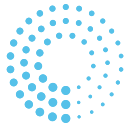




HIMSS™

***Next stop, the cloud:
connected health
on the brink of a new
age in Asia-Pacific***

Seven key takeaways from a HIMSS
APAC virtual government roundtable



HIMSS™



Overview

The future of connected health in the Asia-Pacific (APAC) region is bright. As countries in the region emerge from the Covid-19 pandemic, they are now starting to assess the lessons learned during their response and build on the value their experiences can bring to their digital transformation journeys.

The acceleration of telehealth implementation to meet the needs of a public health crisis on such an unprecedented scale was a huge achievement. It also suggested a way forward in the building of connected health systems that truly embrace the benefits of interoperability in secure environments and enable value-based care delivery.

Many of them are now looking at how they can extend the role of cloud computing to support the next phase of transformation. While some countries have already made a degree of transition to public and hybrid cloud models for EMR systems or individual services, this is still relatively uncharted territory in healthcare.

In collaboration with Amazon Web Services (AWS), HIMSS held a virtual roundtable on 19 October 2022 to examine how cloud computing can help APAC countries drive digital transformation, to understand the challenges that might potentially slow progress, and to discuss how those challenges could be overcome by considering models being pioneered in the United States (U.S.) and some European nations.

The discussion was attended by representatives from governments and regional health authorities from a number of APAC countries. As the roundtable was held under the Chatham House Rule, only the moderators have been identified.

Moderators:



Tom Leary,
Senior Vice President &
Head of Government
Relations, HIMSS



Jeff Coughlin,
Senior Director,
Government Relations,
HIMSS



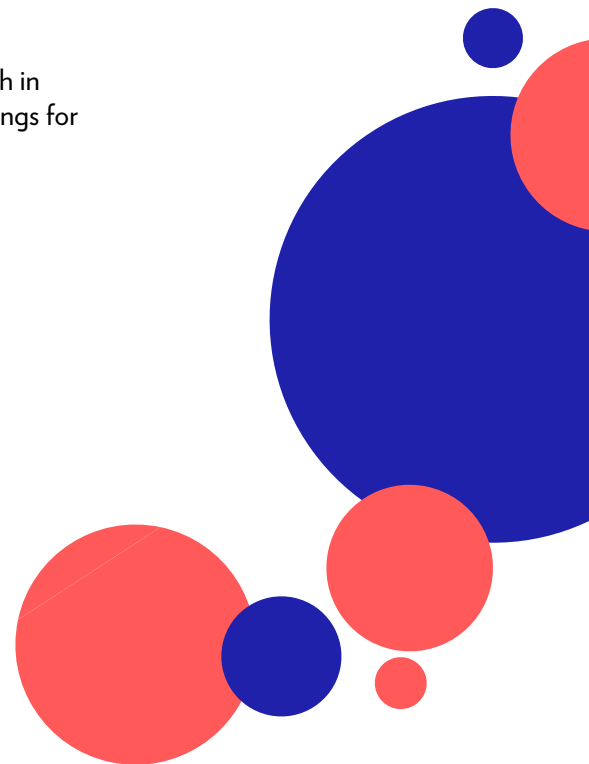
Andrew Wiltshire,
Head of Healthcare
Public Policy,
APJ, AWS

The Covid-19 pandemic revealed the potential for cloud computing and technologies to enable and enhance connected health systems. But it also highlighted the barriers, concerns, and weaknesses that can hinder adoption and innovation.

Jeff Coughlin, Senior Director, Government Relations, HIMSS, started the discussion with an overview of how the pandemic has driven change in the U.S. and the efforts that are now being made to capitalise on this progress of telehealth transformation, which he described as “one of the only silver linings” of the crisis. He said that this success has prompted the U.S. government to accelerate telehealth use across the health system, and some states have already extended their telehealth policies to continue beyond the public health emergency.

Coughlin explained how HIMSS has consolidated its connected health vision around five key policy recommendations, each of which is dependent on cloud adoption across health systems:

- 1** To position cloud technologies to continue to support policy development in interoperability, connected health, data privacy and security, and value-based care;
- 2** To ensure patients have access to telehealth services for standard clinical encounters – and advance secure, value-based, patient-centred care;
- 3** To prioritise the appropriate use of remote patient monitoring technologies – something that will require a robust cloud environment;
- 4** To invest in broadband infrastructure and connectivity projects (in the U.S. the Biden administration has committed \$65 billion for broadband expansion with a particular focus on underserved populations); and
- 5** To share success stories about cloud technologies and connected health in different populations and markets – and to generate insights and learnings for different use cases and care delivery models.





Key takeaway 1:

Covid-19 triggered a rapid acceleration in the digital transformation of healthcare across APAC. It also exposed gaps in health systems, particularly around the lack of interoperability and the proliferation of data silos. The good news is that it showed how cloud-powered connected health could change the landscape for the better and enable rapid innovation.



Andrew Wiltshire, Head of Healthcare Public Policy, APJ, AWS, said that the pandemic had vividly illustrated some of the gaps in health systems across the region: a lack of integrated data systems; the inability to see where resources were or how the pandemic was unfolding within different systems; the disconnection of patient records and the challenge of quickly pulling together diagnostic and patient management tools; the lack of preparation for telehealth and remote care – in both infrastructure and patient systems; the inequities in access to healthcare for some populations in remote and rural areas; and a broader lack of understanding around the role played by data in health systems.

There were, however, many highlights. “We did see how contact tracing could scale massively in weeks,” said Wiltshire. “How sector-wide data interoperability solutions could be deployed quickly, how actionable insights into populations with low immunisation rates could be derived, how a public vaccination system could scale up to hundreds of bookings per second and tens of thousands of vaccination events per hour.”

“We saw how telehealth and remote care at scale could be a trusted delivery channel and close geographic inequities – and examples of scale-ups in multiple ways: the CoWIN vaccination system in India, the Doctor Anywhere telehealth service in Singapore, and government-funded initiatives like [Healthdirect](#) in Australia, which provides information and advice at scale. Much of this was powered by the cloud.”

Wiltshire referenced [research](#) carried out by the AWS Institute in collaboration with Access Health International, looking at what needs to happen to accelerate the adoption and use of cloud across the region.

“There are benefits at every level of the healthcare system. Cloud offers a lot more than data storage and connectivity. It brings things like AI and ML to researchers, big data analytics for public health, it allows you to spin up a digital front door and virtual call centres very quickly, to introduce natural language processing, to bring video and voice capabilities to telehealth systems.”

The research identified a number of significant barriers to cloud adoption, particularly in relation to data security and privacy concerns, and resistance to change among health system managers and clinicians. Many of these concerns are exacerbated by a lack of clarity around cloud regulations in relation to personal data protection and a general shortage of cloud skills, which might explain the lukewarm sentiment for cloud services in some institutions and systems. For Wiltshire, these obstacles are inextricably linked.

“It’s really important that instead of trying to retro-fit digital in terms of each aspect of a healthcare system and each new initiative, there’s a core national digital health strategy that encompasses a whole range of aspects.”

“We need to make change easy and make sure the cloud is bringing benefits to clinicians,” said Wiltshire. “One of the key challenges in the region is the need for greater clarity in cloud regulations – which is essential to give confidence to healthcare institutions, providers, and patients to use digital and cloud-based solutions.”

Part of the solution is to invest in training and skilling up in IT in general and cloud technologies in particular – something that healthcare institutions have fallen behind with. AWS, for example, has compiled a library of more than 500 free courses, interactive training labs and day-long courses, and is committed to training 29 million people globally by 2025.

Access Health International has provided a number of recommendations to help countries to drive cloud uptake by health systems in the APAC region:

- Adopt a cloud-first policy for healthcare, driven by a central digital health authority;
- Use a range of policy tools to realise the full potential of the cloud in the digitalisation of healthcare;
- Develop data governance policies and regulations that ensure healthcare data protection while enabling innovation for better health outcomes;
- Design policies to seed a digital health ecosystem and foster innovation, including government financing for start-ups, talent development, and retention strategies, and more inclusive procurement policies as well as the setting up of cloud pilot sites for reference;
- Build trust in cloud services through streamlining and standardising procurement;
- Assess and invest in creating a foundational ICT ecosystem that furthers cloud adoption; and
- Address capacity building as a priority to overcome key barriers to cloud adoption.

A man and a woman are in a server room. The man, wearing glasses and a light-colored shirt, is pointing with his right hand towards a rack of server cables. The woman, wearing a light-colored shirt, is looking at the cables. The man is also holding a tablet in his left hand. The server room has a blue tint and a perforated metal door in the background.

Key takeaway 2:

Early cloud adopters in the region's health systems are looking at how they can take their strategies to the next level, while other countries consider which type of cloud will meet the data security and privacy assurances required by current regulations. There are still a lot of misperceptions about how the cloud can provide a secure environment for digital health systems and applications.

Even those countries that have embraced a level of cloud in their connected health strategies now have to make choices about the type of cloud technology that is most appropriate for their purposes.

A participant from Singapore noted how cloud enabled the rapid development and rollout of solutions during Covid-19, which would otherwise have been impossible. “We are pushing forward quite quickly on telemonitoring – cloud has allowed us to make that widely deployed for a number of different diseases such as hypertension, psychosis, post-Acute Myocardial Infarction, and so on,” they said.

“Our architectures are split – we have anonymised data in the cloud and we still have the personalised dashboard information with personalised identifiers done on a hybrid private site. We do recognise that some of these things can be moved entirely to commercial cloud eventually, but at this time we are mainly in a hybrid environment.”

Andrew Wiltshire said there are a lot of misperceptions around commercial cloud services – that if you can’t see the server, your data won’t be as secure as it would be on your own. “The reality is that when you move into these cloud environments, you’ve got some of the most security-focused organisations in the world, whose one job is to make sure that their services are secure, that their tools bring all of the security and visibility that IT and system managers need to manage and secure their networks,” he said.

A participant from Australia explained how the development of a set of Whole-of-Government Agreements for the selection of cloud services has helped to create a procurement framework for healthcare entities and their affiliates to provide the assurances they need to move clinical applications to the cloud.

According to a participant from the Europe, Middle East, and Africa (EMEA) region, countries such as the United Kingdom (UK) and Israel have developed clear frameworks for the use of data in the commercial cloud. These are based on assessing the risk of that data moving to the cloud – and the risk of not moving it to the cloud. A clearly specified set of security controls can then be implemented. “In the UK, commercial cloud providers are encouraged to assess their services to show the extent to which they can meet those controls with their standard services or not,” they added.

“There’s a lot of transparency about what is required and what is possible with commercial cloud offerings, which I think makes it more straightforward for healthcare organisations to know where the risk sits and what the governance model they need to set up around that should look like.”



Key takeaway 3:

The experiences of some of the region's early cloud adopters have shone a light on the need for governments to give focused thought to the specific nature and requirements of digital health provision. The layers of complexity around the secure use and re-use of personal data are unique to the health sector – and this raises important questions about the choices to be made between cloud and on-premises infrastructure.

A participant from Australia explained some of the challenges that had to be overcome before moving My Health Record – containing four billion documents and three petabytes of data – to the public cloud. They said it was vital that Australia’s Digital Transformation Agency had set up a framework for procuring cloud services, as well as a security certification programme. When the migration programme started, not all providers were certified – and it would have been impossible for any single state agency to manage such a programme themselves.

The sensitivity of health data, which is governed by strict regulations in Australia, was another impediment. Considerable legal advice was needed to ensure that all the requirements are met – including, for example, how to protect the data.

“These are considerations you would probably all have when you think about moving towards services where a lot of the management is done off-shore, where there is the ability to swing the data off to other nodes or jurisdictions,” they said.

“The hosting arrangements need to be architected accordingly... and there are long-term considerations. Is it really cost-effective to host these amounts of data in the public cloud? We don’t have an answer yet, but personally, I think a long-term model is probably going to be a hybrid.”

“The rule of thumb is that you need to have a true data centre,” said a participant from the region. “We are migrating most of our health applications to the hybrid cloud in the next five years. We also offer data services to universities.”

“The cloud development environment has enabled us to respond very quickly to our Covid-19 policies – for example, quarantine requirements – virtually developing and delivering a system in a few days.”

Key takeaway 4:

There is a gulf between native cloud health system providers and some of their established EMR counterparts when it comes to flexibility and new business models. EMR vendors are in a transitional phase as they embrace the cloud, and many of them are now moving ahead with hybrid systems. But the pace is being set by native cloud vendors as they continue to disrupt the landscape and drive the connected health conversation.



One Australian participant noted that it is common to find large-scale EMR vendors putting up barriers to cloud implementation, and questioned their commitment to new business models.

Another replied that some of these vendors are migrating their workloads to AWS, and that this modernisation is driving their architecture to include better resiliency, and improved operational costs and performance.

“It’s taking time,” they said. “We are seeing these big EMR, medical imaging, and clinical informatics system vendors thinking about their business models. How do you switch up your business model, how do you move away from these large, perpetual licence software and support agreements to a more SaaS-based business model?”

“Native cloud providers are progressing swiftly with SaaS, whereas larger organisations are going through that transformation activity. From my personal view, it’s going to be a few years before you see significantly large players do a complete transformation. At the moment, they’re working on a hybrid basis.”



Key takeaway 5:

The pandemic showed the growing value of genomic data to every aspect of healthcare delivery. An exponential increase in the volume of data that will need to be managed, stored, and made accessible for rapid research requires will require secure processes, environments, and controls. Projects around the world are showing how cloud computing is enabling effective new models that democratise access to health data.

One participant raised the challenges around the growing value of genomics data in healthcare, suggesting that it is very difficult – if not impossible – to de-identify data on such a scale while understanding the emerging standards and policies around personal data and privacy.

A participant from EMEA said that the cloud is particularly helpful in ensuring the security of genomics data while democratising and accelerating access to it and helping to accelerate global knowledge. The organisation owning and responsible for the data controls the environment in which it is shared.

“They can grant secure access to researchers from around the world whether by a set of access criteria or on a case-by-case basis,” they explained. “They can then attach an analytics environment to that data environment. A researcher can only use tools approved by the responsible organisation, and can do analysis and take away insights, but they can’t leave with the data. In some cases, they can’t leave with the ML model they might have developed, but they can take away the insights they’ve generated in creating it.”

[Genomics England](#) has provided a good example of how effective this model can be. When it moved all its Covid-19 data – some 100,000 genomics records – to the cloud, it generated some cost savings. But most importantly, it rapidly identified genetic markers that indicated whether an individual was likely to suffer from severe or mild symptoms after being infected.

“I think that’s a real step change that we’ve seen from ten or fifteen years ago, when maybe we’d have been sending physical copies of the data around the work, and when it left your hands to some extent you relinquished some security and control of that data. You have full auditability in the cloud, so you can check who’s accessed what, and what they’ve done with it.”

A photograph of a doctor in a white coat and face mask examining an elderly woman in a rural setting. The doctor is kneeling and using a stethoscope on the woman's chest. The woman is sitting on a wooden bench. The background shows a rustic structure with woven walls. The entire image has a blue tint.

Key takeaway 6:

From longitudinal data repositories to the role of start-ups and local health initiatives to counter inequities in access to services, no aspect of healthcare is untouched by the cloud's potential to enable change. APAC countries can turn the challenges of connectivity and data sharing into opportunities for transformation.

The growing number of large longitudinal data repositories for health and disease progression prompted a participant from Singapore to ask that if they are to be used for policy research and even point of care, how will that be enabled to happen?

“There’s a comprehensive repository in the U.S. with over 150 million very comprehensive longitudinal records that people can do wonderful things with,” they said. “We’re deprived of that in Asia. We have much less research being carried out on the Asian phenotype, and China could crack this problem – but we’re not holding our breath for a major sharing from there. And there would be phenotypical differences due to living conditions, air pollution, and so on.”

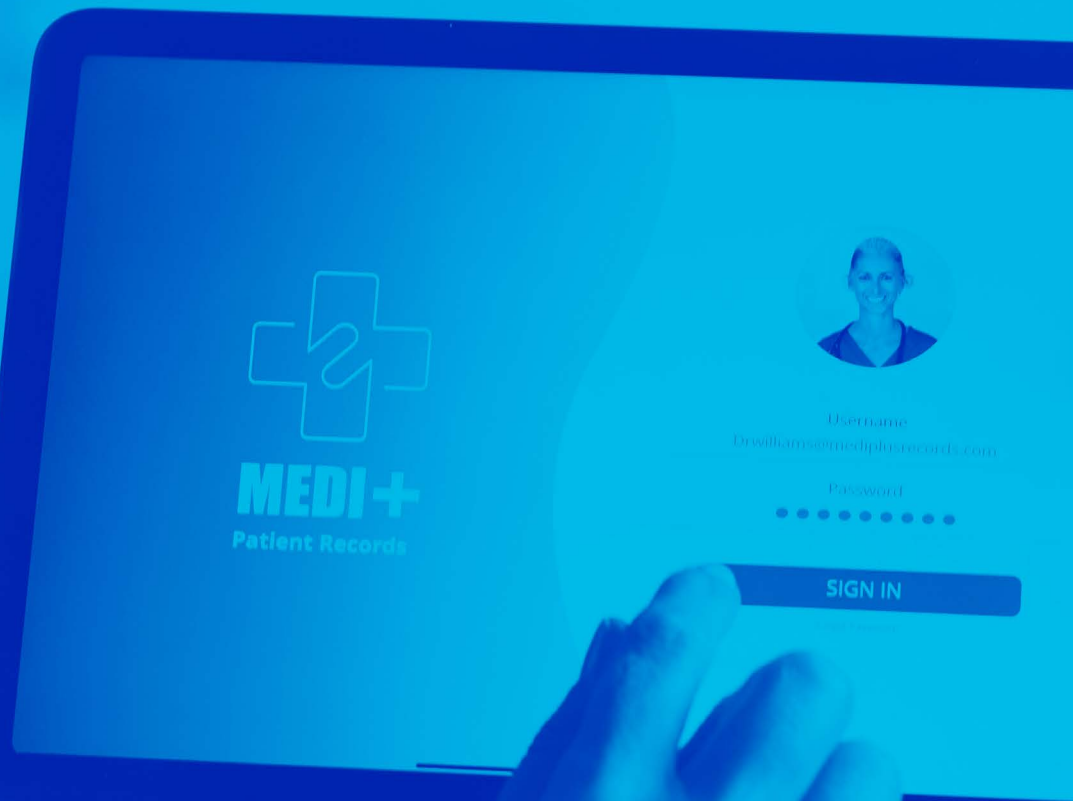
“We’re very interested in seeing how to crack that problem for Asia. We have a good repository in Singapore, with three million records. But it’s not enough. Creative juices are needed to solve this problem, and of course, that doesn’t need to happen in Asia.”

The role of start-ups was raised by a participant from Pakistan, who noted that the lack of availability of off-the-shelf tools and regulations about the use of public data had slowed development at a time when the speed of response to Covid-19 was so important. How can we get them into health ecosystems?

Andrew Wiltshire said this need has certainly been realised on the ground, and it was important to look for credits and start-up initiatives from cloud providers. For example, AWS’s healthcare accelerators help startups get the support they need to take their concepts to the next phase using the power of the cloud. In 2022, it launched three healthcare accelerators focused on [reducing health inequities](#), [aged care and digital health](#), and the [healthcare workforce](#).

The EMEA participant said there are different options for providing access to cloud infrastructure in countries where there might not already be a collection of data centres – outposts, means of placing infrastructure locally but connect it to the cloud, and bringing providers such as AWS into a local data centre.

They also spoke about a recent project in Lesotho and Tanzania – Vodafone Foundation’s [m-mama](#) programme – which received support from AWS’s Health Equity Initiative as an example of a cloud project that improves access to healthcare and reduces inequity. Here, a solution was developed to connect pregnant women and newborn infants and their mothers with emergency transport options when they require life-saving care but are too rural to access the regular ambulance service. The project has so far helped 13,00 patients and led to a double-digit reduction in mortality.



Key takeaway 7:

The experiences of some of the region's early cloud adopters have shone a light on the need for governments to give focused thought to the specific nature and requirements of digital health provision. The layers of complexity around the secure use and re-use of personal data are unique to the health sector – and this raises important questions about the choices to be made between cloud and on-premises infrastructure.

There are a number of data governance models that APAC countries can look to for guidance in developing their own to take advantage of cloud technologies. As the EMEA participant said, there are probably as many models as there are different health systems around the world. They reference the UK and Israel as significant examples.

In the UK's distributed governance model, it is the responsibility of each individual health organisation that controls the data to assess the risks of using and not using data in the cloud. "They have a very detailed tool that data controllers use to assess what they want to do with the data for how long, and what type of data it is," they explained.

"The tool generates a risk score – it's a very clear set of controls and responsibilities. The NHS Digital Data Security and Protection toolkit enables cloud providers to assess themselves against the required criteria."

The Israeli model has a series of risk controls for different types of data, and a clear risk classification system. Governance is split. If the risk goes above a certain threshold, the Ministry of Health reviews the request and assesses where it is content for usage to go ahead. Otherwise, it remains the responsibility of the board of the health organisation.

With such models available as evidence for how effectively and securely health data can be managed in the cloud, it is time for governments to take a holistic look at how the cloud can be used to enable the connected health systems that will drive value-based care in the coming years. Andrew Wiltshire concluded the roundtable with a simple call to arms for all participants.

"Governments have the opportunity to provide clearer guidance for healthcare institutions on how they can compliantly and confidently use cloud services."