WEBINAR 8

Embracing Change

Applying the NDIS Practice Standards in Psychosocial Disability Services

Governance, Information Management and Privacy for registered NDIS providers

WEBINAR REPORT AND TRANSCRIPT

Webinar held on 3 December 2020, 11:00AM – 12:00PM

Presenters

- Daniel Kim – Host, Redback Connect
- Katrina Broadbent, Account Manager of the NDIS Audit Program at PricewaterhouseCoopers
- Mae Tanner, Lawyer and Manager of Training at Justice Connect
- Catherine Scott-Richardson National Manager of Governance, Safety & Quality at Stride

Participants

243 people registered to attend the webinar

TRANSCRIPT

DANIEL KIM:

Yes, a warm welcome and thanks for joining us for Episode eight in the Embracing Change webinar series. I'm Daniel Kim, your host. I'd like to begin with acknowledging the Aboriginal custodians of the land on which we meet. And to me that's the Gadigal People of the Eora nation here in Sydney. I pay my respects to the elders, past, present, and emerging. I also acknowledge the lived experience of people recovering from mental health conditions here today, and in our community and their contributions to the mental health sector, particularly those who contributed to work of this project.

A word used about language in the Mental Health Sector, and its use in reference to the NDIS. In the Mental Health Sector, the term consumer is often used to describe a person accessing a mental health service. In the context of the NDIS, we will use the term participant.

So, the topic today is governance, information management and privacy, and helping us delve into all the ins and outs thereof, are three presenters joining us from across the Eastern Seaboard today, not in the studio. A bit of a change. You need a bit of a change in your life sometimes, if you haven't had enough already in 2020.

But first on the panel is an NDIS approved Quality Auditor Assurance Manager from Pricewaterhouse Coopers, Katrina Broadbent. Katrina, I think I'd just butchered your surname. Katrina Broadbent. Welcome to the webinar. Katrina.

KATRINA BROADBENT:

Hi Daniel. Pleasure to be here.

DANIEL KIM:

Thank you very much. I'll get your name right from now on. But you know - when people like me think of PWC, we might think big four, consulting, huge corporations and so on, but you actually help smaller organisations and providers too.

KATRINA BROADBENT:

Yeah. So as approved quality auditors, PWC act on behalf of the Commission to provide certification services for NDIS providers of all sizes. For both the multi-site nationwide providers and also your single staff providers.

DANIEL KIM:

Yes, looking forward to hearing about how you can help small providers and sole traders as well. Also, Katrina's colleague Beck Auld was also scheduled originally for this program but was called away unfortunately. So, on the plus side we'll be hearing more from Katrina today.

Also joining us from a legal perspective is Mae Tanner, Manager Training for Justice Connect. Great to have you with us Mae.

MAE TANNER:

Hi Daniel. Thank you and hello everyone.

DANIEL KIM:

And Mae, just over the last four years alone, you've been helping hundreds of organisations better understand their legal obligations around privacy.

MAE TANNER:

That's right, Daniel. The part of Justice Connect that I manage is our legal service, legal training service for not for profit organisations, and we deliver legal training on a whole bunch of different topics - but Privacy Law is one of the most popular ones. And this week alone, I've delivered two three hour customised sessions on Privacy Law. So, it's a very popular topic.

DANIEL KIM:

Yes, it's a tough cookie for a lot of organisations out there, particularly when they're already busy enough trying to get their heads around the practice standards for the NDIS - but also, they've got to think about the Privacy Laws too. So, I'm really looking forward to hearing what you have to say with us today.

And our third presenter of course, is National Manager, Governance, Safety and Quality at Stride. It's Catherine Scott-Richardson. A warm welcome to you Catherine.

CATHERINE SCOTT-RICHARDSON:

Thank you, Daniel. It's a pleasure to be here.

DANIEL KIM:

Yes, it’s always wonderful to get a provider's viewpoint on these webinars. At Stride, you've got a particularly long and beautiful history of being in the mental health sector.

CATHERINE SCOTT-RICHARDSON:

That's right. It might not be known by many, but Stride, formerly Aftercare, was Australia's longest established mental health charity. And we provide specialist mental health services to people with mental illness and complex needs, since 1907. We were actually established at that time by Banjo Paterson's niece Emily Paterson, who lived in close proximity to the old Rozelle and Gladesville hospitals, where she started the commencement of psychosocial supports for inpatients who were soon to be discharged or recently discharged.

DANIEL KIM:

Yes, that's such a beautiful backdrop. You're more than just an NDIS provider. There's a lot more you get involved with in the broader mental health sector as well. So, we're particularly looking forward to hearing from you.

CATHERINE SCOTT-RICHARDSON:

That's right.

DANIEL KIM:

So that is our – thank you - knowledgeable panel today. And over on the next slide, we are going to launch the now customary poll, where we ask you to rate your current overall knowledge of the NDIS Practice Standards and registration requirements. When you see it pop up on your screen, please rate your knowledge from low to expert. And if you've joined us for the first time today, what we've been doing is polling the audience at the start and at the end of each webinar. And you don't need me to tell you, we are looking for a trend that isn't downward.

So, moving on while you do answer those (indistinct) polls, and while we wait for the final few poll responses to come through - on the next slide, you'll see where we are up to in the overall 10 part program with today being the last webinar before we break for Christmas and for New Year. And the slide after that lists the three main themes we are covering today, and the various topics within each theme. And moving to the next slide, you can also see all the learning outcomes we are aiming to achieve, from presenting today's content, and have no fear, I will not be insulting your intelligence by reading these out loud for you.

Just some housekeeping while you read all of those dot points, and while we do wait for the final poll questions to come through. Do join the conversation today and ask questions for the panel. We'd like you to click on the dark blue hand icon at the top of your screen. And you'll also notice a light blue icon in the vicinity which will give you access to download resources. And the Resource Pack that's being made available for today is actually quite comprehensive, particularly compared to previous episodes. So, make sure you get your paws on those.

And finally, of course, this webinar is being recorded and will be shared after today's event. So, you can come back to it and we encourage you to share it with others. And Katrina, that means it's now over to you.

KATRINA BROADBENT:

Thanks Daniel. So, for today I’m going to be talking about Governance and Information Management and Privacy, from an auditor's perspective. So, governance is a key foundation in successful business. It focuses on the top down decision-making structure and process that drives an organisation. But for NDIS providers whose main focus is service delivery and data base supports, it may not be a number one priority for you to set aside adequate time to really think about what that governance is, and how it relates to you as an NDIS provider.

As the standards apply across all providers, whether you are a sole trader or multisite national organisation, understanding how governance fits within the NDIS and applies to you as a service provider, can improve the overall quality of supports you provide, and ensure the participant is really at the center of your practice. As auditors, no matter what module or standards we are setting, we want to see that there is a synergy within your operating model. Do your policies align to practice? Are you really doing what it is that you say you do?

I like to think of it as a triangle made up of three equal parts. The first part is documentation. This consists of your policies, information booklets, welcome packs, flyers and websites. How you come across as a provider in a written format. The second part is the system. Your Client Management System, client intake procedure, recruitment of staff, along with training and induction. Feedback and surveys are important too. Not just from participants and families, but also from your staff as well. Finally, the third segment is practice. And this is probably the most important one. Physical service delivery; what you and your staff are doing on the day to day basis with, and for your clients. Do your staff really have an understanding of their role and what it entails? Is there a culture of client focused service delivery, and is the environment you are providing supportive of this culture? Are clients really understanding how your services are assisting in achieving their goal? When we see evidence through an audit that all these things are occurring and not just in silos independently of each other, but really feeding into each other to influence how a provider grows. This is what we refer to as best practice.

So, breaking down the individual outcomes and standards under Governance and Operational Management, you'll see the key words that I've highlighted in bold. Each participant’s support is overseen by robust Governance and Operational Management System relevant, proportionate to the size and scale of the provider, and the scope and complexity of what's (inaudible).

Proportionate, what does that word actually mean? Auditors must take into account the size of the provider. How many staff you employ if any, and whereabouts are you based. The scale of the provider refers to the number of sites, and the scope and complexity of the support. Are you providing supports under multiple registration groups? Do you provide what we consider high risk support, such as Implementing Behavior Support Plan? No two audits are ever going to look the same. Management structures and system, tools may differ between small and large providers, and that's okay Auditors do not expect the same evidence from different types of providers.

In order to achieve the governance and Operational Management Outcome, providers should demonstrate the following indicators. Indicator 1 focuses on opportunities provided by the governing body for people with disability to contribute to the governance of the organisation. Most commonly throughout audit, we find there is a lack of evidence and understanding to support this indicator. Some providers believe a survey is enough but cannot demonstrate how the feedback has actually contributed to organisational change or policy development. Some believe it's just about having someone with a disability on (indistinct).

I want to provide a few real-life examples of best practice we've come across, and hopefully you'll see how that triangle diagram I showed at the start fits into this. When policy and procedures are updated on an ongoing basis, shaped by day to day learning - so for instance incidents, whilst not what we really want to occur, but unfortunately at times, they are inevitable - they result in policy and procedure changes. So, changing the way you do something on a daily basis and therefore demonstrated quality improvement from the learning of that particular incident. Another example we've seen included participants focus groups, utilised for participant related process development and review. So, get your clients involved and their voice heard on what it is they want to see in your service delivery, and how they want their support provided to maximise their goal potential.

Indicator 2 looks at a Clearly Defined Structure. Overall, as auditors, we have identified weaknesses in structure that are set up by external consultants, or off the shelf purchase policies and procedures. These actually provide more work for providers. Along with clearly defining governing roles and responses. This is often overlooked with the assumption that when you hire support staff, they're just going to know what their job is and how to do it. They're going to know their responsibilities and how their roll fits into the big picture. Some examples of best practice we've seen, most commonly involve a clearly defined board structure with regular operating rhythm. This involves clearly defined governing roles and responsibilities that ensure decisions are made and systems monitored and reviewed at regular intervals. This flows through to an overall organisational structure by making sure your organisation structure is clearly defined and there is an understanding of which role fits where.

Indicator 3 looks at the Skills and Knowledge of the Governing Body. Again, overall as auditors, we have identified weaknesses between position descriptions and actual day to day practice. What is written on paper, may not actually be occurring when it comes to service delivery. Also, training. Training is crucial for your frontline workers, but it's often overlooked when it comes to governing members, upper management and the board level, where they may not be interacting with participants face to face on a daily basis. This training is still important to foster a wider understanding throughout the organisation.

Examples of good practice include Board Skills Matrix and Gap reviews, which then lead to identified training needs for all members of an organisation. And a Training Log with details for professional development completed, and by governing members, not just your face to face staff.

Indicator 4 focuses on Business and Strategic Planning. This is a difficult one we often see with small providers. Examples of good practice include Strategic Business Plans that cascade through organisations, with evidence of reviews and updates. So, whether you're a one-man band or a multi-site organisation, forward planning is critical. A great example we've seen was a Compliance Register that took into consideration legal requirements, along with organisational (inaudible) which linked to not only participant needs, but staff needs too.

Indicator 5 focuses on the Performance of Management. We've seen various levels of understanding of what this section requires. Mostly we see a lack of demonstrated evidence in practice. So, there may be policies, procedures, and KPIs in place, but there's no written record to support the implementation of any of these. Examples of good practice include position descriptions, or operational plans with clear KPIs governing roles, along with records that demonstrate (inaudible) in action. Another example includes Performance Plans that demonstrate continuous improvement of each role, with a focus on ongoing training and incumbents with records of (inaudible).

Indicator 6 looks at the Qualifications and Suitability of Management. So, we want to see all roles from the top down able to demonstrate an understanding what it is they are doing and why. This could include a clearly defined structure showing reporting lines, for instance, CEO to (inaudible) Clear position descriptions that outline role and authority, responsibility and accountability that link through to performance review. And through interviews with the auditors, your staff are able to articulate their role, authority, responsibility, and most importantly (inaudible). This includes top management and the executive level.

Indicator 7 refers to Delegated Responsibility. If something happens to the person in charge, touchwood, is there a clear plan as to who would take over and how the organisation would seamlessly provide support to clients? We've seen weaknesses as providers struggled to define this, when minimal people in the business are at startup. Or there's a mutual understanding that there will be someone that takes over. But there's no documentation to (inaudible). Examples of good practice include Delegation of Authority Schedule that defines all organisational activities requiring authority, and roles that are incumbent on that delegation, alongside a Business Continuity Plan that incorporates levels of delegation in the event of a disaster. Again, it's all about forward planning.

And finally, indicator 8 looks at Conflicts of Interest. Overall, as auditors, we have identified weaknesses when conflict of interest policies and processes are not implemented. For example, board meetings not consistently reporting conflicts of interest in accordance with their policy. There's no clear definition of the standing within the organisation of what a conflict of interest is. So how can you expect your staff to really understand what a conflict of interest is. Examples of good practice include Conflict of Interest Policy that covers from governance to direct support conflict of interest. A clearly defined conflict of interest policy and training, to ensure understand by staff on what this entails and how it's managed.

Moving on to Information Management and Privacy from an audit perspective. What is included in these outcomes and what evidence do we look forward to identifying whether a provider will conform to these outcomes, or require further improvement in order to satisfy certification requirements?

Records are the number one source of information used by auditors. So, it's a given that Information Management would be an important consideration for providers, given the level of sensitive and personal information you're collecting from participants when it comes to the NDIS. In order to asses a provider against the outcome and associated indicators related to Information Management, some examples of what an auditor may look at are the type of information that is being collected. Where is it stored? Who has access to this information? For example, is it restricted to specific clinicians and management personnel within your business, or do all staff have access? And how exactly do these controls work?

One element we see provided fall over is in their data storage arrangements. Some providers, again, will purchase an off the shelf program that will manage client contact details and participants plan information but fail to ask the fundamental question as to where is the data being stored? Is it within Australia, or is it housed offshore? In which case, how can we be sure that Information Management System is adhering to relevant state based (inaudible) commonwealth privacy requirements and law. Without knowing this information, it's difficult for providers to evidence they have a sound Information Management System.

You may have an extremely comprehensive policy written in collaboration with the consultant that goes above and beyond leading the outcome and indicators. But unless this system can be demonstrated in practice, it means very little. Policies must align to practice. As auditors, we're going to want to see evidence that the providers policies on Information Management, feeding into their system and process development. Not only will we look at the type of information that is being collected, and the system in which you're storing it, we will also use participant interviews to dig deeper into whether your clients fully understand how and why, that information is being collected and stored.

Providers will often have a very close relationship and rapport with their clients. During audit, we see providers with an excellent information management. All records are kept up to date and secure. Participants are fully informed of where and how their information is to be used. However, when it comes to sign consent in relation to this understanding and agreement, there is none. Some providers rely on verbal consent, which can be hard to evidence in an audit scenario. In particular, what information the participant has provided consent to be used, distributed, and shared.

Alongside support plans, NDIS participant information is often shared (inaudible) multiple providers and agencies. Participants privacy goes hand in hand with information management, and it is the provider's responsibility, to ensure participants privacy is at the forefront of their service delivery. Privacy and dignity is an outcome of the full module on the Rights and (indistinct). The overarching outcome says each participants access to support and protect their dignity and the right to privacy. Before it's broken down into indicators, demonstrate (inaudible).

The NDIS Code of Conduct underpins participants rights to privacy and (indistinct) set out by the UN Convention on Rights of Persons with (indistinct). The Code consists of seven elements that apply to all providers and persons employed or otherwise engaged by them to deliver support and services (indistinct) NDIS. As auditors, we will be looking at these seven elements underpinning the core of your policies and (indistinct). It is more than just having a privacy (inaudible) with a company branding on the top. Whilst it's important that you adopt the code of conduct to reflect the values of your organisation as a provider, NDIS providers should use their existing employee engagement, human resource, and governance arrangements, to ensure compliance. This will include considering whether operational policy procedures and training activities reflect the Code.

We often see providers fall over when it comes to ensuring confidentiality policies and information made available to participants, in the language, mode of communication, and terms that that participant is most likely to understand. An example includes providers failing to offer online accessible information, in regard to their Confidentiality Policy despite providing support through online telehealth platforms, during COVID lockdown.

Again, as auditors, we're going to want to see a model where privacy and dignity is embedded into practice, and the culture within your organisation through examples, such as (indistinct) of information, clear and documented consent, open communication, and information surrounding confidentiality are a focus on individual participants privacy. I'm now going to pass it over to Mae, to speak about the provider responsibility (inaudible) privacy. Thank you.

MAE TANNER:

Thanks very much Katrina, for that wonderful presentation and I think they'll be a bit of overlap in what we're speaking about, that really drills into those key issues. And happy International Day for people with Disability, to everyone who joined us today. I'm really happy to be included as part of this Embracing Change webinar series so thanks very much to the Mental Health Coordinating Council for inviting us along as well.

I'm going to be speaking to you very briefly today about some of the key Privacy Law considerations for NDIS providers. I've got a very short amount of time, so I won't be going into any detail. I'll be introducing some basic information to get you thinking about how the Commonwealth Privacy Laws apply to your organisation, and I'll also be talking about how Justice Connect might be able to help your organisations as well.

So, to that end, I just wanted to explain a little bit about our service. So as Daniel mentioned at the outset, I am the Manager of the Not-for-Profit Law Training Enterprise that's part of the legal charity Justice Connect. So Not-for-Profit Law is a program of Justice Connect that aims to help not-for-profits and charities and social enterprises with legal issues. And we do this in a number of ways.

The first way is through our resources. So we've got over 300 legal resources on our website that have been written for not-for-profit organisations like yours, and they are all available free of charge and I will be pointing you towards some of the relevant ones for today's session at the end of this.

We also have a free legal advice service, and some of your organisations may be eligible for this. We can either provide you with legal advice through our team of in-house lawyers, or if the matter is very specific and outside our range of services, then we can refer you off to one of our member pro bono law firms.

We also do a lot of advocacy in the not-for-profit space and we have a certified social enterprise that provides legal training for not-for-profits. And so that's the part of Justice Connect that I am from.

Before we get into the requirements under the Privacy Act for you as NDIS service providers, I just wanted to provide a little bit of context about why Privacy Laws are so important. I think it's pretty obvious that we're required to comply with the law, that's in itself very important. And there are also some really big penalties that can apply for breaches of those laws. But I think it's equally important not to lose sight of the fact that, what we really care most about is our clients, and other people whose information that we're collecting, their personal dignity and their personal security. And we also care a lot about the trust that those individuals have in our services. Because if we don't have that trust, if we can't rely on a reputation, then we won't be able to provide services. We won't be sought out for our services. So, I wanted to provide a few examples of where charities and not-for-profits have fallen short of Privacy Law standards, and some of the consequences of that.

So, we've had cases where really big charities have made, unwittingly, made information available online through their website, about very sensitive and health matters. We've also seen failures in charities to adequately train staff and volunteers who may be working from home, and therefore exposed to greater privacy risks. We've seen incidences where we've had malicious hackers get into the back end of websites and get hold of information that organisations didn't even know they were storing. And we've also seen warnings that (indistinct) as not-for-profits and charities, we're particularly vulnerable to cyber-attacks because of the large amounts of sensitive information that we're often storing, and because we often don't have the state-of-the-art IT systems in place.

So that's a bit of background for today's session. And I really wanted to look now into whether Privacy Laws might apply to your organisation and how to comply with them. And the way that I'm going to do this is through a case study. Now, before I get into the case study, I do need to let you know that I am today providing general legal information and not legal advice. It's an important disclaimer that I need to give as a lawyer. And also, that I'm talking about the Commonwealth Privacy Act of 1988, and the Australian Privacy Principles, or APPs that sit within that. There might also be a State Privacy Laws and Health Records Act that might apply to your organisation as well. So please be aware of that.

So, in this short session, I've used this fictional organisation of the Health Hub, and the Health Hub is a large, registered charity that provides psychosocial support services to clients under the NDIS. Now, Jerome here is a client, a new client of the Health Hub, and he's made an appointment to meet with Penelope, a case worker, and Penelope's going to collect information from him. And this will include his personal details. So, things like his address and his date of birth and his full name. She's also going to collect information about his home life and culture. About his history of mental illness and about his desired treatment outcomes. So, Penelope wants to know what processes she should have in place, to make sure she's meeting her requirements under Privacy Laws. And the first thing that Penelope will need to know is, does the Health Hub actually have to comply with the Privacy Act?

So, this is a question that you might have as well. And the number one way that organisations are brought under the Privacy Act, is if they have a revenue of more than three million dollars. So, we've said that Health Hub is large. They may need to comply simply because of this. But even if your not-for-profit is a small, or for profit even, is a small business and has a revenue of less than that, you may still need to comply for some other reasons. Now that might be because you have a contract with the Commonwealth Government to provide services for example. And so those services that you provide under that contract will need to be compliant with Privacy Laws. And this would usually be set out in your contract or funding agreement.

Another keyway that NDIS providers can be brought under the Privacy Act is through providing a health service. So, any organisation that provides a health service, not just hospitals and medical practices, it could be something like a school or a childcare organisation that provides some health services as part of the other activities that it does. All of these organisations will be bound by the Privacy Act. And there are also some other reasons why organisations need to comply. And there's also an option to opt in to be governed by the Privacy Act, and when I last checked, there are about six hundred and fifty organisations that have chosen to do this. The main reason that you would do this is to increase consumer confidence and confidence of your clients that you are protecting their personal information and you're prepared to be bound by law to do that.

If you don't think that your organisation is bound by the Privacy Act, then it's still a really good idea to comply with these basic principles. As I said, in the interests of your client’s dignity and personal security.

The next question Health Hub will want to know, and Penelope, will want to know when she's collecting Jerome's information, is what information she's collecting. So, the Privacy Act governs personal information only. And it's important to understand what that is. And it's classified in three ways. And I'll read out what the definition of basic personal information is.

It's information or an opinion about an identified individual, or an individual who's reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not. So, it's quite a wordy definition.

But the key things that you need to take - and it's quite a broad one - the key things that you need to take away from that are, that as long as the information reveals the identity of the person, it doesn't matter if it's true or false, it doesn't matter if it's fact or opinion, and it doesn't matter whether it's been written down or not. So, it's a very broad definition.

And as you can see from the examples that I've popped up on the screen here, all of those pieces of information about Jerome, his name, date of birth, if Penelope takes a photo of him, all of that is considered to be his basic personal information. The next subset of personal information that we need to know about is sensitive information. And here are some examples on the screen. This is not an exhaustive list, but you can get a sense already here. But when Penelope is talking to Jerome about his home life and culture, she may also be collecting sensitive information from him, for example, about his racial or ethnic origin and about his religious beliefs.

The next subset of information, personal information, is health information. And that's considered particularly sensitive and it require special treatment under the Privacy Laws and State Health Records Laws, if they apply as well. So, health information has a broad definition and it includes information about past, present, or future physical and mental health or disability. It also includes personal information collected to provide, or in providing a health service. So actually, we can see that when Penelope is collecting all of this information from Jérome, it could all be considered to be health information if she's collecting it in the context of providing him with a health service.

So, for you, it's really important to know what types of information you're collecting. And Katrina has already talked about the importance of this when PWC audits organisations, they want to know what kinds of information you're collecting, because higher standards are required in particular for sensitive and health information.

So, when Penelope actually goes to collect information from Jerome, there's a few things that she should know first. And at justice connect, when we provide organisations with training on Privacy Law, we use this Personal Information Lifecycle to explain what the requirements are, and we start out by talking about the systems and policies that organisations need to have in place.

And the first relevant principle is Australian Privacy Principle One. And that requires Health Hub to have two things squared off. The first thing is they have to take reasonable steps to implement practices, procedures, and systems to comply with the Privacy Laws. And these are really practical measures that you'll take as organisations to protect people's personal information. Like having private spaces to meet with clients, password protections on your devices, safe storage systems, and Katrina's has already mentioned cloud storage, making sure that that's safe and ideally hosted in Australia, limiting access to information even within the organisation as Katrina's already mentioned as well. So, if Penelope's working from home, think about the extra layers on top of that. The extra measures that Health Hub will need to take to make sure that she's complying on behalf of Health Hub with APP One.

The second thing Health Hub needs to have in place is an accessible privacy policy that explains how it uses and manages personal information.

So, the next step, when Penelope's actually collecting the personal information from Jarome, she needs to be sure of a few things. And collection of personal information is governed by four APP's, two, three, four, and five. The really key ones here are three and five. So, under APP Three, Health Hub must only collect information that's necessary for the organisation's functions or activities. So, Penelope needs to make sure she's not collecting additional information that could expose Health Hub unnecessarily to breach. Penelope must ensure that she collects Jerome's personal information by lawful and fair means. She must collect that directly from Jerome, unless there's a good reason not to. And because she's collecting, sensitive and health information, she also needs to get Jerome's consent.

Next APP Five requires Penelope to explain a few things to Jerome when she's collecting his personal information. And we often call this a privacy statement or a Collection Notice. So at the time or before Penelope collects Jerome’s information, she needs to make sure that she takes reasonable steps to make him understand who health hub is, some basic information about what they do, how they will use his personal information, how they might disclose his personal information outside the organisation and how can he access the Privacy Policy that I mentioned under app one, so that he knows how he can make a complaint about how his personal information has been used, or request access to his personal information.

So back to the case study now, we're back with Health Hub and Jeromy is progressing well and achieving his goals under his NDIS plan, and Penelope identifies that he could also benefit from physiotherapy for an injury to his legs. So, she wants to refer Jerome to another service. Can Penelope share Jerome's information with another service?

So here, Penelope is looking at disclosing Jerome's information and use and disclosure is governed by another four APP's; six, seven, eight, and nine. The key one that we need to consider here is APP Six. And I often refer to this as the golden rule of privacy. And what APP six says is that you can only use and disclose personal information for the primary purpose for which you collected it. Unless there is consent or unless another exception applies. Thankfully, because Penelope has complied with the other privacy obligations that precede these ones, she has already explained this primary purpose to Jerome under app five with that Privacy Statement. So, we know how she can use the information. If this type of referral wasn't mentioned in the Privacy Statement, then Penelope would need to go back and seek Jerome’s consent to provide the information to the organisation she's referring him to. And in any case, it is best practice to always get consent when doing a referral, so that's the best thing for Penelope to do.

So, Jerome begins to feel a bit uncomfortable about what notes Penelope is taking about him and he wants to get access to his files. So, we've got a question now from Penelope, does Jerome has a right to access his own personal information? And the answer is yes. Under Privacy Laws, and particularly here we're looking at APP twelve, Jarome has a right to access his own personal information. There are some exceptions to this, but they are quite limited. So, it's important to know when you're taking notes about clients, to be thinking about who might be able to access this information and that could include the person you're writing in about.

There are some other APP's you need to consider in this part of the personal information lifecycle. As you can see, there are four more. APP ten, requirements to keep information up to date and ensure the quality of that information. APP eleven, to take steps to keep Jerome's personal information protected and secure. And APP thirteen, if Jerome has been able to access his personal information and he wants Health Hub to correct anything in there, then Health Hub is generally required to do so.

The final thing that happens in our case study now is that over the weekend, Penelope bumped into a former colleague Saima at a barbecue. And Penelope knows that Saima will want to hear all about how Jarome is going. And so, Penelope shares the latest details of his treatment and progress at the barbecue, talking loudly over the sound of sizzling sausages. Is there a problem with this?

So, what Penelope has done could be a breach. A breach of privacy is an unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information. And the regulator for the Privacy Act, the office of the Australian Information Commission, has best practice guidance about how to deal with a breach. And this will include, containing the breach, assessing how serious it might have been, potentially notifying the individuals affected and the regulator, and reviewing practices and making sure that these kinds of things don't happen again. There is also now a Notifiable Data Breaches Scheme where there's been a serious breach, and this includes requirements like notifying individuals affected and notifying the regulator. And after there's been a breach, as I've mentioned, it's important to review your processes and go back to the beginning of that information lifecycle and make sure that you've got all the right systems and policies in place.

So hopefully that's given you a bit of a flavor of some of the key considerations that you need to take as NDIS providers, to make sure that you're complying with these really important laws. Obviously, it's been a very brief overview, but as I mentioned at the beginning, there are a lot of ways that Justice Connect can help your organisations, and I wanted to point you to some specific resources that we have.

So if you go to our website, which is www.nfplaw.au and you go into the people involved section, we've got a whole free Privacy Guide that's been written for not-for-profit organisations, with some really helpful examples in it. And that also sets out both State Laws that I mentioned that could also apply to your organisation. We also have a Fact Sheet on How to Comply with the Notifiable Data Breaches Scheme I've just mentioned. And another Fact Sheet on Cyber Security.

We may also be able to provide your organisations, as I mentioned at the beginning, with legal advice. So, head to our website and click on the link, legal advice, to find out more about that and to lodge an inquiry if you'd like to. And we also, as I mentioned, provide legal training that's customised to your organisation. So when it comes to Privacy Law, we would customise a three hour session, go into detail on all the principles that I've mentioned in an engaging interactive way, so that all of your staff and volunteers and board members, understand how to comply with these really important obligations. And finally, we also provide shorter webinars on all of these topics, where you can sign up, anyone can sign up for a small fee, and we have recently delivered one of these on Privacy Law, and it's still available on our website. So, go along to training and webinars to find out a little bit more about that. I think that's all we've got time for today. So, thanks so much everyone for listening.

DANIEL KIM: Thank you Mae. Thank you. Yes, thank you for taking us through it so thoroughly Mae. And also thank you to Katrina before. Understanding what all of this looks like for a provider to implement and manage is the next topic. So, Catherine, it's over to you.

CATHERINE SCOTT-RICHARDSON:

Thank you, Daniel, and thank you Katrina and Mae. They were both really interesting presentations. And while listening to you, I have curbed my natural instinct to want to desperately rewrite what I'm about to present to try and make it more interesting.

As Daniel mentioned in the introduction, I'm from Stride and we are Australia's longest established mental health charity, providing specialist mental health services. So, we do provide a full range of mental health services designed to support those with a lived experience of mental distress. So, the care and support we provide ranges from assistance with developing skills to manage day to day tasks, right through to fully supported accommodation to those with complex needs. We also cover a range of demographics from infant mental health, really young kids, young people through our Headspace programs, adults and also support families and carers. So, what I'm hoping to do today is share very briefly, how stride operationalises Governance Information Management and Privacy within this very unique service context.

So, governance is a framework that accounts for all of the processes of governing organisations and businesses. It's a structure that holds our board and leaders accountable for continuously improving operations, service delivery, staff, and processes and financial performance. Within Stride we're led by a board whom are advised by a number of board subcommittees such as the Service Quality and Safety Committee and the memberships of these committees is additionally drawn from the executive and leadership teams. The board members are drawn from the human services sector primarily and supported with a comprehensive induction and some bespoke mental health training, such as First Aid in Mental Health.

The internal committees that then report into the executive and leadership forums enhance currency of knowledge and practice. And the role of governance within mental health organisations such as Stride specifically, tends to look a little bit different than it does in other types of industries. So, we're interested in maintaining and improving the quality and safety of consumer participant care. This falls under what we call clinical or service delivery governance whereas the business performance, the compliance with laws and regulations, as well as ethics, tends to fall under corporate governance. So, there is a strong connection between corporate and service delivery governance, because our revenue cycles and reimbursement policies tend to fall under corporate governance, but they directly affect the reimbursement monitoring and risk management activities that then come under our clinical governance.

So, governance in health care organisations such as Stride, does continue to evolve, as we navigate our way, to designing and implementing an integrated governance system that hopefully transcends clinical service delivery governance and corporate governance effectively. I think this is an area of burgeoning interest within the not-for-profit sector, and I think it's also an area that we are going from strength to strength, as we start to incorporate a greater degree of participation from our consumers, our carers and NDIS participants.

Information Management, I've broken up into how we use the information and the actual information technology. So, Stride requires participant confidentiality to be maintained to the highest standards and to comply with legislative requirements. All participants must be informed about consent, confidentiality, and how that information will be recorded and used. In the case of minors, so our infants, early childhood, young adults who might not be of legal age, this also involves the informed consent, confidentiality, and information sharing, be discussed with their parents, the next of kin, their adult guardian.

All information collected must be recorded in the relevant database or electronic medical or participant records system approved for use in each program delivery area, in line with numerous funding body and legislative requirements. So, I don't know if other not-for-profits experienced this same phenomenon, but we've had a number of electronic medical records historically that haven't necessarily talked to each other or engaged with each other. Things like SupportAbility, MasterCare, and I’ve also included there – RiskMan incident reporting System

So, using the information, we collect data to report on consumer participant type, access, program activities, performance, and must be de-identified when used for funding or reporting purposes, or even used within Stride for service review and service planning purposes. Participant information can only be collected, shared or transferred and reported upon, with consumer participant consent.

Have appropriate security mechanisms for both electronic records and hard copy records and must be maintained to the highest standards and in compliance with state and federal legislation. On commencement of employment, staff and volunteers are orientated to, and advised of their obligations, to comply with federal privacy legislation in addition to Stride’s own procedures and guidelines on confidentiality and acceptable use of the information technology. I'm sorry, this isn't more interesting. Usually would try to jazz it up and make it a bit more interactive.

Onto the Information Technology. So, we ensure that there's comprehensive authorisation systems in place, to manage access to information in order to support sound decision making and facilitate high quality of care and participant services. As a clinician, that's something that's super important to me, that we're able to balance that tension between our obligations, but whilst remaining incredibly person centered and ensuring that the care we deliver isn't compromised or obstructed in any way.

Our electronic records are backed up regularly to ensure that information isn't lost, and archive participant files are kept securely and in accordance with state and federal legislation on information retention requirements.

Onto privacy, which again, is also a little bit of a dry area when I talk about how this is operationalised within our sector. So, under general duty, very broadly speaking, our obligations in respect of mental health worker, consumer participant confidentiality, are determined by a combination of professional ethics, Common Law and legislation. So, we do employ a range of workers and professionals, some that AHPRA registered health professionals - others that we employ as support workers or youth workers. So, there are some slightly different requirements for different staff. Hence, I've used the term, our general duty.

Our release of information, those third-party disclosures, I've chosen to focus on a little bit more because they're often the most ambiguous. They're very time sensitive as a rule, and they tend to pose the most amount of confusion for teams and workers within the not-for-profit space. Certainly, where I tend to feel the most inquiries as it is a little bit less straightforward.

So, there's a lot of different scenarios that we encounter within Stride. Whether it's a subpoena, it's a request for information from Department of Child Safety. It might be a request for information from another health professional or simply a request by the participant or consumer to access their own file. We have a number of procedures in place within the organisation that we've built on more recently and established some templates for staff to use, particularly for the legislated request for information. And these are accompanied by a series of incredibly boring, but very, very useful fact sheets that I refer to in a series of masterclasses that I've been running, for managers and workers within the organisation. The, premise behind these masterclasses has not just been to build the capability of the workforce, but also to increase their confidence in being able to respond to requests for information, to be part of these third party disclosures in a way that's safe and ethical, but as I said, also very person centered and doesn't obstruct care in any way.

So, in conclusion, and just three key messages, there is quite a delicate tension between corporate and clinical governance as it stands within mental health organisations. And this is irrespective of whether they are public, profit or not-for-profit. And then in consideration of this, information management comprises both the architecture and the administration of the systems, and how we best use those systems to shape and enhance quality service delivery. Within mental health organisations like stride, obligations around participant privacy is determined by professional ethics, Common Law and legislation. So, I hope that you're all still awake. I'm going to refer back to our gorgeous host, Daniel with some Q&A. Thank you.

DANIEL KIM:

Thank you for your insights, Catherine. I don't know about being boring. In fact, the impression I got from you was the whole story was about moving from a place of confidence and kindness, to one of structure and demonstrated competence. That was the feeling I got. And I'm sure there's so much there for other providers who might also be on that journey.

That does bring us to the Q&A session though, so now on the slides, you'll see the Q&A with all the panel members. We've got a few questions to get through today, and looking at the time, this is probably one of the most well time kept webinars I've ever been a part of. So, we might have time to get through everything today, and if we do, I'm sure it's a first for us. In case we do run out of time, we'll make sure to get back to you offline via the Post Webinar Resource Pack.

But a quick reminder, for those of you who haven't already asked the question, it's a dark blue hand icon at the top. Now one of the things we've done is, due to the number of questions we've been getting live, but also due to the number of questions we've received pre-submitted as part of your registration process, we've actually gone through and collated similar questions or connected different questions where the answers hit similar themes. So, if some of the questions we're about to go through now sound a bit like generic FAQ's, it's because they are. So, Let's go through these one by one.

First question is for you, Katrina. In your experience, what are some of the model’s service providers are using to provide opportunities for participants to contribute to governance and development of organisational policy?

KATRINA BROADBENT:

That's a good question. So generally, people who have an opinion and they're going to be happy to contribute their opinion, if it means there's going to be change for the better. So, it's important to give participants a platform for them to voice it and make sure it's accessible. So, don't just expect participants to have the confidence to speak up. Tailor feedback opportunities to allow accessibility for all.

You'll find the most valuable information come directly from the horse's mouth. Through things like Participant Focus Group is a great way of ensuring a wide range of participants voices are heard. Participant Advisory models that support key participants to provide input and feedback directly to the board, in order to influence decision making. Providing draft policies to participants, families and carers, prior to finalising. This will provide them an opportunity to comment and actually shape the policy before it's finalised and distributed. And finally, a use of what we call a Consumer Technical Expert on the board and in upper management. So those with lived experience of the NDIS will take on positions of decision making within the organisation in order to ensure participants best interests are at the core of everything you do.

DANIEL KIM:

That last point is pretty interesting, having a consumer on the panel. Here’s a question for you, Catherine. Can you tell us about some of the mechanisms Stride uses to get input from your workforce on management processes?

CATHERINE SCOTT-RICHARDSON:

So, this is an area that we've gone from strength to strength on within Stride. We now have annual staff engagement surveys. In addition to periodic pule surveys for all of the workforce. We have internal intranet-based staff feedback portal that's monitored and tracked. We're also part of the 360-degree leadership program, which gives further opportunity. And we have monthly operational supervision sessions between all of our direct reports, in addition to quarterly leadership forums and half yearly management forums.

DANIEL KIM:

Thank you very much, and here's a question for Mae. What are some of the factors NDIS service providers need to consider in terms of data storage and security?

MAE TANNER:

Thanks Daniel, for that question. I can see that there's been a few questions coming up live on that one, so it's obviously a hot topic. I did mention the APP eleven and that's the one that requires you to take reasonable steps to protect the personal information that you're keeping from misuse, interference, and loss, and from unauthorised access and modification and disclosure.

So, you're required under the Privacy Act to do this. How are you meant to do it? Well, it's basically all of those common-sense reasonable steps that you can take, and these might be part of your organisation's governance and culture, training staff, making sure everyone understands your systems. And they might be more administrative or technical measures that you might take as well. And just a few examples of this, having a clean desk policy, encrypting files on computers, having password protection, secure access to buildings, making sure that people who are working from home have adequate security on all their devices as well.

A couple of the questions that came up that I wanted to address. Really good question and something that Katrina and I have both referred to is, when you're having other providers take care of your security in some way. So, it might be cloud storage, or it might be CRM systems, consumer or customer information management systems. So, the question was, are we responsible for their security, or are they responsible?

So, you need to make sure as an organisation that's bound by Privacy Laws, that those organisations that you contract with, will meet the same standards that you're required to meet. So, you do need to understand how they operate. And when you have a contract with an IT Provider, you need to make sure that they're bound by all of those APP's that you need to meet as well. And if you don't take these sorts of reasonable steps, then you could in fact be liable, along with them, for a data breach that they've caused. So, a really important thing to consider when you're changing your IT Systems for example.

The other thing that I saw come up with, can we keep our records electronically? Under Privacy Laws, I mean, unless you've got any other legal obligations to keep paper records, you are of course, permitted to keep your records electronically. But this is all part of having secure systems and the requirement under APP Eleven to take steps to make sure that they're secure. So, you do need to make sure for all of the physical and electronic information that you're keeping, that you're protecting it in all of these ways. And it also takes us back to that first stage, if you can remember in the Personal Information Lifecycle, of making sure that you've got all of these systems set up before you even start collecting and storing people's personal information.

DANIEL KIM:

Yeah, it's a really hot topic, isn't it? And increasingly so cyber security.

MAE TANNER:

Absolutely.

DANIEL KIM:

In Australia we've got big interest in the topic. Globally we've had in the recent years, like the whole GDPR thing happening in Europe. The Sony attacks in North Korea. All the big International level stuff happening. More and more people are really thinking about cyber security and then how that pertains to them as a provider. Lots of – I've notice heaps of those questions come through so thank you everybody for those. And a quick reminder. It's the light blue – sorry, dark blue hand icon If you want to get more questions in to the panel.

Here's another question for Katrina. Tell us a little bit about good practice in terms of expectations around board skills development.

KATRINA BROADBENT:

Yep. So, this is a good question. Firstly, it's really important that you start off with the right group of people on the board. So, a good mix of skills and experience that are matched with the organisation's objectives and strategic goals. So not just anyone, not just people with board experience. Board members really need to have a really solid understanding of everything that you do. Not just observing from afar. So, the board members should be aware of the additional legislative compliance, quality and safeguard regulations of the NDIS and have a really firm understanding of what it means. Board members receive an induction to the organisation like any other staff member, and their role and legal responsibilities, including conflict of interest, is defined and very clear. Also, an identification of potential skills gap or learning needs of each of the board members. So, has the board undertaken an analysis of skills they require under the NDIS? And how is the organisation going to go in filling these gaps?

DANIEL KIM:

Great, Thank you. Here's another question for Catherine. How does stride support the implementation of Privacy and Information Management requirements?

CATHERINE SCOTT-RICHARDSON:

Thanks Daniel. So, in collaboration between service delivery teams and our I.T. Department, Stride has some pretty comprehensive processes to ensure, not only I.T. continuity, information management and security, appropriate network access and security, and the appropriate use of I.T. resources. So, our I.T. Department does regularly review our information management requirements, against both Australian and International standards, to ensure that we're complying and improving on opportunities to strengthen our information management systems. Training is also super important and delivered to staff around consent and release of information to ensure again, that compliance piece against privacy legislation and standards.

DANIEL KIM:

Great, Thank you very much. Here's another question for Mae coming through. What actions can service providers take if a participant is not willing or not able to sign a service agreement?

MAE TANNER:

Thanks Daniel, and this one really goes back to consent. And if we think back to our scenario about Jerome and Penelope when she was collecting Jerome's consent to provide information.

DANIEL KIM:

Oh yes, good old Jerome and Penelope.

MAE TANNER:

And so, remember that Penelope needed to cover off on a few things. So, she needed to make sure importantly for this, that she provided him with a privacy statement. So, when she's collecting Jerome's information, she needs to explain what she's going to do with that information and a number of other things. And because she's collecting sensitive and health information, she needs to get his consent. And that's what we're coming back to when we're talking about a service agreement - providing these services in the context of Privacy Law. Penelope can't actually collect the information unless she has Jerome's consent. So, a lot of the questions are a bit broad, but if Jerome's not willing to sign a service agreement, then he's not giving his consent, and Penelope can't collect his information or then provide him with a service. So it's really important that Penelope explains all of this to Jerome and takes the time to make him understand what his information's going to be used for, why, and also perhaps the ways that it's going to be protected so that he gets some sort of assurance.

DANIEL KIM:

I mean, sometimes it's so much about communication, isn't it? That's the core part (indistinct).

MAE TANNER:

Absolutely. Yeah, and remembering that all this is about your client's dignity, and it should be very client focused and as others have mentioned as well, making sure that your clients are sort of dictating the terms of how their personal information is going to be used to a degree.

DANIEL KIM:

I love that, I mean people think about the practice standards and the registration requirements is like another thing to do, but the real goal is to enhance the quality of life for the participants.

MAE TANNER:

Absolutely.

DANIEL KIM:

A question coming through for Katrina here again. What are the expectations of NDIS workers documenting service provision, complaints and incidents?

KATRINA BROADBENT:

So, I guess the number one rule with auditors is we want to see documentation of everything. You can talk about, about how things have happened and how you've managed them but unless you actually have written evidence to show us, we can't take it into account. So, all complaints and incidents are required to be documented.

So more than that, alongside an incident report, there should be an Incident and Complaints Log that feeds into some sort of Continuous Improvement Log. So again, referring back to that triangle diagram I showed at the start, where policies align to practice. Also keep in mind that there's requirements under the NDIS to report complaints and incidents to the Commission.

So one thing we will ask as auditors, when it comes to staff interviews, will be around ascertaining whether your staff have an understanding of how complaints and incidents are reported within your organisation but also making sure they're aware of how participants and staff complaints can be lodged. And also, that understanding of the requirements when it comes to reporting incidents to the Commission.

DANIEL KIM:

Yes, that old triangle diagram. Thank you, Katrina. I'm a sucker for diagrams and models and frameworks. This kind of stuff gets me. Here's a question coming through for Catherine. In your presentation, you mentioned that you are introducing a new CRM, what criteria are you using when deciding on a CRM?

CATHERINE SCOTT-RICHARDSON:

Okay, so there's a number of following criteria that will apply. It needs to be versatile. So, we need to be able to integrate various operational functions. So, for example, the consumer record keeping piece, tracking NDIS performance and plan utilisation, needs to have capacity for NDIS billing, administering and tracking surveys, and also inclusive of outcome measures, which is the piece around the quality improvement for the consumer or participants.

It needs to be secure. So, this takes into account both external securities, so keeping the information secure from external threats and risks, and internally as well, so ensuring that only relevant staff have access to the information that they need in order to deliver care. Very importantly is that it's user friendly so that the workforce can access it and make the best use of it. That it's flexible so we can run it on various hardware platforms. We have a very mobile workforce who aren't always behind a desktop computer. So, it also needs to be able to be accessed and used meaningfully on both phones and tablets. And that the system is able to give us back some analytics to able to give the workforce and data driven insights to improve outcomes for the participants.

DANIEL KIM:

Great. Thank you, Catherine. Here's a question coming through for Mae. What do service providers need to consider when seeking participant consent for recorded images, video and sound? It's probably a follow up to the last one you answered.

MAE TANNER:

Yes, Thanks Daniel. I can see consent's been a hot issue in the questions, the live questions as well. So, I might just take a bit of time to explain a few things about the legal requirements for consent.

So, consent has to be informed, voluntary and specific. So those three things mean that you need to go back again to that privacy statement that I mentioned and really be thinking about - okay, when we're collecting this information, and remember that videos and photos are personal information too, are we explaining to the person what we might be using those for, and are we really getting proper consent?

So, it needs to be informed, voluntary and specific. And the person giving the consent must have capacity. And I think capacity is a really, really important issue when it comes to disability and mental health, making sure that the person you're dealing with, at the time that you're dealing with them, does genuinely have capacity to provide consent. So, set out exactly what you're going to use the information for.

Make sure that you've met these four requirements for consent. Getting expressed consent is always best. As Katrina said, the best way to get consent is written consent but that's not always possible. And especially when more and more of us are working remotely and we might not be face to face with the person. So, if you can't get written consent from someone, that's okay. As Katrina said once again as well, make sure that it's documented. So, you need to have this Privacy Statement document - what have you said to this participant about what you're going to do with the video or photo or other piece of information. Make sure that the Privacy Statement’s documented and make sure that you write down that you really have got the person's consent.

And remember, once again that if they don't want to give you their consent, then you're actually not able to collect the photo or video or whatever it is in the first place. So, it's really important to make sure that you cover off on all of that.

DANIEL KIM:

Great, Thank you. We are going through so many questions today. This is exciting. A question for Katrina, how do service providers evidence compliance with the privacy and dignity module?

KATRINA BROADBENT:

So, I think this follows on a lot from what Mae has already spoken about. But just really clear policies and procedures on participant privacy, but not just in collection of information but in-service delivery as well. So when it comes to consent, again, as Mae has highlighted, what we've found particularly now that we're doing a lot of remote audits with COVID, where written consent cannot be stored or whether you haven't received it from participants because you're no longer doing that face to face service delivery - having a note in your CRM system about the consent procedure that you've gone through with the participant and then ensuring that that consent is actually documented, and there is enough for you to be able to prove that there is in fact consent.

One important thing that we find a lot of providers miss, is ensuring that information is provided to participants around withdrawing consent and also changing their consent. So, providing a Consent Policy at the beginning of service delivery and having them agree to that is not enough. They really need to understand over the course of their - supports that they're receiving - how can they change that consent if they really want to?

DANIEL KIM:

Great. Thank you very much for that. There's a question that came through while your presentation was on as well, and I can answer this one, so I'll do it. It was a question from Sheridan. She wrote, there is so much great info here, but it is going very quickly.

Will there be a transcript available? So that's directly part of your presentation Katrina. And the answer Sheridan is yes, the transcript will be available. I'll take you through the details of that at the end of Q&A, which we are fast approaching.

We've got a question here - where did we get up to? For Catherine, how does Stride approach conflict of interest? I might just preface that by saying it might be the last question we take for today.

CATHERINE SCOTT-RICHARDSON:

Staff are required to declare and manage any perceived or real conflicts of interest. And we do this through our People and Culture Department where we actually have a specific Conflict of Interest Disclosure Template.

We also have a service delivery operation designed in a way to ensure that there's an appropriate separation between teams that may have a conflict of interest, and where they might need to be management of dual roles. For example, NDIS core supports and support coordination teams are typically managed separately, to ensure that information is only shared in accordance with privacy and consent requirements. And that NDIS support coordination involves ensuring that where Stride may be offered as an NDIS core supports option, that additional service providers are also offered to participants under choice and control.

DANIEL KIM:

Great. Thank you very much for that Catherine. So, in the interest of time, as the MC, I will call the Q&A to a close here. We did have a few other questions that did come through and we'll probably get the MHCC to respond to you directly offline, through a Post Webinar Information Pack. And those questions were the ones about whether organisations should priorities Commonwealth Laws or State Laws, and about what to do if a person doesn't have capacity for consent. But that does bring us to the end of the program for today. And that's also the second last slide for today, where we now naturally, want you to rate your overall knowledge, having watched this webinar.

So, a poll will pop up on your screen. Please let us know how you would rate your knowledge now from low to expert. And Let's have a quick look at the results that are coming through. For the first poll we had 56 percent of the people were saying they were at the second stage building. About 20 percent on sound, 10 percent on advanced and very small on the other either end of the spectrum, low and expert.

And if I go to the ones that are coming through now, nobody is now on low. So, everybody who had rated themselves lowest, they've all moved up. The bulk of the responses are coming through at the sound level, the number three. And it's moving from two to three. We've got more advanced people than before and got more experts than before. So, I think we can provisionally call this a very informative webinar. And that means Katrina Broadbent, Mae Tanner, Catherine Scott-Richardson, thank you very much for your insights today.

MAE TANNER:

Thanks very much Daniel.

CATHERINE SCOTT-RICHARDSON:

Thanks Daniel.

DANIEL KIM:

And moving to the final slide, of course, we want you to visit the Embracing Change Project Web page. And you can do that by selecting the project's tab under the Our Work section on the MHCC's front page. Here is the answer to Sheridan's questions before. You'll be able to access resources for each webinar, including archived recordings, transcripts, slide packs and resource packs. And I think I saw a question from Tommy as well. So that's where you can go to get all of those.

We will be breaking for the festive period and we'll be returning in February. So do enjoy your break, if you do have one, and keep an eye out for an invitation to register for the next webinar, which is on Quality Management and Improvement. A couple of final reminders make sure you download the resource pack, under the light blue hand icon - not the hand icon, but it's the light blue icon at the top. And please help us with our formal evaluation of the project by completing a quick survey, to which you will now be automatically redirected. Thank you once again for joining us. Remember to be kind to yourself and to others over the holiday period. Stay safe and we'll catch you on the other side of the New Year.

ENDS.