, for example, a record access control that requires the code to unlock it, then that person attempting to do that unlawful access [00:37:00] to the record would actually be blocked. So that's why we encourage actively take control of your records, set your record access control, and be accountable for what happens with your data. But unfortunately, in life and society, people will always choose to do bad things. If it occurs on the My Health Record system, or it occurred in a private health practice, or at somewhere else in the bigger ecosystem, that risk is there and it's something that we're very ... and we take seriously.

[00:37:30]
Mark Metherell: Under the access control in monitoring, is it the case where somebody's MHR was accessed without their knowing, is there a [inaudible 00:37:35]?

Tony Kitzelmann: If they've actually taken control and set it up. If they don't, then it'll be ... given the audit log, which is retained. But if they're not actually proactively involved in the management of their record and their data, then that audit would just sit there inside the log forever.

Mark Metherell: [00:38:00] Right. Okay. We'll end up with lots of ... somebody with a chronic condition, complex and multiple conditions, is going to end up with a very long record, aren't they?

David Hansen: They will. And I don't think that's any different to people who are in the health care system now. For a long time, doctors in hospitals knew how sick people were by how thick their medical record was, as an indication. [00:38:30] And so I think there's an opportunity with My Health Record, with it being digital, to be actually able to search data. So this is where are, using modern technologies and modern information and data search technologies, heading into artificial intelligence, to be able to actually use the data to support better health care.

[00:39:00] And so that's the value of bringing this data together, whether it's on our phone or in My Health Record, or using My Health Record together with hospital data in hospitals, or at the GP clinic, to provide more information to the clinician, to provide accurate information, again, back to the data quality and people engaging with their health record. But then also, in the future, as we learn more and more about disease progression and early indicators and new screening technologies, etc., to be able to provide better health care to everyone in Australia.

[00:39:30]

Mark Metherell: Aaron, from the perspective of your group, who's, of course, as you've mentioned, have particular sensitivities, are you persuaded that the health professionals can, by and large, be trusted to deal properly with the My Health Record data they see?

Aaron Cogle: Generally I think we have to say yes. There are laws in many of the states and territories that restrict disclosure of HIV status for health care professionals. And by and large, they have been successful. I think the- [00:40:00]

Section 2 of 3 [00:20:00 - 00:40:04]

Section 3 of 3 [00:40:00 - 00:59:42]

Aaron Cogle: Have been successful. I think the one bit that I would point to, is that if a healthcare professional makes an access onto my health record system that goes against the rules of my health record, then there are mechanisms by which that person- it's a crime, I think. It's a crime, and so there are mechanisms there by which that person can be held to account, but not held to account for the consequences that it causes to the person whose information has been breached.

[00:40:30] So for example, if someone accesses a file, finds out that a person is HIV positive, discloses that information and then that person loses a job, their relationship is destroyed and the consequences flow on. That person doesn't have an ability to be able to get compensation from the scheme or to be able to chase the person that's done that to them.

I would say that's a gap in the system.

Mark Metherell: Yes. Has this been considered a tool? Compensating people who have been harmed in this way, do you think Tony?

[00:41:00]

Tony Kitzelmann: So, from the My Health Record, the answer is no. Because that's, I think that risk has always existed, whether it occurs in a healthcare clinic where the doctor's hold, and the doctor has a lawful and authorized access to the data.

[00:41:30] The other consequences of life that simply people doing things that are wrong and inappropriate that exist whether the My Health Record System is there or not. From our point of view, we purely deal with the law which is this has to be done in accordance with our legislation, which is very explicit. And if the trust as a healthcare provider accessing their data is broken, there are criminal liabilities that are associated with it and the agency takes that very seriously, because it's not their data. It belongs to their citizens, and it's their job to protect it.

Mark Metherell: [00:42:00] David, we've seen the government is moving to introduce amendments to the MHR legislation to tighten up on privacy and security of records. Do you think that will solve the outstanding issues in terms of privacy and security for MHR?

David Hansen: So I think the government's responded and the agency's responded to community concern around that they opt out of privacy and security issues. The agency said that the changes reflect the current policy within [00:42:30] the agency to providing access to the data, so tightening that up with the legislation. But, and it's gonna solve one of the problems, I think actually discussions like this, educating people, letting people know what the privacy and security tools are on top of My Health Record. Really letting [00:43:00] people know what is going on, I think that provides a sort of security and knowledge to the community that the data's safely and securely held.

Mark Metherell: Aaron, are you convinced that we've hopefully plugged the gaps?

Aaron Cogle: I think that we've yet to see how this is gonna play out, but there's a key difference between the way that the law operates at the moment in relation to your files with your doctor. So there's legislation in most of the [00:43:30] states and territories which, as I said, prevents disclosure of HIV status without consent. But the issue with My Health Record is once that information which is the same information, is moved across into the My Health Record, then the My Health Record Act seems to allow sharing at a much lower bar.

So for example, if any participant in the My Health Record System, by that I'm thinking about contractors or IT professionals, not necessarily health professionals. So any participant in the system, reasonably perceives that [00:44:00] there's a reasonable risk to health or life or public health, then that information can be disclosed, and that's not the case. Currently under the law at the moment in most of the states and territories, in order to disclose and HIV status without consent, you would have to have an imminent risk to life and you would have to be able to identify the person that the imminent threat was to.

[00:44:30] So that is a significant watering down of the ability to reasonably share that information. And what's a reasonable belief that there is a threat to public health? Well, we know that treated HIV means that you don't pass it on. We know that HIV is a lifelong chronic condition, but it's fully treatable and people live long and very normal lives with HIV in the modern era.

[00:45:00] So while we in the community at Napland know that is the case, that's not very widely understood, that news. So what would a court determine is a reasonable belief? Would a person be able to disclose HIV because they thought it was reasonable to suggest that person was about to pass HIV on, even though that wasn't the case? We wouldn't be able to find that out until it went before a court, and by the time it gets to a court, that's somebody's life that's being turned upside down.

[00:45:30] So I think there are still, the changes that they have proposed to the act are really welcome, and I think they tighten up the security a lot. But there are still big issues that we need to look at, and I would like to hope that are future changes to tighten up that security, to really replicate what's happened at the state level for example will happen.

Mark Metherell: Dean, what's your view from the perspective of people with mental illness? Do you think things are tight enough when it comes to people with those conditions?

Dean Martin: [00:46:00] Well fortunately, mental illness is less stigmatized now then previously, but it is still a very stigmatized condition. I think that there are times when people with mental illness don't get the care that they need because the focus is on the mental illness. My Health Record is an opportunity for those people to actually have some of their physical health issues addressed as well, by making that information more broadly available.

[00:46:30] [00:47:00] I think it's actually going to probably work in favor of a lot of people that have mental illness or mental health issues. The same with chronic conditions and disability, I think that by having the information in one place instead of having to go through a yay thick file of notes and trying to find relevant information, care summaries and things like that, will actually make a huge difference to those people where the relevant information is much more easily accessible. There's a risk to that as well, but I think that risk is far outweighed by the potential benefits that people with mental illness, people with chronic conditions or disability, the benefits are going to probably be quite significant.

[00:47:30]
Mark Metherell: Do you think the healthcare professionals, not only doctors but other allied healthcare people, nurses et cetera, do you think enough has been done to educate and train them to make the most of MHR? Are you aware of that at all?

Dean Martin: I think it's something that will evolve over time. It's not gonna happen instantly, and I don't think there's a training session which will fully explain what the potential benefits might be.

[00:48:00]
Mark Metherell: You're nodding in agreement there.

David Hansen: Yeah, so look a couple of things I'd bring it back to. One is digital literacy, while it would be really good to be able to spend the time training the workforce to the amount that it probably needs, realistically that would be a hugely expensive exercise for our health system which is obviously already stretched for money.

[00:48:30] So that's why the system's need to continue to evolve to really meet the
digital literacy of, not just our population, but also our workforce. We're
seeing now, with the electronic medical records being introduced to
hospitals, that when large EMR programs go live in hospitals, they tend to
spend a lot of time training the doctors and clinicians on those systems
[00:49:00] which tend to be a bit more complex than My Health Record. They
certainly tend to look after, to be there to support people while they're
having an acute episode or a considerable time in hospital.

And certainly that will help bring up the digital literacy of the health workforce. So there's an evolutionary thing as we continue to make these systems better and easier to use, and also as people get used to using those digital tools in the health system.

Mark Metherell: Tony, we've had a question from Melissa, who asks what does a person in
[00:49:30] a domestic violence situation need to consider before making a decision
concerning a My Health Record?

Tony Kitzelmann: So the My Health Record and the domestic violence situation is a troubling environment for society to deal with. The important thing to remember, Melissa, is this is your record. Take control of it, assert your control over that so that no one else can gain access to your record so that you have that level of commitment to that.

[00:50:00] Also, note that this is something the agency is very conscious about right now and about how we respond to society's requirements, and this is something that you as the consumer have control to protect your data and put those restrictions on there so that you can remove other person's ability to see it. And also remember that it's your record. This is something that you can take ownership for and control on.

Check the audit logs to make sure that you understand who is accessing
[00:50:30] your record, so that you are informed about what is going on with your
health data. It sits here in our system and we have that protection around

it, and it's important for you to understand that it's yours and those protections exist for you to be aware of what goes on.

Mark Metherell: What about the children of a parent who's affected in domestic violence?

Tony Kitzelmann: So that would be under our children and care program where we actually have gone to the level of providing that next level of protection around those. Cause when children are vulnerable, persons are vulnerable, the [00:51:00] agency has to take a more proactive role in regards to supporting that.

So that is a program that we're currently working on, and we're doing a lot in this space to make sure that those protections are just overflowed across there. It's always the concern, and I hear people saying what if my spouse got access to the record and was able to see where the healthcare was provided for a child who might be either at risk or in a domestic violence situation or in care?

[00:51:30] The ability to restrict those records exists today, and it's something that we encourage the owners of the record to take control of immediately. You should always remember, take control of your records, set your record access control, monitor the use of the data and be proactive about your content.

Mark Metherell: And also, sorry another one for you is, Deb asks how is My Health Record any different to similar systems in the UK and Singapore which have experienced nasty security breaches? Isn't MHR just as vulnerable?

[00:52:00]

Tony Kitzelmann: No Deb it's not. So when we looked at the examples, and I'm gonna make the assumption that you're referring to the Warner-Cry incident that occurred in the UK last year, or the Syntel breach that occurred. In both those circumstances, there was an attack against a piece of infrastructure that wasn't the core central repository, and occurred in a primary healthcare facility. In Singapore, it was in a hospital, and we had the similar situation in the NHS digital.

[00:52:30] The My Health Record system is a large, resilient piece of infrastructure. Whilst attacks will occur in their broader eco-system, we're privileged by having the ability to bring scale to our security and provide a robust model that goes further than what you would see in a normal private health clinic for example, where a breach may occur.

Mark Metherell: Right. Sorry, another one for you Tony. Jane asks, I've had a My Health [00:53:00] Record for the last few months. I have been to the doctor's many times since, but I have no records displaying, which means the doctors are not uploading. Why do people have to ask their doctors to upload? It makes us feel uncomfortable. Why can't they just do it?

Tony Kitzelmann: Because this is the joy of having control of your record. David talked about digital literacy, I spoke to my GP about My Health Record and said, my personal health record not the My Health Record. I said, "Is my treatment for my prescription being uploaded on the system?" And he goes, "I don't [00:53:30] know." And I said, "But I want it." And he went, "Oh, okay." And he did it. He jumped in, logged in and put it up there. I actually asserted my right as the owner and said. "Do your job. Put my data up here, I want it available when I need it."

So unfortunately, take control of your record. If your healthcare provider isn't uploading, ask him to upload. It's your data. I think that as society changes, we're gonna demand more out of our healthcare practitioners [00:54:00] because we're gonna become more aware and more empowered. If I've gotta get my car serviced, I go to a place that I trust and they look after it and do a good job on it.

If my doctor doesn't give me the service I need, I'm just gonna go somewhere else to get the care I want and where they're respectful and [inaudible 00:54:09]. If I don't want an upload, I want them to respect that, but if I want it uploaded, I expect them to respect that and put that data up on the system.

Mark Metherell: If a doctor's part of MHR, doesn't it happen automatically? I mean if you have an MHR record, isn't the prescription PBS and Medicare data going on to your record?

[00:54:30]

Tony Kitzelmann: So the PBS and MBS data doesn't go up, but there are also the health summaries that are uploaded, the interaction between the doctor- there may be something there for example, if you see your GP and he puts some notes on your file about something, a chronic disease or just a general update, Tony needs to lose a little bit of weight. That's the sort of stuff that you have the right to say, "Put it on my record." That's, information I want to be available.

David Hansen: And look, I might add at that point that digital literacy and use of My Health Record is one thing for our healthcare, but I think increasing health literacy in the community is gonna be a really important part. My Health [00:55:00] Record is only a tool, same with the electronic medical records and the electronic health records. Increasing the health literacy of our population is really important as well.

And individually, whether you have a My Health Record and take control of it, or whether you opt out and particularly if you opt out; you need to think about how you do manage the information about your healthcare so that you can be telling your healthcare providers about your health history.

So I think there's a whole range of things whether you're using My Health
[00:55:30] Record or whether you're not, is to be literate about the sort of health
information that your doctor needs. And to Tony's point, making sure
you're getting really good care from those health professionals.

Mark Metherell: Dean, do you get the impression that typically people as they become more aware of My Health Record, are going to be perhaps more assertive, wanting more information available on their record? Do you have a feel for that?

Dean Martin: I certainly hope so. I'll give you an example. I think there's an assumption
[00:56:00] that information already flows, and it should. But actually, in many cases it
doesn't and the consequences of that can be quite severe. So I think that
the more that people understand how My Health Record works and the
more that they, as everybody's been saying, take control of that
information, are assertive about what's there, what isn't there; then the
better the care and treatment they'll actually get and the fewer mistakes as
well.

[00:56:30]
Mark Metherell: Would that be your view Aaron? Do you think from the people you're representing, wanting their doctors to put up the information?

Aaron Cogle: Yeah. There's definitely many different viewpoints within the communities
that I represent. Many people think that the benefits to My Health Record
[00:57:00] outweigh the risks and particularly people with multi-conditions, multi-
morbidities are poly-pharmacy for example. So it can stop things like being
prescribed the same medication a number of times, and people who've
already benefited from that.

But there are large parts of the communities I represent as well which are
already at risk of criminalization in the society in which we have. And My
Health Record presents some risks in relation to that, so the question
[00:57:30] really for my membership is to make an informed decision about
understanding what the benefits to your health of My Health Record can
be, but then also understanding that information can be shared with the
tax office, the immigration department, ATSEC, et cetera.

So if that's the case and you don't want it to be shared in that fashion, then you might want to make a decision to opt out for now and see how it plays out.

David Hansen: Can I just add though? The legislation changes are very explicit, that to
occur, will have to be done through a judicial process and that's something
[00:58:00] that we take seriously, because a lot of people think that the tax
department could just call up and say hey, I wanna see Tony Kitzelmann's
health record. If it's not valid and aligned and if it's not jurisdictionally

supported through a legal process, then that would be unlawful and we would not release that, cause it's not our data.

Aaron Cogle: Absolutely.

David Hansen: We just wanna be on top of that, cause that perception that the tax office can just come along is like, no I don't think so. My tax return has nothing to do with my health.

[00:58:30]
Aaron Cogle: Absolutely. That definitely was the case before. It's not the case now, and those changes are absolutely welcome. But in some circumstances, which we don't know yet, through a legal process, so warrant and subpoena; that information may well be able to be shared in future, but that hasn't been before a court yet. So we don't know when, and those are the kinds of risks of criminalization, policing and surveillance that people in already surveilled, criminalized parts of the community need to be congnisant of when they're thinking about signing up for a My Health Record.

[00:59:00]
Mark Metherell: Right, thanks Aaron. Well look, I think we've run out of time. I don't know if anybody wants to make any closing remarks.

Tony Kitzelmann: If I may, just a bit of a plug for my team, the professionals that support me. This is your record, folks. Jump on board, take control of your health data, put a record access control on there and look after it. It's yours.

Mark Metherell: Thanks very much, Tony. Thank you David, thanks Dean, and thanks Aaron.

Aaron Cogle: Thank you.

[00:59:30]
Mark Metherell: And just so you know, the next in our series is digital inclusion in health literacy and that will be at this time next Thursday. Thank you and good afternoon.

Section 3 of 3 [00:40:00 - 00:59:42]