



Overcoming  
Barriers to  
**Cloud Adoption**  
**in Public Healthcare**  
in Asia Pacific

# AWS INSTITUTE

---

## **AWS Institute**

The AWS Institute is a thought leadership and executive education program to accelerate digital transformation for public sector executives.



## **ACCESS Health International**

ACCESS Health International is an advisory company and implementation partner that focuses on improving health innovation and ensuring that all people have a right to access high quality and affordable healthcare. ACCESS Health provides professional consulting and resource matching services to both public and private sector players. ACCESS Health has made a significant impact in the health and aging industry by fostering health innovations through unique partnerships among entrepreneurs, policymakers, corporations, and investors.

# Table of Contents

1. Executive Summary .....	2
2. Introduction to the Cloud .....	5
3. Key Research Findings on Cloud Adoption for Public Healthcare in 12 Asia Pacific Countries .....	6
3.1 Cloud for Public Healthcare – a Readiness Framework .....	7
3.2 Readiness of High-Income Asia-Pacific Countries: Key Findings .....	10
3.3 Interview Insights: Drivers and Benefits of Cloud Adoption .....	14
3.4 Interview Insights: Barriers to Adoption of Cloud for Public Healthcare .....	16
4. Recommendations .....	29
5. How Can Public Healthcare Benefit from the Cloud? .....	38
5.1 Cloud Drives Health System Transformation Through Data-Powered Solutions .....	38
5.2 Healthcare Organizations Benefit from Leaner, More Strategic Operations to Offer High-Quality Patient-Centered Care .....	40
5.3 Patients Receive More Accessible, Personalized, High-Quality Care .....	42
6. Acknowledgements .....	44
7. Endnotes .....	45

# 1. Executive Summary

The cloud has often been called a game-changer for digital health, but its true benefits have only come to the fore since the onset of the COVID-19 pandemic.

In Asia Pacific, as in other parts of the world, the pandemic requires an immensely coordinated and timely response from governments and society at large to protect public health and the economy. The cloud, specifically hyperscale cloud, with its highly scalable data storage and computing capabilities, has played an instrumental role in the response and in helping develop national health systems' resilience to the pandemic. From contact tracing to population disease surveillance, cloud services have helped healthcare ministries and public and private health systems rapidly set up informational technology (IT) infrastructure and deploy applications that can scale up and down with the number of COVID-19 cases. Cloud-powered telehealth services have taken critical healthcare services to densely packed cities as well as underserved rural areas.

Governments are using the cloud to stay on top of COVID-19 case data – with the collection, monitoring, and exchange of data at local, national, and global levels driving crucial policy decisions. Moreover, the rapid rollout of COVID-19 vaccines would not have been possible without cloud infrastructure supporting vaccine development, manufacturing, and distribution.<sup>1,2,3</sup>

However, COVID-19 is only one of the many public healthcare challenges that the Asia-Pacific is facing. A large and rapidly growing aging population, rising healthcare costs, an increasing chronic disease burden, and a shortage of healthcare personnel are putting pressure on national health systems. Digital healthcare has been widely recognized as an important tool in health systems – throughout the Asia-Pacific region, most governments have put forward national digital health strategies to guide health system practitioners into digital adoption. However, few digital health strategies have fully outlined the guidelines and mechanisms for cloud adoption.

Given the cloud's important role in strengthening health systems, ACCESS Health, in collaboration with AWS Institute, carried out a study to better understand the enablers and barriers to cloud adoption in public healthcare in the Asia-Pacific, and how these challenges can be overcome. We examined the extent and patterns of cloud adoption in 12 Asia-Pacific countries: Singapore, Australia, New Zealand, South Korea, Japan, Malaysia, Thailand, Indonesia, Vietnam, Philippines, India, and Bangladesh. We analyzed each country's digital healthcare landscape – digital health policies, systems, solutions, and notably the policies applicable to and uses of cloud technologies and services in health systems. We interviewed nearly 40 policymakers, healthcare Chief Information Officers (CIOs)/Chief Medical Informatics Officers (CMIOs), and digital health experts in these countries to understand their perspectives on cloud adoption for public healthcare.



## Methodology

We began our analysis by identifying and studying the key factors that enable the adoption of the cloud for public healthcare. The Asia Cloud Computing Association (ACCA) lists the following four factors as being critical enablers of a country's cloud readiness: infrastructure, security, regulation, and governance. Based on our research, we identified four additional factors that are important enablers for the use of cloud in public healthcare: national policies and mandates for digital health, cybersecurity, and privacy policies specific to healthcare data, the nature and maturity of the health system, and the maturity of its digital health system.

To further calibrate our findings, we classified the 12 countries into three groups based on their income as we observed that countries' adoption of Information and Communications Technology (ICT) was closely linked to their GDP.

- **High-income:** Singapore, Australia, New Zealand, South Korea, Japan.
- **Upper-middle-income:** Malaysia, Thailand.
- **Lower-middle-income:** Indonesia, Vietnam, Philippines, India, and Bangladesh.



## Findings

On further analyzing these countries based on the readiness factors identified, we found readiness and adoption were largely linked to the country's income group. We found that within the high-income group, Singapore, Australia, New Zealand, and South Korea are the most advanced in their readiness and adoption of cloud for healthcare. In the second group, Thailand has seen wider adoption than Malaysia. However, the latter is more forward-looking in terms of policies, having adopted a Cloud First Policy for the public sector. In the lower-middle-income group, India and Vietnam have seen greater adoption of cloud than their peers.

Cloud services benefit public healthcare systems at three levels: at the health system level as a whole, at the healthcare organization level, and at the individual patient level. To fully realize the potential for cloud services to benefit health systems, and the opportunities to unleash further innovation in the healthcare industry through successful cloud adoption, we outline four strategies for national policymakers and health system practitioners to consider:

### R1. Countries should adopt a Cloud First Policy for healthcare driven by a central digital health authority.

A Cloud First Policy for healthcare directs government health agencies to consider using cloud-based technology solutions ahead of other IT solutions. This will allow public healthcare organizations to optimize infrastructure cost and access scalable IT resources while building a connected healthcare ecosystem. A well-crafted Cloud First policy leads to cost savings, greater security, and flexibility in adjusting IT usage.

### R2. Use a range of policy tools to realize the full potential of the cloud in the digitalization of healthcare.

The right policy tools, built around critical enablers such as interoperability, regulations, and procurement, can help overcome organizational resistance to digitalization and enable quicker and wider adoption of the cloud.

**R2.1. Develop data governance policies and regulations that support healthcare innovation for better health outcomes.** Data privacy and protection policies and regulations are a key building block of digital health. Clear data governance policies and principle-based regulatory frameworks must be built that ensure risk-appropriate governance based on internationally recognized standards.

**R2.2. Establish open standards for data interoperability and data exchange for a patient-centered connected healthcare system.** The establishment of standards and mandating interoperability can enable the collection and use of healthcare data to its full potential.

**R2.3. Design policies to seed a digital health innovation ecosystem.** Many governments, particularly in Group 2 and Group 3 countries, use conventional financing models to provide funding to startups instead of venture capital-based structures. For digital health systems to mature, governments will need to create a strong innovation ecosystem supported by policies and incentives, including procurement policies that are startup-friendly, and a better support system for startups.

**R2.4. Build trust in the cloud by streamlining and standardizing procurement.** Guidance on procurement along with the establishment of minimum service standards for cloud service providers (CSPs) can help organizations adopt cloud with greater confidence. Such policies will also help to mitigate concerns around cloud data governance, vendor-concentration risks, and business continuity.

### R3. Assess and invest in creating a foundational ICT ecosystem that furthers cloud adoption.

All lower-middle-income countries cited the need for more adequate supporting ICT infrastructure. Governments must establish policies and create an investment plan that addresses the required physical ICT infrastructure as well as the human resources needed.

### R4. Address capacity building as a priority to overcome the key barriers to cloud adoption.

Educational programs and training are needed to close knowledge gaps and to design and build human-centred digital health applications. A designated body for capacity building such as a Centre of Cloud Excellence or equivalent must be empowered to drive such initiatives in partnership with the private sector and in line with international best practices.

Collectively, these strategies can help accelerate innovation in public healthcare by addressing seven key barriers that key stakeholders perceive are holding back cloud adoption. These were identified through our analysis of the enablers and detailed interviews with public healthcare decision makers and experts.

## KEY PERCEIVED BARRIERS TO CLOUD ADOPTION IN HEALTHCARE

### > Misperceptions around security and privacy of cloud-based data:

Respondents cited that due to a lack of awareness or understanding of the cloud, policymakers and/or healthcare organization management often held misperceptions around security and privacy of cloud-based data, which showed a gap in understanding the benefits and security capabilities of the cloud. The lack of personal data protection and healthcare regulations in some countries has also added to this perception.

### > Resistance to organizational change:

In the absence of mandates or incentives to drive digitalization, factors such as an insufficient understanding of cloud services' benefits, fears of revenue loss, and opposition to changes in clinical workflows have been cited by respondents as barriers for healthcare facilities considering cloud adoption.

### > Low clarity on cloud data governance regulations:

Complexity and ambiguity in data governance regulations, along with little to no training imparted to healthcare IT staff on the application of regulations to healthcare data, were cited as obstructing cloud adoption.

### > Inadequate infrastructure:

Respondents considered weak foundational ICT infrastructure, including inadequate internet bandwidth, poor hardware quality, and poor mobile connectivity in rural areas, as impacting cloud adoption, especially in Group 3 countries.

### > Budgetary constraints:

Respondents cited the cost of cloud migration in terms of planning, implementation, and the training of IT staff and clinicians as a major barrier for public healthcare organizations with already strained budgets.

### > Shortage of cloud skills:

Respondents in three out of 12 countries cited the shortage of cloud skills as among the top 3 barriers to cloud adoption, specifying that few professionals could understand both cloud technologies and their application to the healthcare sector.

### > Low awareness of cloud benefits:

Respondents in all countries perceived the understanding of cloud services, their use and range of benefits to be limited, impacting the uptake and adoption of cloud services across the health system.

## 2. Introduction to the Cloud

Cloud computing is the on-demand delivery of information technology services such as computing power, storage, and applications via the internet, based on a pay-as-you-go pricing model. Cloud is not a new form of technology but a new model for delivering computing resources. It offers significant benefits for the health sector because of these key advantages:

- the availability of scalable computing resources and the latest technology on-demand
- the ability to integrate data and provide real-time access to data across geographical boundaries that allow collaboration and interoperability
- no upfront commitment on hardware or its management, and
- the ability to pay only for what is used

### Types of cloud services:

There are three types of cloud services offered with the Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models being the most relevant for this report.

#### 1. Infrastructure as a Service (IaaS):

These services provide the basic building blocks for cloud IT.

#### 2. Platform as a Service (PaaS):

PaaS offers a platform for building, testing, and deploying applications and is mainly used by software developers and software companies.

#### 3. Software as a Service (SaaS):

This is a complete product that is run and managed by a service provider.

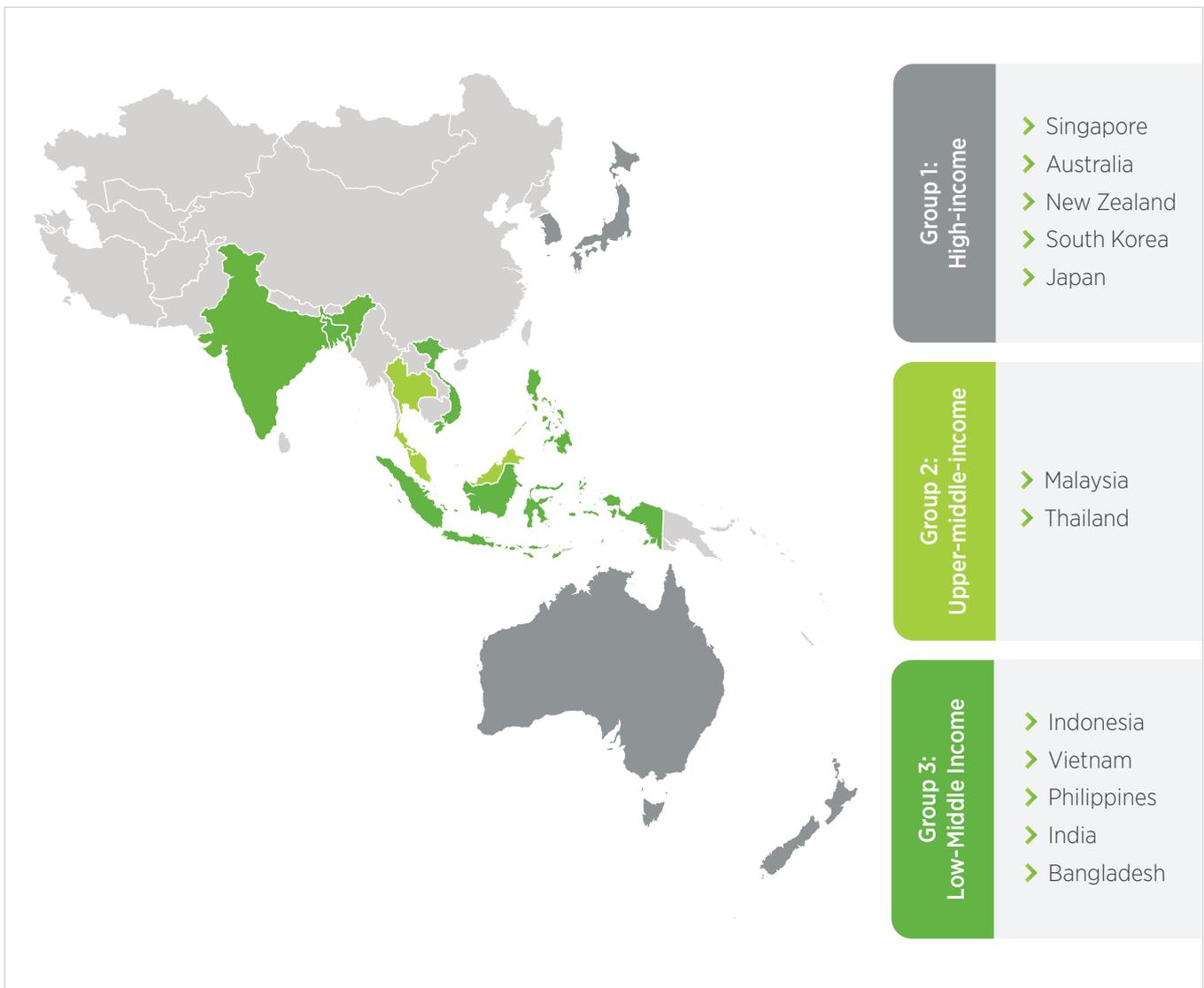
While cloud services can be deployed fully in the cloud (hyperscale), fully on-premises, or as a combination of both, governments, and national healthcare organizations such as the UK's NHS are increasingly adopting a Cloud First policy for the advantages listed above.<sup>45</sup>



# 3. Key Research Findings on Cloud Adoption for Public Healthcare in 12 Asia Pacific Countries

## Introduction

The following sections bring together our findings from primary and secondary research sources for 12 countries in Asia Pacific as listed below. Since countries' ICT spending is highly dependent on their GDP, we divided the countries into three groups based on their GDP to understand the variation of cloud adoption within and across groups.



The research was carried out through a review of existing literature and 40 interviews with policymakers, public and private hospital CIOs and CMIOs, health-IT experts, and advisors to governments on digital health in these 12 countries.

The following sections present key insights gathered from our research on the enablers of, drivers of, and barriers to cloud adoption.

### 3.1 Cloud for Public Healthcare – a Readiness Framework

National policies and mandates for digital health initiatives, healthcare data security and privacy regulations, the nature and maturity of the health system and the maturity of digital health initiatives are healthcare-specific factors that influence a country's readiness and adoption of cloud.

According to the Asia Cloud Computing Association (ACCA) that annually publishes the Cloud Readiness Index,<sup>6</sup> the following are the key enablers of a country to be cloud-readiness for a country:



Infrastructure

**International Connectivity:** International bandwidth is key to developing cloud services while also enabling domestic users to access international cloud services.

**Broadband Quality:** Average download speeds are indicative of fast and reliable access to the cloud.

**Power Grid, Green Policy and Sustainability:** Stable, continuous access to power, water, and sustainable energy enables the building and maintenance of data centers.



Security

**Data Center Risk:** This parameter assesses risks to data centers in a country including infrastructure, legal capabilities, the tax environment, and exposure to natural disasters.

**Cybersecurity:** This parameter assesses cybersecurity technologies, technical frameworks, standards, initiatives, ICT education and infrastructure for data in the cloud.



Regulation

**Business Sophistication:** Governments' facilitation of setting up businesses and supporting new players is important to developing the cloud industry.

**Freedom of Information:** The flow of data across borders is essential for unleashing the full potential of the cloud.



Governance

**Privacy:** The assurance that users' information is held securely and protected, the adherence to international data privacy standards and a central enforcing authority is key for cloud adoption.

**Government Regulatory Environment:** Strong regulatory frameworks that enable the use of cloud and e-governance technologies enable cloud adoption.

**Intellectual Property Protection:** Robust protection and enforcement of intellectual property rights are important for innovation, which is especially important for cloud as an emerging technology.

Over the following pages, we used the ACCA cloud readiness framework to derive a framework for the adoption of the cloud in public healthcare and identified the following additional readiness factors that are specific to healthcare. We also identified specific parameters for each factor and analyzed countries based on these parameters to understand their readiness for cloud adoption. The analysis uses both available quantitative data from secondary sources as well as our qualitative assessment based on primary and secondary research.

Each comparison table also shows how cloud is being used in public healthcare in each country.

Readiness Factors for Cloud Adoption in Healthcare	Parameters
<p><b>1</b> <b>Nature and maturity of the public health system:</b> Basic healthcare infrastructure, national schemes such as universal health coverage and national health insurance schemes help centralize public healthcare data and ease the way for cloud adoption.<sup>7</sup></p>	<ul style="list-style-type: none"> <li>• UHC Service Coverage Score</li> <li>• Nature of system</li> </ul>
<p><b>2</b> <b>National policies, mandates, or incentives for cloud-enabled digital health initiatives:</b> National mandates and incentives for digital health initiatives are needed to drive cloud adoption as our research has shown that the healthcare sector is more conservative than other public sectors in its adoption of digital technologies.<sup>8</sup></p>	<ul style="list-style-type: none"> <li>• Cloud First Policy</li> <li>• Cloud for Public Healthcare Mandate/Policy</li> </ul>
<p><b>3</b> <b>Sophistication and maturity of the digital health system:</b> Digital readiness of healthcare systems have a strong influence on the use of cloud technologies.</p>	<ul style="list-style-type: none"> <li>• Maturity of digital health initiatives*</li> </ul>
<p><b>4</b> <b>Data protection and privacy regulations for personal data, with separate provisions for healthcare data.</b> With healthcare data accounting for the largest share of publicly disclosed data breaches in 2020, it is not surprising that adequate regulations need to be in place to enable cloud adoption in the sector.<sup>9</sup></p>	<ul style="list-style-type: none"> <li>• Legislation on personal data protection</li> <li>• Data Protection &amp; Privacy Legislation for Healthcare Data</li> <li>• Data governance regulations for healthcare data in the cloud</li> </ul>



## Cloud Readiness Enablers for Public Healthcare

<b>National Policies and Mandates</b>	<b>Healthcare Data Security &amp; Privacy Regulations</b>
<ul style="list-style-type: none"> <li>• National Policy/Mandate for Adoption</li> <li>• Incentives for Digital Health Initiatives</li> </ul>	<ul style="list-style-type: none"> <li>• Data Security Regulations</li> <li>• Data Protection &amp; Privacy Regulations</li> </ul>
<b>Nature &amp; Maturity of Health System</b>	<b>Maturity of Digital Health System</b>
<ul style="list-style-type: none"> <li>• Basic Healthcare Infrastructure</li> <li>• Universal Health Coverage Scheme</li> <li>• National Health Insurance Schemes</li> </ul>	<ul style="list-style-type: none"> <li>• Digital Health Leadership</li> <li>• Digital readiness of healthcare systems</li> <li>• Digital Literacy of Healthcare Staff</li> </ul>



### Cloud Readiness Enablers for a Country [ACCA]

<b>Cloud Infrastructure</b>	<b>Cloud Security</b>
<ul style="list-style-type: none"> <li>• International Connectivity</li> <li>• Broadband Quality</li> <li>• Power Grid, Green Policy, and Sustainability</li> </ul>	<ul style="list-style-type: none"> <li>• Data Center Risk</li> <li>• Cybersecurity</li> </ul>
<b>Cloud Regulation</b>	<b>Cloud Governance</b>
<ul style="list-style-type: none"> <li>• Business Sophistication</li> <li>• Freedom of Information</li> </ul>	<ul style="list-style-type: none"> <li>• Privacy</li> <li>• Government Regulatory Environment</li> <li>• Intellectual Property Protection</li> </ul>

## 3.2 Readiness of High-Income Asia-Pacific Countries: Key Findings



The countries in this region vary greatly in their development, in their healthcare systems and the adoption of technology which together has led to varying rates of cloud adoption. The following are some key findings based on the comparison above and a detailed analysis of the 12 countries' digital health landscape, policies, cloud adoption, and corresponding legislation:

- Cloud readiness, the extent of cloud adoption, and its uses are greater in Group 1 (High-income) countries. These factors drop with a country's income group.
- Only six out of 12 countries have a Cloud First policy, with five having a cloud for healthcare mandate or policy.
- In Group 1, Japan lags behind its peers despite showing high readiness. A conservative mindset has led to resistance to newer digital technologies.
- In Group 2, Thailand is slightly ahead in terms of cloud adoption despite Malaysia showing more readiness.
- Most Group 3 countries show low readiness due to the absence of conducive policies, data privacy, and security legislation, and lower ACCA cloud readiness scores.
- The pandemic has been a key driver of cloud adoption, especially in Group 3 countries, with their largest cloud-enabled health initiatives being launched post-COVID-19.
- Vietnam is ahead of other Group 3 countries, except India, in cloud adoption despite the lack of enabling legislation due to its higher digital health maturity.
- India and the Philippines are ahead of their peers in enabling policy and legislation. However, India is making progress at a more rapid pace when compared to its peers, including the Philippines.



### 3.2.1 Cloud Adoption for Public Healthcare: Readiness of High-Income Asia-Pacific Countries

READINESS FACTORS	SINGAPORE	AUSTRALIA	NEW ZEALAND	SOUTH KOREA	JAPAN
<b>UHC Service Coverage Score (out of 100)</b>	86	87	87	86	83
<b>ACCA Cloud Readiness Index Rank (2020)</b>	81.5	71	77.1	72.7	71.3
<b>Cloud First Policy</b>	✓	✓	✓	✓	✓
<b>Cloud for Public Healthcare Mandate/ Policy</b>	✓	✓	✓	✓	✗
<b>Legislation on Personal Data Protection</b>	✓	✓	✓	✓	✓
<b>Data Protection &amp; Privacy Legislation for Healthcare Data</b>	✓	✓	✓	✓	✓
<b>Cloud: Data Privacy/ Security Legislation for Healthcare Data</b>	✓	✓	✓	✓	✓
<b>Nature of system</b>	Multi-payer program providing national health insurance.	Universal health coverage through Medicare.	Single-payer, tax-funded program providing universal health coverage.	National health insurance covers 97% of the population.	Universal health Insurance system.
<b>How is the cloud being used for healthcare?</b>	Singapore's public hospital network has fully adopted cloud with diagnostics & imaging not yet fully on cloud. Precision medicine is developing, and AI/ML applications are also in use.	Teleconsultations, research, public portals, health data storage, and precision medicine, are some areas of use.	Patient administration and management systems, clinical portals, laboratories, picture archiving and communication, radiology, pharmacy, eReferrals, and ICU systems.	EMRs, precision medicine, insurance services, research and data analysis.	Cloud is mainly being used for research and recently for managing COVID-19 vaccinations.

### 3.2.2 Cloud Adoption for Public Healthcare: Readiness of Upper-Middle-Income Asia-Pacific Countries

READINESS FACTORS	MALAYSIA	THAILAND
UHC Service Coverage Score (out of 100)	73	80
ACCA Cloud Readiness Index (2020)	68.5	60.2
Cloud First Policy		
Cloud for Public Healthcare Mandate/Policy		
Legislation on Personal Data Protection		
Data Protection & Privacy Legislation for Healthcare		
Cloud: Data Privacy/ Security Legislation for Healthcare Data		
Nature of system	Universal health coverage through the National Health Insurance scheme.	Universal health coverage through social health insurance.
How is the cloud being used for healthcare?	Diagnosis & imaging, supporting national health data warehouse MyHDW.	Telehealth, Patient administration, patient access, office productivity solutions, CRM.

### 3.2.3 Cloud Adoption for Public Healthcare: Readiness of Lower-Middle-Income Asia-Pacific Countries

READINESS FACTORS	INDONESIA	VIETNAM	PHILIPPINES	INDIA	BANGLADESH
UHC Service Coverage Score (out of 100)	57	75	61	55	48
ACCA Cloud Readiness Index Rank (2020)	55	46.2	55.3	56.7	—
Cloud First Policy	✗	✗	✓	✓	✗
Cloud for Public Healthcare Mandate/ Policy	✗	✗	✗	✓	✗
Legislation on Personal Data Protection	✗	✗	✓	✗	✗
Data Protection & Privacy Legislation for Healthcare Data	✗	✗	✓	✗	✗
Cloud: Data Privacy/ Security Legislation for Healthcare Data	✗	✗	✓	✗	✗
Nature of system	National health insurance	Universal health coverage through national health insurance.	Universal health coverage through national health insurance.	Mixed health system	Mixed health system
How is the cloud being used for healthcare?	BCCR for less-sensitive healthcare information.	Some parts of the HMIS, population monitoring systems, telehealth.	COVID-19 surveillance.	Some parts of the HMIS incl. patient registration, patient admissions, billing, labs, pharmacy, disease surveillance.	Telemedicine, data analytics.

### 3.3 Interview Insights: Drivers and Benefits of Cloud Adoption

Our research into cloud adoption indicates that the key drivers of cloud adoption come in two forms – internal to a public healthcare organization and external forces.

#### Internal Drivers for Cloud Adoption

##### ➤ Improved data reliability and security

Healthcare organizations are moving to the cloud to ensure that their data is available and accessible when they need it. Hyperscale cloud services enable this by building multiple redundancy measures into their systems to ensure 99.9% server uptime with multiple data backups.

##### ➤ Scaling data storage

Public health organizations benefit from the scalability of cloud-based data storage when the number of patient visits fluctuate, as was the case when the COVID-19 pandemic overwhelmed healthcare systems. The flexible “pay-as-you-go” IaaS model can offer secure, flexible solutions to help healthcare organizations quickly and strategically scale data storage.<sup>10</sup>

##### ➤ Scaling computer power

Cloud services allow public healthcare systems to ramp up IT infrastructure quickly to implement new projects, test new projects, and carry out research by utilizing other highly advanced and sophisticated tools such as artificial intelligence, machine learning, and blockchain in an agile manner.<sup>11</sup>

##### ➤ Enabling remote work and collaboration

Cloud computing removes the barrier of geographical location, enabling remote working and solutions such as telehealth and remote care through real-time data access.<sup>12</sup>

##### ➤ Lowering infrastructure costs/moving to the variable cost model

Cloud-based systems optimize costs and shift health-IT budgets from capital expenses (Capex) to operating expenses (OpEx). Cloud computing helps optimize IT infrastructure and server costs.<sup>13</sup>

##### ➤ Data-powered decision-making and automation (machine learning, predictive analytics, IoT, AI)

The relationship between AI and the cloud can be especially useful for improving public health outcomes by bringing in productivity and efficiency to research, diagnoses, and drug discovery, to name a few.<sup>14</sup> An AI-powered cloud environment learns from the data it collects, makes predictions, and solves potential problems before the user even notices them.<sup>15</sup>

#### External Drivers for Cloud Adoption

##### ➤ Cloud First policies/mandates

Digital transformation policies for the public sector, and specifically the healthcare sector, such as Cloud First policies in Group 1 countries or as mandates driving national digital health, can be a key driver of cloud adoption.<sup>16</sup>

##### ➤ Continuity of care

Patient-centered national health systems and schemes adopt cloud technology as a key enabler of healthcare information exchange for continuity of care.<sup>17</sup>

##### ➤ Insurance/reimbursement models

In many Asian countries (Japan, South Korea, Singapore), countrywide National Health Insurance Systems (NHIS) have often led to enhanced adoption of cloud-enabled processes and systems, including automated claims processing, electronic health and medical records, and information exchange. Such initiatives call for centralization and standardization of healthcare data, the availability of which speeds up claims processing, provides a basis for regular data audits, and leads to risk stratification and population health management.

##### ➤ The COVID-19 pandemic

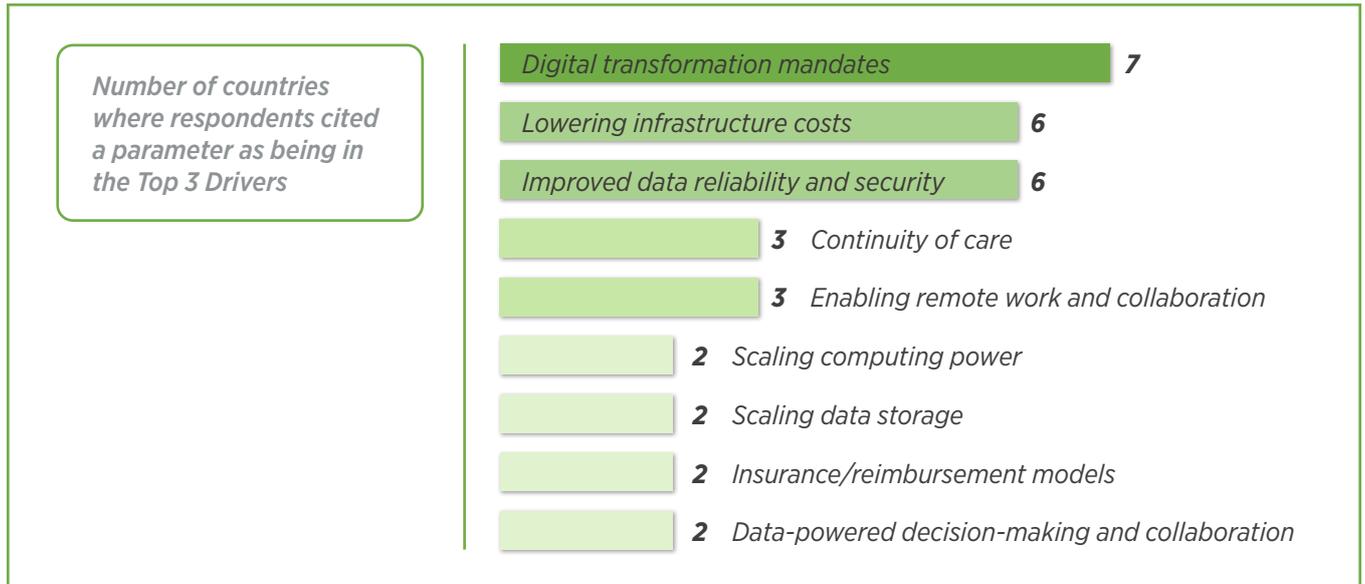
The pandemic has inadvertently been instrumental in driving up cloud adoption across all three groups. However, it is Group 3, the lower-middle-income countries, which have seen the greatest growth in cloud adoption for this reason.

### 3.3.1 Top 3 Perceived Drivers of Cloud Adoption for Public Healthcare

Respondents in these 12 countries identified the following as being among the top 3 drivers of cloud adoption for public healthcare.\*\*

1. Digital transformation of healthcare policies/mandates
2. Lowering infrastructure costs
3. Improved data reliability and security

*Drivers of Cloud Adoption in Public Healthcare based on interviews*



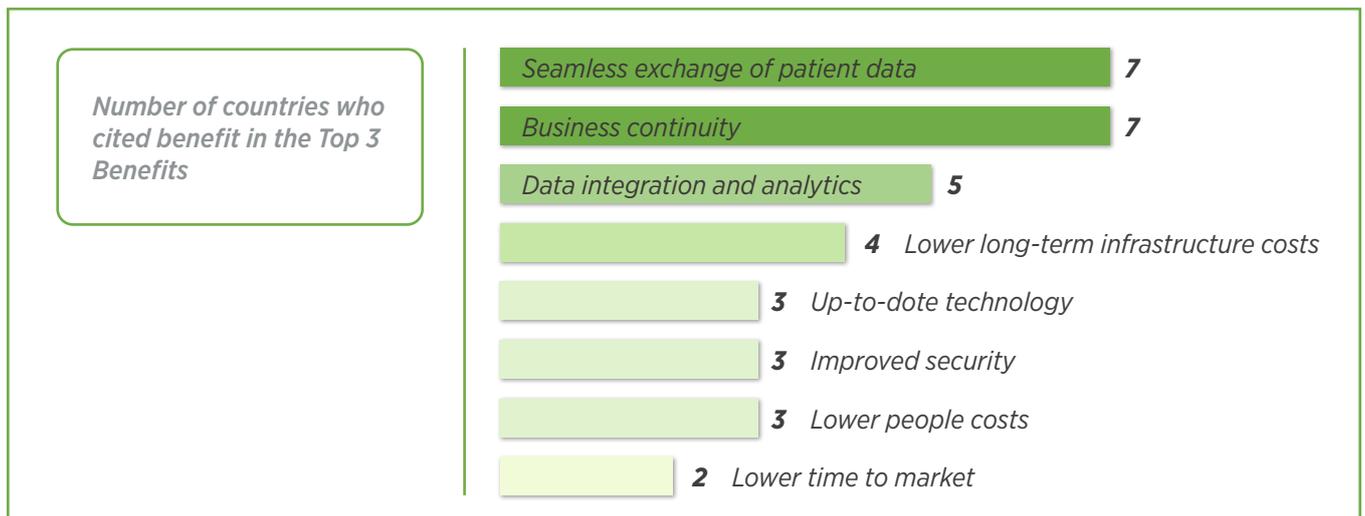
\*\*The COVID-19 pandemic was not included as a driver for this survey.

### 3.3.2 Top 3 Perceived Benefits of Cloud Adoption for Public Healthcare

Respondents in these 12 countries identified the following as being among the top 3 benefits of cloud adoption for public healthcare.

1. Seamless exchange of patient data
2. Business continuity
3. Data integration and analytics

*Drivers of Cloud Adoption in Public Healthcare based on interviews*



### 3.4 Interview Insights: Barriers to Adoption of Cloud for Public Healthcare

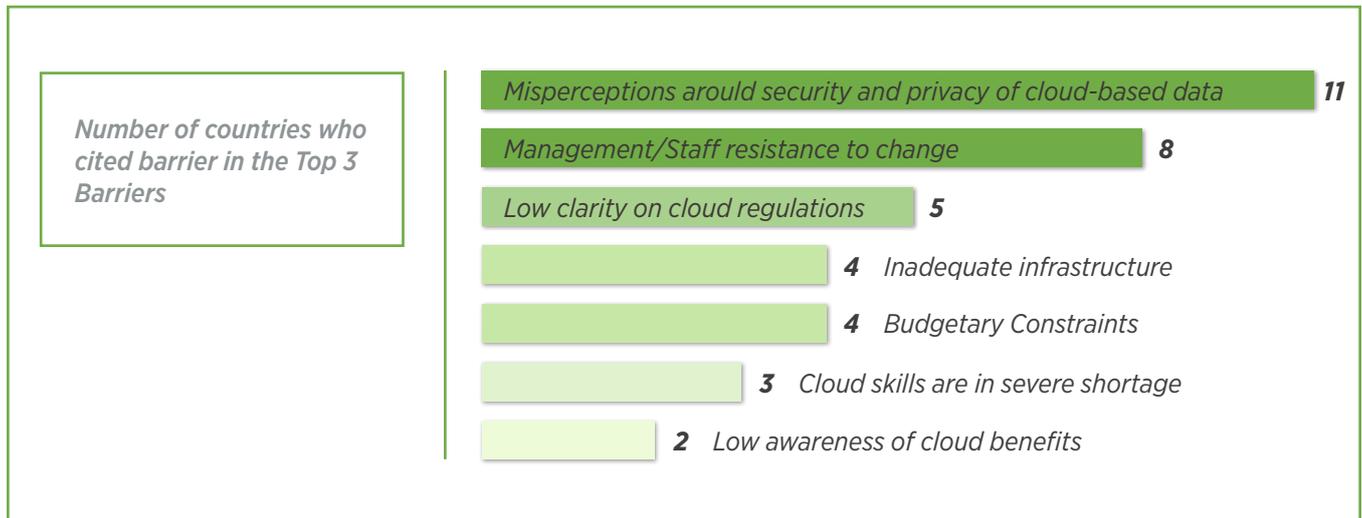
The following insights are derived mainly from the interviews we carried out to understand the barriers—both perceived and existing—and attitudes towards the adoption of the cloud for public healthcare. The research was supported by a review of existing literature.

#### 3.4.1 Top 3 Perceived Barriers to Cloud Adoption for Public Healthcare

Respondents in these 12 countries identified the following as being among the top 3 barriers to cloud adoption for public healthcare.

1. **Data security and privacy concerns**
2. **Management/staff resistance to change**
3. **Low clarity on cloud regulations**

*Barriers to Cloud Adoption in Public Healthcare based on interviews*



It is interesting to note that respondents in three out of 12 countries considered ‘improved security’ as a key benefit of cloud adoption while ‘data security and protection concerns’ were cited as the overwhelming barrier for nearly all countries. This goes to show that there are knowledge gaps and a lack of clarity as to the data security and privacy risks of healthcare data in the cloud.

### 3.4.2 A Detailed Look at Barriers to Cloud Adoption in Public Healthcare

The following section looks closely at the existing and perceived barriers to cloud adoption in public healthcare. While some of these barriers are the result of inadequate supporting infrastructure, policies and regulations, a significant number stem from a poor understanding of cloud technologies and a lack of clarity around cybersecurity in the cloud.

#### Barrier 1: Misperceptions around the security and privacy of data in the cloud

Data security and privacy concerns were overwhelmingly cited as a top concern, apprehensions grounded more in a lack of information than fact and driven by the high sensitivities attached to healthcare data. While some governments and national healthcare organizations have recognized the security benefits of the cloud and therefore subscribed to a Cloud First policy, the lack of awareness and misperceptions around these capabilities amongst policymakers and healthcare organization management in most of the surveyed countries has become a significant barrier to cloud adoption.<sup>18,19</sup> In 11 out of 12 countries, it was cited among the top three barriers to cloud adoption.

This concern was driven by the following factors:



#### 1. Data storage

Respondents reported that stakeholders perceived not being able to physically point to or see exactly where data was being stored raising concerns that the data was not secure. Additionally, respondents mentioned that uncertainty around where healthcare data is being stored has driven fears of citizens' private data being accessible by parties in the host country.



*"[The] number one (barrier) is the public's perception of security and the second is respect for the national sovereignty of the citizens' dataset and how to ensure that."*

— Dr. Robert Grenfell, Health Director, Health & Biosecurity, CSIRO, Australia

*"Governments are highly concerned about the use of cloud services because they don't want their data going out of the country. This localization aspect is particularly relevant when it comes to personal health data."*

— Dr. Peter Drury, Digital Health Transformation Consultant, Health IT Expert

## 2. Data breaches and privacy concerns

Reliance on a third party for securing or storing the data at a location that was not visible drove the perception that the data may be more open to data leaks and breaches of privacy. Additionally, the multi-tenant nature of hyperscale cloud with data centers being shared among many clients is perceived as a security risk.

Some interviewees equated the security of healthcare data in the cloud with that of mainstream office productivity SaaS software such as Office 365 and held the perception that both were equally insecure.



*“It’s important to understand the concerns of governments – they are concerned about cyber-attacks, data breaches, misuse, apart from other concerns.”*

– **Dr. Hishamuddin Badaruddin, Adjunct Assistant Professor (CoRE, Duke-NUS), Health IT Expert**

*“There is a growing movement and demand from patients to be able to control which data goes into which systems.”*

– **Stella Ward, ICT leader in the public sector, New Zealand**

*“The government is slowly adopting cloud for healthcare in Indonesia, but people still believe that their data is not safe and secure in that digital system.”*

– **Digital Transformation Consultant, Indonesia**

*“There is no such thing as utilization of public cloud because healthcare data should be in a private cloud to preserve data privacy.”*

– **Health IT Expert, Malaysia**

*“Most hospitals have concerns about allowing their data to go outside the hospital even though the law allows it. They have concerns about security on the cloud because they are not yet confident it is fully secure.”*

– **Health IT Expert, Malaysia**

## 3. Lack of personal data protection regulations

Personal data protection regulations are key to enforcing security in cloud-based environments. However, in some countries, such as India and Vietnam, the regulations around personal data protection and healthcare data protection are still in the draft stage. With the cloud perceived as a riskier, shared environment, the lack of personal data protection legislation becomes a further barrier to cloud adoption.



*“There is a lack of confidence in the security of the cloud as health records are critical data, and they should not be hacked or accessed by unauthorized users. Moreover, the Personal Data Protection bills have not yet been passed by the government.”*

– **CIO, super-specialty public hospital, India**

#### 4. Low confidence in cloud service providers

Some respondents mentioned that the lack of guidelines around cloud services' standards has led to lower trust in the capabilities and security of cloud services.



*"The biggest barrier towards cloud adoption in Malaysia is the lack of regulation explicitly stating the standards and on the utilization of cloud-based solutions."*

— **Matthew Yong, Health IT Leader, Malaysia**

*"Government cloud services need to undergo major improvements and have to comply with international standards."*

— **eHealth specialist, Philippines**

#### Barrier 2: Management and/or staff are resistant to change

IT-related change management is difficult in any sector, but it is particularly challenging in a high-touch, high-impact setting such as healthcare. Respondents in eight out of 12 countries cited resistance to digitalization among the top 3 barriers. There are multiple factors that lead to resistance from healthcare organizations' management and staff:

##### 1. Revenue and loss-of-business concerns

Respondents cited that healthcare organizations' management sometimes fears that the digitalization of healthcare will require them to share patient data with other healthcare organizations, and this will lead to a loss of business and revenue cuts.



*"Japan has been behind other countries in digitization, especially in medical care. Each hospital has its own data center or data server, which may not be connected to cloud services. This is because data sharing is not well-established in Japan even now. The government promotes such data sharing but based on the business model or medical [model] provided, data sharing may reduce their revenue. This element delays all data sharing and digitalization in the medical field."*

— **Health-IT expert and MOH Advisor, Japan**

## 2. Moving from a capital expenditure (CAPEX) to an operating expenditure (OPEX) model

Most healthcare organizations have relied on heavy capital expenditure investments to set up their own data centers, purchasing space, equipment, software, and a workforce for operating and maintaining these systems. While an advantage of cloud systems is the flexibility of the pay-as-you-go or operating expenses (OPEX) model, the change in procurement and expensing becomes a barrier for hospitals who perceive the IT budget cuts as a financial loss.

In some health systems, procurement of non-physical assets such as the cloud is not completely developed.



*“The concept of hiring (resources) in the government has not been completely developed. When we go for cloud, [the] inventory management team would ask for the name of the equipment, proof of purchase and infrastructure. But the cloud is not [a] physical [asset]. It is resources you are hiring. These misconceptions still remain in the mindset of public administration people.”*

— CIO, super-specialty public hospital, India

## 3. Concerns about being locked into a vendor

Some respondents cited vendor lock-ins as a barrier, with respondents in Singapore and New Zealand mentioning that their policy is oriented towards a multi-cloud model to avoid such a situation.



*“The challenge [in cloud technology] would be to ensure that there is no vendor lock-in. When we start adopting cloud technology, moving from one cloud services provider to another is challenging because of vendor lock-in.”*

— Manisha Mantri, Joint Director, Centre for Development of Advanced Computing (CDAC), India

## 4. Changes in workflow

Re-engineering applications for the cloud may result in a change to workflows that clinical staff find takes away their time from attending to a patient and adds to their work.



*“Change management has become a major issue as doctors are reluctant to change the workflow and the software that they are accustomed to using.”*

— Dr. Zafar Hashmi, Former Head of Technology, Healthdirect Australia

## 5. Concerns about data ownership

Some healthcare organizations perceive storing data in the cloud as giving control and ownership of the data to the cloud service provider and are concerned about CSPs deriving value from this data without the healthcare organization or the public sector benefiting.



*“Organizations also know that having data gives them more power. They don’t want to share that power and send the data out of the organization.”*

— Ji Sun, Deputy Director, HIRA, South Korea

## 6. No mandate or incentives to use the cloud

Some respondents felt that without a mandate from a central authority or policies supporting incentives, there would be limited adoption of the cloud.



*“Incentives are needed as a motivator for hospitals to adopt the cloud.”*

— Dr. Raymond Sarmiento, Director, National Telehealth Center, University of the Philippines, Manila, Philippines

## 7. Migration-related productivity concerns

Disruptions to work due to the migration and the risks of data loss during the transition were also key concerns.



*“Continuous operations are another barrier for cloud adoption. Should hospitals decide to adopt cloud, they are worried that the transition phase would entail the creation of guidelines for the new system, training of personnel, provision of enabling infrastructure, and an increase in security protocols that need to be put into place.”*

— Healthcare Digital Transformation expert, Thailand

*“Migration to the cloud is not easy, and extra efforts have to be taken to ensure that data is secure because it is then not on-premises.”*

— Dr. Zafar Hashmi, Former Head of Technology, Healthdirect Australia

*“There is still contingency planning that is required as far as having data storage is concerned. For, e.g., backing up health information in two data centers so that vital health information is not lost.”*

— National Digital Health expert, India

## 8. Limited digital literacy of healthcare staff

The cloud is a key enabler of the digitalization of healthcare. However, healthcare staff in developing and high-income countries alike may struggle to use digital technologies – the switch required to a more digital way of working is perceived as a barrier.



*“Aside from regulations, the mindset of doctors and healthcare providers is very conservative relative to other sectors. Their competencies in technology are relatively low – mindset is a big problem.”*

– **Health Data expert in the public sector, Japan**

*“Cloud is an emerging technology in the last 2-3 years in Vietnam where transitioning from a visible IT infrastructure to something abstract is new to hospital management. This is why I think it will take a long time for the cloud to be embraced and trusted completely.”*

– **Tam Phan Hong, Director of Cloud Infrastructure (FPT Smart Cloud), Vietnam**

*“Government-provided platforms have software that support EMR applications. The issue is that clinicians are not using this system for generation of electronic medical records, but rather only for lab reports, patient demographics and visit episodes.”*

– **National Health IT Expert, India**

### Barrier 3: Low clarity on cloud regulations as applicable to healthcare data

Respondents in five out of 12 countries cited the lack of clarity in data protection regulations, specifically how healthcare data should be transmitted through and stored in the cloud, in the top three barriers to cloud adoption.

The lack of clarity stemmed from any of the following cases:

#### 1. Missing regulations and/or enforcement

The country’s personal data privacy and protection regulations did not specifically mention the cloud.



*“In order for South Korea to shift towards the use of public cloud, the regulations surrounding cloud-based solutions and data privacy must be reviewed and revised. Currently, I don’t see this happening anytime soon due to practical and realistic reasons as well as public clamor for data security.”*

– **Dong Jae Yang, Digital Health Expert, South Korea**

*“The fact of the matter is that these regulations are silent about the cloud. Truthfully, the real concern here is that the Personal Data Privacy Act (PDPA) is silent about the security of healthcare data.”*

– **Health IT Expert, Malaysia**



*“There is no specific healthcare data security regulation for electronic data in place. The government must put this in place. More regulations should be developed, especially on how data can be protected and the limitations of its implementation. The government must also educate the public about the regulations surrounding cloud and how this type of technology can benefit them.”*

– **Dr. Agus Mutamakin, Chief Information Officer, Dr. Cipto Mangunkusumo Hospital, Indonesia**

*“The main problem is not the lack of regulation but its apparent lack of clarity and enforcement. In most instances, the government provides guidelines for the use of technologies in public hospitals. But since this field is dominated by doctors, the compliance is very low due to the apprehensions of these healthcare professionals and that their main priority is patient care and not these digital technologies.”*

– **Healthcare Digital Transformation expert, Thailand**

## 2. Unclear or complex data classification

Data classification regulations specify which class of sensitive data can be migrated to the cloud. When these regulations are ambiguous or too complex, there is confusion around which datasets could move to the cloud.



*“Every country has its own data security regulations; there is no harmonization around data security. Within a country, hospitals have different regulations. There is a need to unify regulations.”*

– **Dr. Roberta Sarno, Head of Digital Health (APACMed), Health IT Expert**

*“In order for more organizations to adopt cloud, the government has to step in and make the regulations easy to follow and straightforward for users.”*

– **Digital Transformation Consultant, Indonesia**

## 3. Inadequate training

While data privacy and protection regulations applicable to healthcare data have been legislated, their complexity, along with a lack of training and awareness, has resulted in low understanding and application. Healthcare organizations also fail to clearly establish data security and data protection policies and procedures.



*“Regulations are very well-classified – healthcare data are arranged according to sensitivity (4-5 classifications) with some overlaps. However, I don’t think everyone from the IT staff has clarity about these. Their competency and literacy in handling the data is not very high.”*

– **Health Data expert in the public sector, Japan**

*“Data classification and security are well defined. Yet [in piecemeal] they are not clearly understood. Standardized implementation and capacities remain a challenge.”*

– **Stella Ward, ICT leader in the public sector, New Zealand**

#### Barrier 4: Inadequate infrastructure is a significant barrier to cloud adoption

The lack of adequate internet bandwidth and sub-standard hardware is a key barrier to cloud adoption in developing countries such as Indonesia, the Philippines, India, and Bangladesh. In countries such as Bangladesh and India, power cuts are a frequent occurrence that often disrupt data transfers. Rural areas in some high-income countries such as Australia are also lagging in cloud adoption as they lack the connectivity required.



*“Most of the cloud services are accessible only through level 3 and level 4 cities or towns apart from the metros. In rural areas, it is still not fast enough even though they have a dedicated line provided by the Ministry. This is the main challenge hindering cloud adoption and development. There are huge non-government organizations who are still not using IT services.”*

— **Policymaker, Health Technology in Public Healthcare, India**

*“There needs to be a bridging of the digital divide across segments of the society in order to realize digitization in this time and age.”*

— **Fabian Bigar, Chief Executive Officer (Strategic Change Management Office, MyDIGITAL), Malaysia**

*“IT systems are poorly implemented, which leads to many operational problems with hardware being sub-standard. Internet bandwidth, too, is a big challenge – it is needed for the cloud, and when the government doesn’t have the bandwidth set up, we face problems. Our servers, internet and electricity services are regularly disrupted which leads to work getting interrupted. We have to wait till the service comes back on. We don’t have any backup servers.”*

— **Health IT Consultant to Government, Bangladesh**

#### Barrier 5: Budgetary constraints

As most public health organizations already have overstretched budgets, the cost of human resources and tools required to move to the cloud can be a major deterrent to cloud adoption.

These costs can arise due to any of the following situations:

##### 1. Re-engineering legacy applications

In countries like Australia and South Korea, where public health organizations have been using on-premises-based solutions, the cost of re-writing applications to optimize them for the cloud can be daunting. The figures are even higher for complex or custom applications.



*“How do you take care of the huge cost of the transformation to the latest technology? This is another challenge because there is already an existing setup. Catering to the fresh requirements comes at a cost. The challenge of how this cost can be borne by different stakeholders of the health system needs to be addressed.”*

— **Manisha Mantri, Joint Director, Centre for Development of Advanced Computing (CDAC), India**

## 2. Fresh cloud migrations

While many emerging economies in the early stages of healthcare digitalization are free from the baggage of legacy applications, employing technical experts and cloud specialists can be an expensive exercise. Many of these countries also prioritize building more healthcare facilities in their budget allocations, which leads to a paucity of funds when it comes to their IT budgets.



*“Cloud service providers should think about how they can lower the costs for the government as the cost is a big issue.”*

— **Health IT Consultant to Government, Bangladesh**

*“Funding for cloud migration is key and should be addressed first before plans can materialize.”*

— **Dr. Raymond Sarmiento, Director, National Telehealth Center, University of the Philippines, Manila, Philippines**

*“One of the main barriers by these public hospitals is the imminent budget cuts and reallocation they would experience once they adopt the private cloud from the government. In hindsight, it will lessen the burden from their end in terms of work efficiency, but the idea of budget cuts prevents them from transitioning towards this kind of digital technology.”*

— **Healthcare Digital Transformation expert, Thailand**

*“The government hasn’t built enough of a system to compensate the providers for moving to cloud or to reduce the cost. Clinics and smaller institutions are not motivated to use the cloud because there is no reason for them without a separate compensation from the government.”*

— **Ji Sun, Deputy Director, HIRA, South Korea**

*“There is limited availability of budget for migration from traditional systems given that resources are mostly diverted to manage the COVID-19 pandemic – vaccines, testing facilities and hospital services.”*

— **Fabian Bigar, Chief Executive Officer, Strategic Change Management Office (MyDIGITAL), Economic Planning Unit**

## 3. Low interoperability

In most of the countries included in this report, respondents mentioned that healthcare data is siloed and fragmented. Collecting and standardizing data is costly since multiple systems need to be able to talk to each other, both inside and outside the healthcare organization.<sup>20</sup>



*“The public healthcare system has a lot to do to ensure interoperability of health records even within the public health system.”*

— **Fabian Bigar, Chief Executive Officer, Strategic Change Management Office (MyDIGITAL)**



*“One problem I am trying to solve at the moment is to get people’s national COVID record matched to their local health record. That sounds easy to do, but it’s not because of the way the system is structured... So, it means the harmony of the record is not necessarily there yet.”*

— **Dr. Robert Grenfell, Health Director, Health & Biosecurity, CSIRO, Australia**

*“There is a fragmented implementation of Health Information Systems in Indonesia with limited interoperability. There are many HIS implemented by institutions across the board, but due to the absence of regulations, technical standards and poor design, implementation has been limited – it has been at the discretion of the management and has been taking place in silos. Moreover, there seems to be a disconnect in terms of HIS being utilized, given the varying preferences of both national and local hospitals due to decentralization. The variations in systems without a central policy and coordination between different levels of government and districts have made it difficult to integrate data.”*

— **Prof. Surahyo Sumarsono, Health-IT Consultant, Indonesia**

*“EMR and other standards are not enforced properly for adoption to take place, and this is a trend that is not just limited to government hospitals.”*

— **CIO, super-specialty public hospital, India**

## Barrier 6: Cloud skills are in severe shortage

The shortage of advanced cloud and security skills across all sectors and across the globe remains higher than ever – however, according to respondents, the situation is even direr when it comes to a highly conservative sector such as healthcare. The use of the cloud in healthcare requires policymakers, cloud architects, security experts, and healthcare-IT staff to have a good understanding of both the healthcare domain and cloud technology, the rarity of which has become a significant barrier to cloud adoption.



*“Skilled professionals for implementing IT services are lacking in Japan. There are not many talented people who can do that in the country.”*

— **Health Data Specialist in the public sector, Japan**

*“When it comes to the cloud in a healthcare setting, there is a knowledge and skills gap. The centralization of healthcare that is now being planned/underway is expected to bring together various departments and ensure a standardized approach, so skills and awareness come up to speed.”*

— **Stella Ward, ICT leader in the public sector, New Zealand**

*“Even many technical people are not confident about the cloud. If I want to move one application to the cloud, then I need to look at what changes are required and people require training to do so. Many people are not trained to do this.”*

— **CIO, super-specialty public hospital, India**



*“There is a requirement for competent and capable human resources. An entire cadre of human resources, including privacy experts, security experts that will check on vulnerability, technical experts for subject matter are needed. Not a lot of human resources are knowledgeable in putting systems on the cloud.”*

— **Dr. Raymond Sarmiento, Director, National Telehealth Center, University of the Philippines, Manila, Philippines**

*“The most difficult challenge to overcome is the openness and willingness of the staff and management of hospitals to adopt cloud technologies. Even if it is provided for them, they will not utilize it until they are not ready and equipped with the necessary skills to operate them.”*

— **Digital Transformation Consultant, Indonesia**

## Barrier 7: Low awareness and understanding of cloud benefits

With the cloud being a more abstract form of technology, people at all levels, from policymakers and healthcare management to staff and end-users, find it difficult to understand how the cloud works and how organizations can benefit.

### 1. The return on investment (ROI) in moving to the cloud isn't clear

With a limited understanding of the cloud, procurement agencies and policymakers are slow to recommend its use.



*“People don't understand what the difference between a server and the cloud is. CSPs talk about what the cloud is but don't explain the benefits. How is the new solution different from what they currently have? What will the ROI be? All of these are missing.”*

— **Michael Stahl, Digital Health Advisor and Consultant to APAC Governments**

### 2. Unmet expectations

Overselling by CSPs leads to dashed expectations as organizations do not fully understand what resources are needed to migrate and maintain systems in the cloud.



*“Overselling to the decision-makers in public and private organizations who have limited understanding of the cloud is eclipsing the reality of the purpose of cloud, its design considerations, and therefore, the return on investment.”*

— **Arvind Sivaramakrishnan, Chief Information Officer (Apollo Group of Hospitals), India**

*“There is poor understanding of the cloud amongst policy makers. CSPs need to make decision-makers more aware of the benefits.”*

— **Health IT Consultant to Government, Bangladesh**



*“The government has to strengthen its information dissemination campaign on the benefits of cloud so it would be welcomed by end-users and the public.”*

— **Dr. Raymond Sarmiento, Director, National Telehealth Center, University of the Philippines, Manila, Philippines**

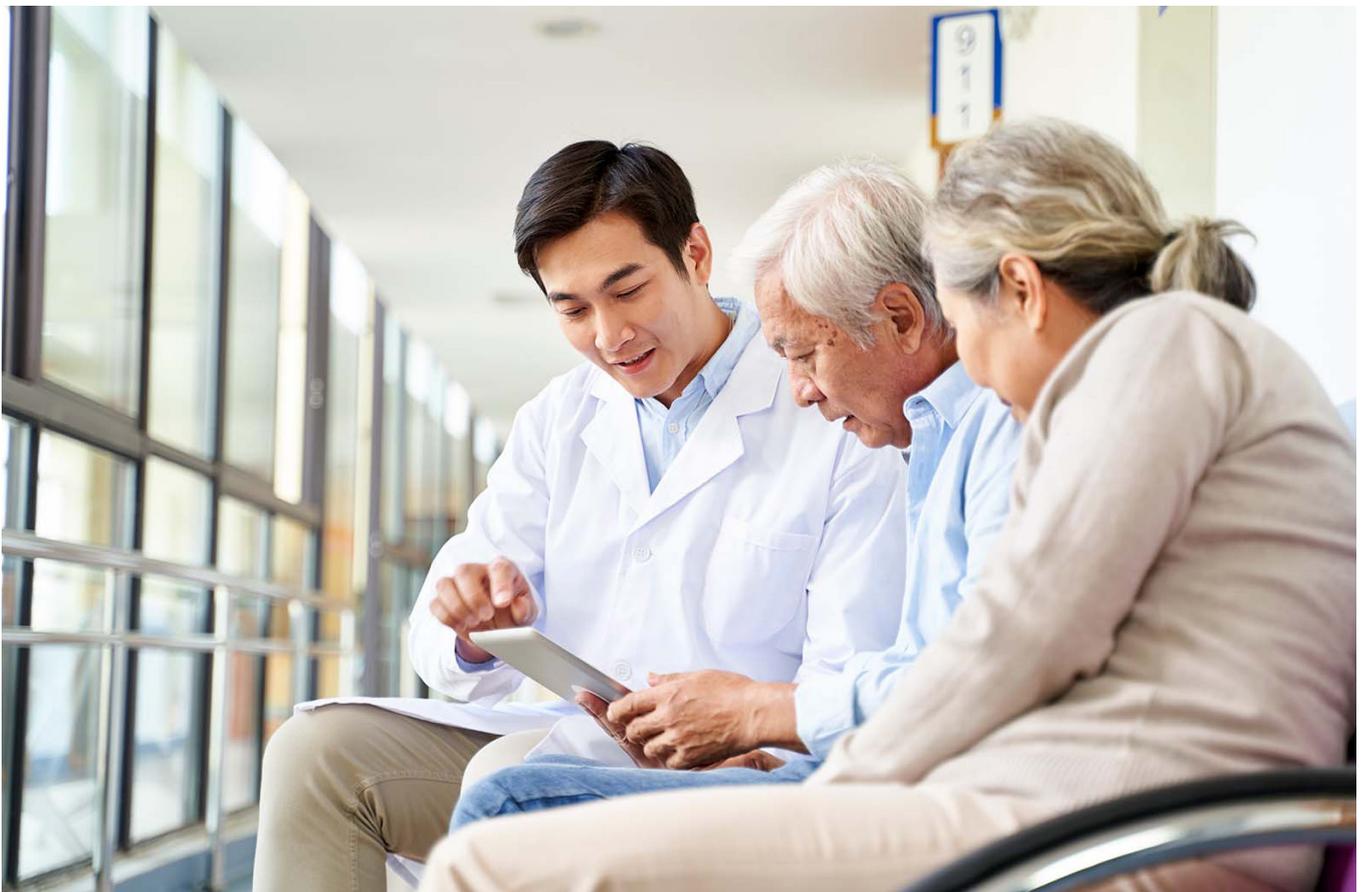
### 3. Data sharing concerns

Many ministries and agencies are either reluctant to share data or aren't aware of the benefits of sharing data, which makes them reluctant to use the cloud for solutions that require data sharing.



*“There is little demand for scalability or cost reduction because so far, data utilization is really poor. There is a lot of data being captured for every citizen; however, there is low awareness on how this data can be utilized, there are no plans to utilize this data. The government has no incentives to focus on utilization.”*

— **Health-IT expert and MOH Advisor, Japan**



## 4. Recommendations

Despite the widely varying contexts—economic, social, and political—our assessment showed common barriers across countries that affect the extent to which a country has or can adopt cloud-based systems for healthcare. To a large extent, the barriers arise out of fundamental gaps: information, stakeholder engagement, financial resources, and policies regarding the use of the cloud for public sector-driven healthcare services. These gaps are not unreasonable given that the cloud is an emerging technology, and cloud services, its applications, and risks are evolving quite rapidly. Government agencies and regulatory bodies are challenged to keep pace with innovations that provide significant public value while ensuring they do not harm public interests.

Based on a comprehensive review of cloud adoption practices in the region and globally as well as insights from expert interviews, we put forward a series of recommendations that countries can adopt to reach the clarity needed to assess and deploy appropriate cloud-based solutions for healthcare services.

The purpose of the recommendations is to provide a series of options for countries to consider for implementing the cloud effectively in service of national health goals.

### RECOMMENDATIONS FOR HEALTHCARE POLICYMAKERS

- R1:** Countries should adopt a Cloud First Policy for healthcare driven by a central digital health authority
- R2:** Use a range of policy tools to realize the full potential of cloud in the digitalization of healthcare
  - R2.1:** Develop data governance policies and regulation that ensure healthcare data protection while enabling innovation for better health outcomes
  - R2.2:** Establish open standards for data interoperability and data exchange for a patient-centered connected healthcare system
  - R2.3:** Design policies to seed a digital health innovation ecosystem
  - R2.4:** Build trust in cloud services through streamlining and standardizing procurement
- R3:** Assess and invest in creating a foundational ICT ecosystem that furthers cloud adoption
- R4:** Address capacity building at priority to overcome the key barriers to cloud adoption

## R1: Countries should adopt a Cloud First policy for healthcare driven by a central digital health authority

### What

A Cloud First policy for healthcare pushes government health agencies to consider using cloud-based technology solutions ahead of other IT solutions when a new IT project or a refresh is initiated.

### Why

A Cloud First policy will help federal and state health ministries and healthcare organizations save on IT infrastructure costs and access scalable IT resources at a level of security generally higher than on-premises solutions. The use of the cloud helps build a connected healthcare ecosystem that is necessary for the realization of inclusive, efficient, and cost-effective public healthcare.

Cloud adoption can also spur advances in public health as its scalable nature is more suitable for data-driven innovative solutions such as analytics, AI and machine learning solutions that are now driving innovation across sectors. The cloud is also vital for helping healthcare startups scale.

### How

- **Fully commit to the cloud** through a Cloud First strategy enforceable at all levels of government.
- **Empower a new or existing Digital Health Authority** to drive national strategies for cloud adoption in healthcare.
- **Establish a multi-stakeholder consortium** to advise on developing a roadmap for migration and implementation.
- **Formalize budgeting and procurement processes.**
- **Establish timelines for cloud migration along with implementing the appropriate training and education programs required for digital upskilling for healthcare personnel.**



The UK's NHS has declared 'Public Cloud First' to be a part of its architecture principles, stating that digital services must move to the cloud unless there is a clear reason not to do so.<sup>21</sup>

New Zealand's Chief Digital Officer helps drive ICT and specifically cloud adoption in the government through the issuance of guidance on procurement and implementation of cloud services.<sup>22</sup>

## R2: Use a range of policy tools to realize the full potential of the cloud in the digitalization of healthcare

**What** Introduce a range of policy tools, including mandates, financial and non-financial support, incentives, and shared risk models at the central and sub-regional levels to overcome resistance to cloud adoption.

**Why** The lack of an enforceable mandate has stalled digital health transformation initiatives in countries such as India and Thailand. Unclear ownership of digital health initiatives and the absence of a clear chain of command have further led to fragmented and siloed implementation. The right policy tools, built around critical enablers such as interoperability, regulations and procurement, can help overcome organizational resistance to digitalization and enable quicker and wider adoption of the cloud.

**How** The following mechanisms may be built into national digital health strategies and policies to improve cloud adoption:

- **Mandate** the digital transformation of healthcare enforceable at all levels of public healthcare systems. Mandates should be supported by budgetary and technical assistance.
- **Improve the adoption of the cloud through financial incentives** such as reimbursement schemes, extrabudgetary grants, and non-financial incentives such as shorter reimbursement cycles.
- **Shared-risk models** may lower the risk of adopting a digital solution by having the government bear a portion of the risk.
- **Consider the use of disincentives** such as exclusion from participating in national insurance programs and/or reduced service fees.

In the US, the Health Information Technology for Economic and Clinical Health Act (HITECH) introduced incentives related to healthcare information technology, including financial incentives for the use of electronic health record (EHR) systems among providers.

The Act increased the rate of adoption of EHRs from 3.2% in 2008 to 14.2% in 2015. By 2017, 86% of office-based physicians had adopted an EHR, and 96% of non-federal acute care hospitals had implemented certified health IT.<sup>23</sup>

In Singapore, nursing homes that subscribe to NHelp—an IT system offered free to them by the Ministry of Health (MOH) for three years, and at subsidized rates after that—will also be hosted on its healthcare cloud, H-Cloud. Such nursing homes will no longer need to buy and maintain their own systems, as NHelp provides all the programs they need, such as those for finance and rostering.



## R2.1: Develop data governance policies and regulation that ensure healthcare data protection while still enabling innovation for better health outcomes

**What** Data privacy and protection policies and regulations are a key building block of digital health. Clear data governance frameworks must be built that ensure risk-appropriate governance based on internationally recognized standards.

**Why** Given the sensitivity of health data, it is necessary to ensure its integrity, availability, privacy, and protection. Health data breaches and misuse will only increase as the volume of health data grows. However, some Asia-Pacific countries, including India and Vietnam, have not yet passed data protection regulations. At the same time, it is important to ensure that regulations do not hamper innovation through overly restrictive regulations preventing data sharing and use. Governments must develop a clear framework that allows secure collection and sharing of data between people, healthcare organizations, and the government while ensuring data protection and privacy.

**How**

- The Digital Health Authority must work with regulatory bodies and stakeholders to **develop, update, and provide training on regulations** pertaining to data security, data privacy and protection, and data localization policies.
- **Establish a central authority for the monitoring and accreditation of CSPs**, such as the FedRAMP in the US, developing mechanisms and policies for oversight and compliance, including the selection of monitoring tools, SLA violation, audit types and frequency, and accreditation procedures.
- **Regulations must be in accordance with the risk profile of the datasets** in question and in line with international standards and best practices.
- Policies should **address reporting and transparency requirements** for organizations that collect, use, and store health data. **Individuals should be given greater access and control over their data.**
- Develop and implement accountability-based instead of jurisdiction-based regulations that ensure that businesses responsible for storing and transferring a country's health data continue to follow the country's data protection rules regardless of where the data is stored.



In 2016, Singapore's Ministry of Health (MOH) completed a study mapping the world's first Multi-Group Cloud Security (MTCS) Singapore Standard to the healthcare sector. The private healthcare sector was also given guidance on the mapping between the different security groups and healthcare datasets.

The mapping guidelines showed, for example, that MTCS Level 1, the base group, could be used to host publicly available information such as clinical standards and terminology systems; Level 3, the most stringent, could be used to host clinical, administrative support systems such as billing and admissions data.<sup>25</sup>

## R2.2: Establish open standards for data interoperability and data exchange for a patient-centered connected healthcare system

**What** Fully interoperable systems enable the exchange and use of health information across organizations, regional, and national boundaries. Open standards allow users greater choice in adopting a solution that meets their needs while allowing portability across vendors.

**Why** Health data is needed for three critical purposes: for healthcare financing, for epidemiology & disease management, and for enabling resource optimization and e-governance. Respondents in a majority of the countries that have been the subject of this report have seen fragmented implementations of digital health solutions, which is more pronounced in large countries such as India and Indonesia. This obstructs the collection, sharing and analysis of health data across health systems, severely limiting the benefits of digital health solutions.

When interoperability standards are established and implemented, allowing the exchange of standardized health data via the cloud securely and in real-time, the full potential of digital health systems can be unleashed, boosting not just national but global health outcomes.

**How** Policymakers must build interoperability into their digital health frameworks from the beginning and take the following steps:

- **Establish common open standards for data interoperability** and data standardization in electronic health records (EHRs) and health information exchange (HIE) services that are internationally recognized and design a roadmap for stepwise implementation.
- **Mandate interoperability** for payers, providers, and healthcare organizations.
- **Establish incentive programs** for compliance with standards and the adoption of EHRs.
- **Provide training in the tools, standards, and regulations applicable** through national and regional cloud centers of excellence or equivalent capacity-building bodies.
- **Participate in data-transfer agreements** such as the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules (CBPR) that enable international interoperability while ensuring the respective country's privacy rules are enforced.



In 2020, the US Centers for Medicare and Medicaid Services (CMS) mandated the use of the FHIR (Fast Healthcare Interoperability Resources) standard among many CMS-regulated payers and providers by July 1, 2021.

### How interoperability improves digital medicine<sup>26</sup>

#### AI and Big Data

- provide algorithms with clear data structure and semantics
- ensure validity of analysis results
- create trust in digital technologies

#### Medical Communication

- enable easy information retrieval
- avoid medical errors caused by communication barriers
- reduce documentation burden
- empower patients

#### Research

- improve the use of real-world data (e.g. for large-scale observational studies)
- create new research hypotheses (with data mining and AI)
- enable remote development of analysis scripts

#### International Cooperation

- pool data across organizations (e.g. rare diseases, precision medicine)
- tackle global public health issues (e.g. infection control, epidemics)
- provide global access to new technologies

## R2.3: Design policies to seed a digital health innovation ecosystem

**What** Policy and budgetary support is needed to boost digital health innovation that can help support the government in tackling public healthcare challenges.

**Why** Many Asia-Pacific governments are struggling under the burden of large public health challenges. Digital health technologies and services can be a game-changer in improving health outcomes by enabling more efficient, cost-effective, and inclusive healthcare. However, the innovation ecosystem in most developing countries has not evolved to serve today's digital economy.

Governments in these countries still look to traditional financing models that require collateral to provide funding support to startups, a requirement that most startups cannot meet. Procurement is often archaic – tilted heavily towards companies that have an established track record, leaving little room for startups to work with public sector providers. In the interest of safety, governments also tend to over-regulate the digital health space, which stifles innovation. Governments should instead look to nurture their fledgling innovation ecosystem through restructuring policy changes and financing for startups. Comprehensive regulations can be put in place at this stage once the digital health system has scaled and matured.

A big share of startups' cash burn is typically in the area of online platforms and infrastructure costs, which continues for several years prior to monetization occurring. By partnering with cloud service providers and offering cloud credits, governments can play an important role in helping digital health startups scale.

**How**

- **Government financing for startups should be restructured** towards a venture capital model.
- **Design policies that support digital health startups with financial and non-financial incentives**, including investor matching, capital injections and funding assistance, as well as dedicated entrepreneurship programs such as accelerators and incubators. Tax subsidies for startups, especially refundable R&D tax credits as offered by the UK and Canada and SME grants, can go a long way.
- **Develop more inclusive procurement policies** that support smaller players and startups as opposed to turnkey vendors of a certain size and scale.
- **Build startup support networks** along with the private sector, including cloud service providers, R&D centers, academic institutions and entrepreneurship agencies.
- **Attract, retain, and build a talent pool in cutting-edge specializations** such as AI/ML and in emerging healthcare areas such as genomics and precision medicine.
- **Set up cloud pilot sites** to test and scale the adoption of cloud services.
- **Foster data-driven innovation** by encouraging 'open data' practices and data sharing by and between public and private players.

Singapore's Government Technology Agency of Singapore (GovTech) has made procurement more inclusive by inviting smaller companies to submit proposals and allowing them to partner with other companies as the procurement process proceeds further. It has also made the procurement period more flexible by allowing companies to submit proposals later in the procurement cycle.<sup>27</sup>

In 2017, ACCESS Health Digital worked with India's National Health Authority (NHA) to launch the Social Entrepreneurship Accelerator (SEA) to help Indian HealthTech startups and vendors implement Open Digital Health Standards that are applicable globally. As an AWS Activate provider, SEA worked with AWS to provide healthtech startups with free AWS credits, technical support, mentorship, and market access to help startups grow their business.<sup>28</sup>

A research fund set up by the Australian government, the **Medical Research Future Fund**, injected \$19.8 million in a digital health accelerator, **ANDHealth**, the government's largest investment in digital health. 10 companies selected in its initial pilot program raised over \$70 million, created 300 jobs and undertook 44 clinical studies over four years.<sup>29</sup>



## R2.4: Build trust in cloud services through streamlining and standardizing procurement

**What** The digital health authority should establish policies and issue guidance that enables streamlined and standardized procurement of cloud services.

**Why** Budgetary concerns and a limited understanding of cloud services have hindered the adoption of the cloud. Guidance on procurement along with the establishment of minimum service standards for CSPs can help organizations adopt the cloud with greater confidence. This will also help mitigate concerns around cloud data governance, vendor-concentration risks and business continuity.

**How**

- **Issue procurement guidance** specific to the risk profiles of applicable datasets, cloud computing service types (IaaS, PaaS or SaaS), cloud deployment models (public, private, community, hybrid) in line with internationally accredited security and privacy standards.
- **Issue a list of certified CSPs** that meet the minimum level of standards as outlined in the procurement guidance. Alternatively, allow organizations to self-assess or appoint an independent third-party assessor to identify a suitable cloud service based on the procurement guidance issued.
- **Allow 'smarter procurement'** by buying as a single enterprise at the central or sector-level and standardizing contracts.
- **Define detailed Service Level Agreements (SLAs)** that address data governance in the cloud, service and data availability, risk management and remedial measures, exit management and other service considerations.
- **Mitigate vendor-concentration and lock-in risks by modifying requirements to include** hybrid and/or multi-cloud models, cloud portability, and technology-neutral architecture as appropriate.

The New Zealand government has negotiated commercial agreements with CSPs to create a marketplace that enables government organizations to access cloud services with a single price book and standard terms and conditions. The government is also developing a marketplace to give government organizations access to a catalog of cloud services.<sup>30</sup>

The Australian Cyber Security Centre and the Digital Transformation Agency have released guidance to help government agencies assess CSPs and their services.<sup>31</sup> Its Infosec Registered Assessors Program (IRAP) initiative provides assurance that ICT systems meet the Australian government's cyber security standards.<sup>32</sup>



## R3: Assess and invest in creating a foundational ICT ecosystem that enables cloud adoption

### What

The central government must establish policies and create an investment plan to build a strong ICT foundation for cloud adoption spanning both:

1. The physical resources needed, such as international and domestic broadband connectivity and newer digital technologies, broadband quality, and reliable power.
2. A sustainable talent pool for bringing the country's ICT strategy and vision to life.

### Why

The COVID-19 pandemic has highlighted the importance of core ICT infrastructure for rapid, convenient, and affordable delivery of essential national services such as teleconsultations, remote diagnosis and monitoring, secure health data storage, exchange, and transfer. Our research shows that developing countries such as Indonesia, India and Bangladesh are lacking in such infrastructure, impeding the use of digital health technologies, including the cloud.

Moreover, in countries as varied as New Zealand, Japan, and the Philippines, interview respondents noted a significant skills gap both in IT technologies and cloud services in the local workforce. Investing in this ICT foundation will be key to the growth of cloud-enabled digital technologies. Moreover, a national Cloud First policy will help governments reduce taxpayer spending on IT infrastructure and adopt a more scalable pay-as-you-go approach to IT while enabling improved service delivery.

### How

- **Assess gaps in ICT infrastructure and skills in the existing ICT strategy and create an investment plan**
- **Mobilize sustainable financing** by establishing a dialogue between all stakeholders, including multilateral organizations and development banks, to mobilize the financing and investments needed.
- **Establish a national plan for ICT upskilling:** A multi-pronged approach may be needed to reduce the gap, including both short-term intensive re-training and upskilling courses as well as IT skill programs in primary, secondary and tertiary education.
- **Adopting a national Cloud First strategy** will speed up cloud adoption.

**New Zealand's Cloud First Policy:** The New Zealand government requires public sector organizations to accelerate their adoption of cloud services—in a balanced way—so they can drive digital transformation. The Cloud First policy requires organizations to:

- adopt public cloud services in preference to traditional IT systems.
- make adoption decisions on a case-by-case basis following a risk assessment.
- only store data classified as RESTRICTED or below in a cloud service, whether it is hosted onshore or offshore.<sup>33</sup>



## R4: Address capacity building at priority to overcome the key barriers to cloud adoption

**What** Narrow the cloud services knowledge and implementation gap through education coupled with technical assistance.

**Why** Resistance to digital technologies by hospital management and administration was cited as one of the major barriers to cloud adoption. Knowledge gaps in understanding how cloud technologies work and its benefits, a shortage of cloud in healthcare skills, along with the poor design of cloud-enabled digital health applications, have all contributed to this reluctance and need to be addressed with high priority.

**How** The ministry of health, digital health leadership, regional and multilateral health organizations, donors, and other stakeholders should develop a coordinated strategy for capacity building. A designated body for capacity building such as a Centre of Cloud Excellence or equivalent can play an important role in addressing gaps through the following:

### Education, training and awareness:

- A Massive Open Online Course (MOOC) based model can be used for education and training on a large scale.
- Develop module-based curricula for healthcare professionals on digital adoption and training with a specific focus on cybersecurity risks and implications.
- Guide healthcare organizations to clearly set out data protection and privacy regulations in line with policy guidelines.
- Healthcare IT personnel should be trained in developing the skillsets and expertise needed to design and manage the use of cloud services in healthcare applications according to their respective security classifications.
- Decision-makers at all levels of government must also be groomed to understand technology use and its implications, including the use of the cloud.
- Best practices, success stories and lessons from failure using the cloud should be disseminated not only among policymakers but across the healthcare ecosystem nationally and across borders.
- Change management models such as ADKAR and ADOPTS should be implemented to overcome resistance to the cloud and digital technology adoption.

### Digital Health Applications:

- Guide organizations in the best practices applicable to migrating legacy applications to the cloud and adopting cloud-native approaches – these are crucial to realizing greater returns on investment in the cloud.
- Consider the use of PaaS and SaaS-based digital health for small and medium-sized hospitals that together cater to a majority of the population, as these require relatively lower training. Technology neutrality is also an important principle to be implemented to lower time spent on training if switching to a new vendor.
- Stakeholders and end-users must be brought together to design digital health applications in keeping with best practices such as the UNDP's design principles for digital applications.<sup>34</sup> This will address end-users' concerns and improve attitudes towards digitalization.



**The African Alliance of Digital Health Networks' Digital Health Leadership Program aims to build capacity in digital health leaders through training, mentorship and providing support through peer networks. This is intended to drive confidence, better management and improvements in the planning and execution of digital health initiatives.<sup>35</sup>**

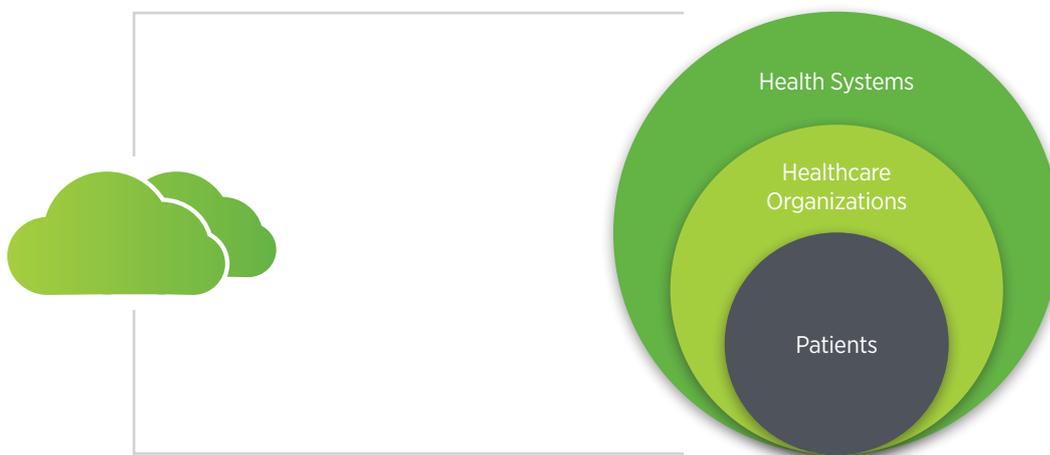
**The Malaysian Digital Economy Blueprint aims to develop "Digital Transformers" to groom highly skilled civil servants comprising technical experts and professional ICT-related talent.<sup>36</sup>**

## 5. How Can Public Healthcare Benefit from the Cloud?

Cloud technology offers a multitude of benefits for healthcare, a sector that is generating ever-increasing volumes of data, with new clinical breakthroughs coming at a rapid pace. At the same time, the sector is also facing challenges in terms of data and operational fragmentation. Cloud technologies can help maximize these opportunities and address these challenges through their hyper-scalable data storage and computing power, by facilitating the exchange of real-time data across devices and geographic locations and as an enabler of data-powered decision-making.

Throughout the sections below, we describe how the cloud brings benefits to the healthcare sector at three levels: health systems as a whole, hospitals and healthcare facilities, and to patients.

*Cloud brings about benefits to healthcare systems at three levels*



### 5.1 Cloud Drives Health System Transformation Through Data-Powered Solutions

Health systems throughout the Asia-Pacific region are grappling with the twin demographic shifts of aging populations and an expanding middle class, which mutually contribute to a rise in chronic conditions and a demand for high-quality services. Consequently, health systems are shifting from acute-care-centric models to chronic disease care that is patient-centered, personalized, and efficiently delivered. With this shift comes a high demand for data integration as value-based care gains traction and as health systems invest in long-term, community-based care models.

Cloud-based solutions support health systems to transform their care and financing models. Screening and diagnostics, health data exchanges, and connected care systems enable healthcare providers to right-site care: providing the right care at the right time and in the most appropriate location or facility. Medical research, population health management, logistics management, and financing services support health systems in responding to current healthcare needs while strategically planning for future needs.

The real-time health information of an entire population, coupled with advanced predictive tools such as AI and ML, are powerful tools for the public health system to monitor people's health and drive health-seeking behavior. Health systems can invest in innovation through cloud technology, as it provides access to important datasets in secure conditions.



The Thai Ministry of Public Health uses a cloud-based artificial intelligence system and mobile application data to predict public health risks and gastrointestinal disease hotspots, mitigating the risk of epidemics. With an accuracy rate of 80%-90%, the AI model analyzes photographs of public restrooms and brings sanitation issues to the notice of local restroom operations staff.<sup>37</sup>

Due to its scalability, cloud technology can adapt to large amounts of data such as genomes and DNA sequences gathered from next-generation sequencing.<sup>38</sup> The information collected can promote earlier detection and prevention of diseases and develop better diagnostic and treatment plans.<sup>39</sup>



The US National Cancer Institute implemented Broad Institute’s FireCloud and Seven Bridges Genomics’ Cancer Genomics Cloud in 2015. The cloud spaces were open to the public, who could analyze and develop analysis workflows to detect patterns and anomalies within genomic sequences. This improves access across medical research institutions, driving the pace for innovations and discoveries.<sup>40</sup>

Since the beginning of the COVID-19 pandemic, there has been broad recognition of the importance of digital health infrastructure for resilient health systems. Countries that quickly developed and deployed secure digital health tools were better at containing SARS-CoV2 in 2020. Notable initiatives included applications for contact tracing, testing, and epidemiological analysis, along with the use of telehealth to reach patients who could not travel or for whom it was not safe to visit the clinic or hospital.



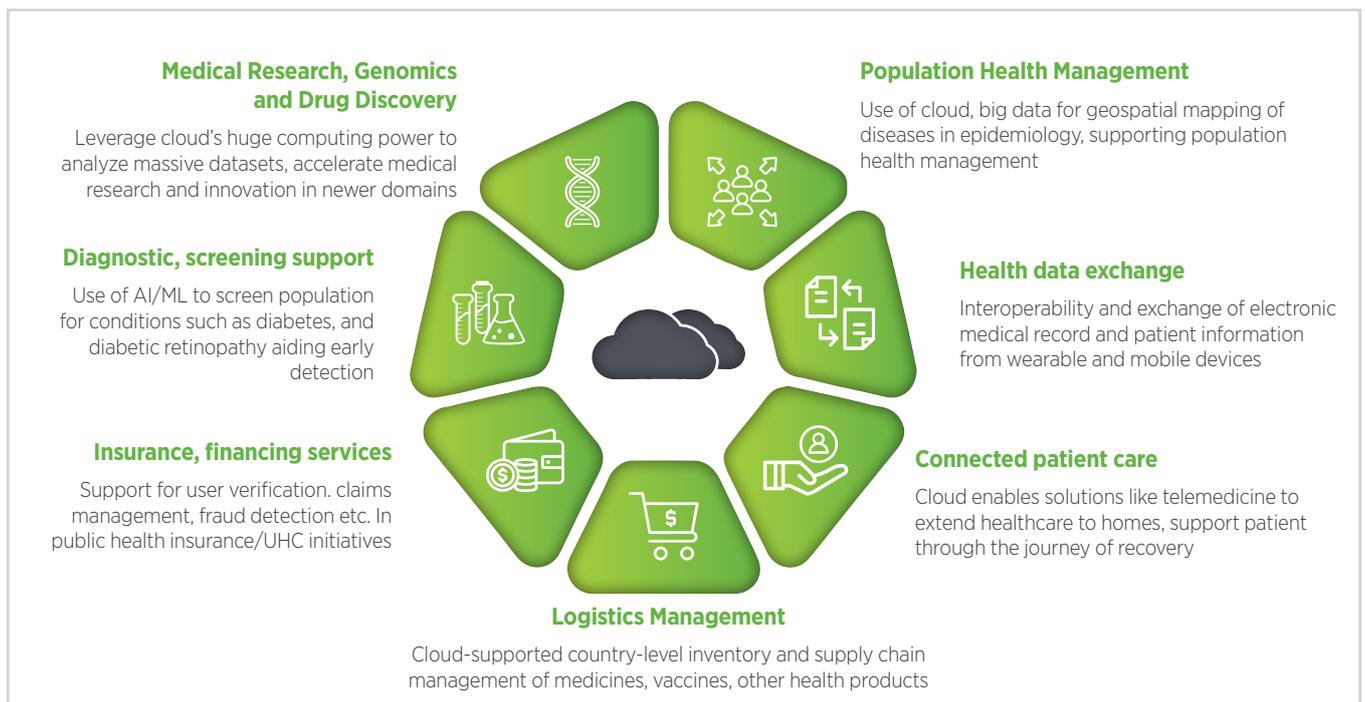
The Republic of Korea introduced the Epidemic Investigation Support System as a part of the COVID-19 response, which shortened the contact tracing process from 24 hours to 20 minutes for the South Korean population during the initial wave of the pandemic.<sup>41</sup>



The UK’s automatic syndromic surveillance system scans National Health Service digital records to pick up clusters of a respiratory syndrome that could signal COVID-19.<sup>42</sup>

The pandemic also shone a light on sub-national inequities in access to healthcare. The importance of digital health tools that are interoperable and universally available underpin the realization of universal health coverage (UHC); only with digital technologies will countries be able to achieve the iron triangle of UHC: access, cost, and quality. Doing so will require infrastructure and tools that are both secure and adaptive. Interoperability of data connects the entire health system with a click, and through cloud adoption, patient data becomes readily available for gaining insights to facilitate UHC healthcare planning and implementation.

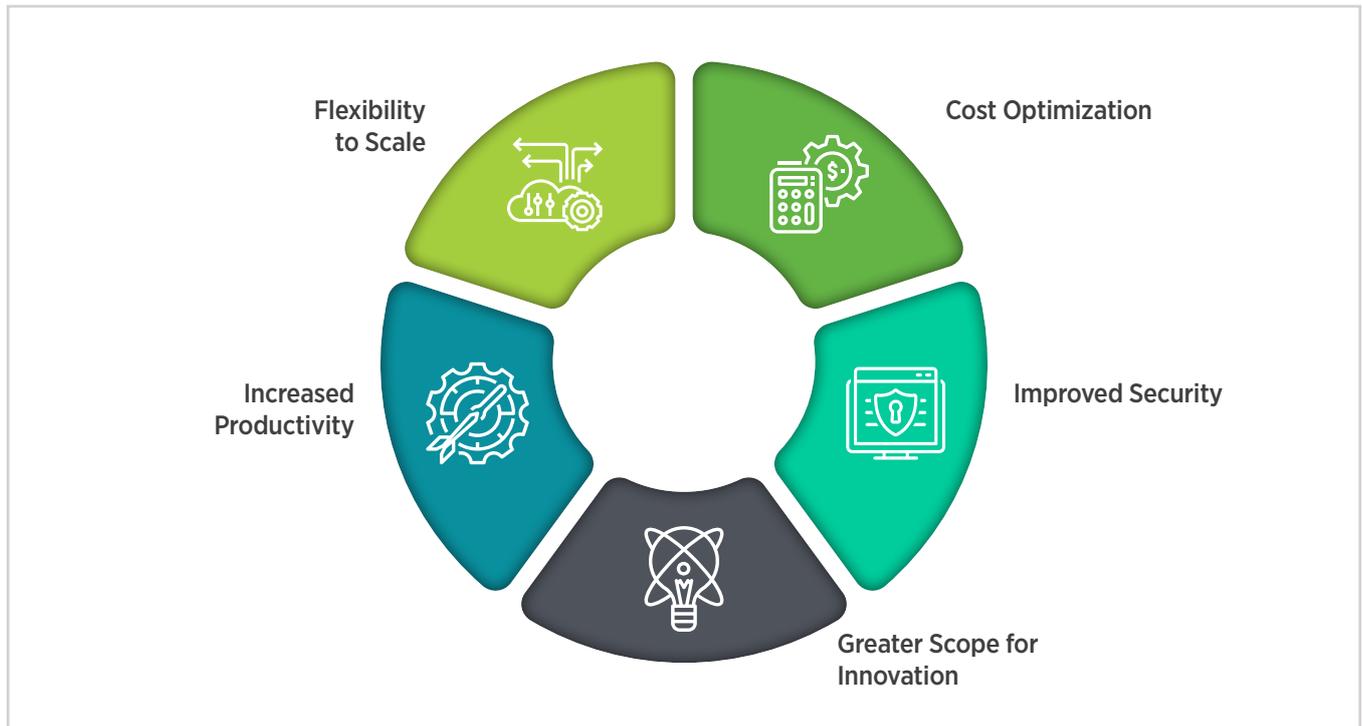
*Benefits of cloud for health systems*



## 5.2 Healthcare Organizations Benefit from Leaner, More Strategic Operations to Offer High-Quality Patient-Centered Care

By transferring the operational load of IT systems' procurement, upgrades and maintenance to cloud service providers (CSPs), healthcare organizations can focus on their core services: patient care. The cloud provides a host of benefits to healthcare organizations, as shown below.

*Benefits for government healthcare organizations*



### Flexibility to Scale

While on-premises systems require additional investment and implementation time, cloud computing allows healthcare organizations to rapidly scale storage and computing abilities up or down without any time delay at a marginal increase in cost. Cloud computing adapts to the needs of healthcare systems at all times, enabling organizations to handle varying scales of operations to implement national programs, store higher volumes of patient health records and respond to crises such as the COVID-19 pandemic. By ensuring that services continue to be available even amidst high spikes in demand, cloud services ensure business continuity.

According to a study published by the *Journal of the American Medical Informatics Association*, during the pandemic, the country's telehealth services for urgent care grew by 683% and by 4,345% for non-urgent care.<sup>43</sup>

Indonesian telemedicine startup Halodoc, which runs on AWS cloud, found that active users of its services have reached more than 20 million people in Indonesia, which was a 10-fold increase in the first quarter of 2020 from the year before.<sup>44</sup>



## Cost Optimization

Migration to the cloud reduces upfront investments in IT infrastructure, enabling access to scalable IT resources through a pay-as-you-go model. It reduces government investments in establishing data centers, which require upgrading, maintenance and resources over time. Studies show that cloud computing is more cost-effective compared to analytics tools supported by local data centers, especially for data-intensive projects such as biomedical, translational research.<sup>45</sup>



Singapore's Healthcare-Cloud (H-Cloud) is a nationwide private cloud that seeks to reduce operational costs by an average of 55% by 2025.



## Improved Security

Governments often cite security concerns as a reason for hesitation in migrating from legacy IT systems to cloud-based systems. However, if designed and implemented correctly, cloud-based systems can be more secure than information held on-premises. For on-premises systems, any harm to the data center can result in losing valuable patient and organizational information. Robust cloud options include automatic backups and data recovery—which minimize loss in the event of a breach—and automatic upgrading to the latest security patches.<sup>46</sup>

Cloud service providers are subject to strict and extensive security and compliance regulations across the globe, especially as more organizations dealing with highly classified data, such as the US Department of Defense, are migrating to the cloud.<sup>47</sup> Consequently, industry leaders such as AWS, Microsoft Azure and Google Cloud invest heavily in ensuring the security and privacy of data through multiple physical and digital security measures. It would not be possible for a healthcare organization to achieve such high levels of security on its own without exceeding its IT budget.



In 2017, the Republic of South Korea launched the Precision Medicine Hospital Information System (P-HIS), a program to implement precision medicine in hospitals. The program aggregates sensitive information from multiple sources and thus needs to be secure. The Korea University Medical Center (KUMC) collaborated with Clinerion, a Swiss-based provider of “anonymized identification” technology. Clinerion's Patient Network Explorer anonymizes data at the source hospital and de-anonymizes the same data at the destination, ensuring the security of the data exchanged.<sup>48</sup>



## Greater Scope for Innovation

Cloud-based systems provide real-time health information and advanced predictive tools such as AI and sophisticated analytics, which can be used by healthcare organizations to carry out research across large datasets, and avail of clinical decision support tools. Data extrapolation and analysis across departments can help improve the patient experience, adhere to quality standards, and make use of new technologies and applications.



The U-health program is a unique health innovation by the Korean government that allows the monitoring of patient data collected from wearable healthcare devices. Under this program, the Seoul St. Mary's Hospital at the Catholic University of Korea undertook a pilot program that developed algorithms to monitor blood glucose levels for patients. Research suggests that innovation such as this can reduce physician time by 50% and reduce out-of-pocket costs incurred by the patient.<sup>49</sup>



One of the largest private hospital chains in India, Apollo Hospitals, partnered with Microsoft's AI Network for Healthcare to apply machine learning and AI to cardio-vascular health records to develop an Indian-specific heart risk score. The heart risk score, along with Apollo Hospitals' AI model, helps predict a patient's risk for heart disease and allows doctors to establish an earlier diagnosis and create a patient health plan.<sup>50</sup>



### Increased Productivity

Cloud computing boosts productivity for both clinicians and IT teams. Post-migration to the cloud, internal IT teams do not have to procure or manage hardware or operating system requirements. The cloud allows for virtual collaboration between stakeholders, including hospital departments and government divisions.<sup>51</sup> Its agile infrastructure enabled remote working during COVID-19, as it provided better flexibility to switch over to virtual interactions and deploy resources quickly.



The state of South Australia's Department for Communities and Social Inclusion provides health services for people with disabilities through a network of non-governmental organizations (NGOs). The Department deployed a single software-as-a-service (SaaS) cloud platform provided by Salesforce, which automates contract administration and processing of payments to NGO partners. After adoption, processing time was reduced from an average of five weeks to less than three days. The South Australian public agencies have employed whole-of-government contracts that enable access to DCSI's Salesforce platform.<sup>52</sup>



Accenture, in its 'The Cloud Imperative in Healthcare' report, observed that healthcare organizations implementing a multi-cloud operating model saw a 20% to 50% productivity spike and a 30% to 80% improvement in quality while leveraging a two to eight times increase in speed to market.<sup>53</sup>

## 5.3 Patients Receive More Accessible, Personalized, High-Quality Care

### *Benefits for patients*



By creating a connected healthcare ecosystem, the cloud helps patients better manage their own health.



## Easier Registration, Access to Medical Records and Reimbursements

With cloud computing and its scalability, patient registration, outpatient processes and billing are streamlined and far more efficient. Moreover, with their data stored in cloud files, patients can access their health records remotely at any time. This creates greater transparency in the healthcare system and helps patients take ownership of their own health.<sup>54</sup> Billing processes become well-connected to patient insurance, allowing for smoother transactions.



Singapore allows citizens to access hospital discharge summaries, test results for chronic diseases, health screening records, and upcoming medical appointments from its HealthHub.sg website and its app.



## Continuity of Care

Cloud technology allows for secure exchanges of patient health records across hospitals and healthcare organizations. This makes patients' health data available to pharmacists, doctors, and financial entities, promoting continuous care of the patient. With a smooth exchange of information, patients can be given the best care no matter where they are. Cloud-based solutions also encourage medical personnel to collaborate and provide the best care possible for the patient.<sup>55</sup>

The rise of telehealth has also allowed continuity of care, permitting the inclusion of patients who were otherwise unable to travel or get care services to also access healthcare services at a lower cost. It reduces travel time and reduces the risks of disease spread in hospitals while helping patients manage chronic diseases through remote patient monitoring.<sup>56 57</sup>



Collaborate Health Cloud is a technology startup based in Greece that aims to improve patient care through team-based and patient-centric diagnoses. Through their Team-Based Diagnosis feature, the startup provides patients access to second opinions and reduces time costs for collaborative diagnosis to administer the best possible care for the patient.<sup>58</sup>



Partners HealthCare is a US-based non-profit network of healthcare providers that offer remote monitoring and other programs for heart failure patients. The organization has enrolled over 1,200 heart failure patients since 2006 and has reduced hospital readmission among its clients by 50%. Patients send real-time data on heart rate, blood pressure, and weight on a day-to-day basis, improving patient analytics and promoting patient education and care.<sup>59</sup>



The Smart Health Video Consultation (SHVC) initiative in public hospitals in Singapore enables patients to follow up with physicians virtually after being discharged from hospitals.<sup>60</sup>



## User Engagement and Patient Feedback

Through cloud solutions, user engagement and feedback portals can be managed to gain valuable insight into patient and user experience. This promotes better care and the provision of services for patients. Patient feedback and user engagement also improve communication between patients and medical personnel and improve personalized delivery of medical services. Moreover, the cloud also enhances patient inquiry systems, ensuring faster and higher quality responses to patients' administrative queries.<sup>61</sup>



Google Cloud provides a Contact Centre AI, a virtual agent that converses with patients and assists them with complex administrative or medical issues. They also released a cloud solution, Rapid Response Virtual Agent, which was created specifically for the COVID-19 pandemic.<sup>62</sup>

# 6. Acknowledgements

ACCESS Health and AWS Institute are deeply indebted to the 40+ policymakers, public healthcare leaders, and digital health experts for sharing their valuable insights on cloud adoption in the Asia-Pacific region for this report.

## Amazon Web Services

### PROJECT ADVISORS

**Agne Makaускаite**,  
Head of Public Policy for Regulated Industries, APJ

**Andrew Wiltshire**,  
Healthcare Policy Lead, Public Policy APJ

**Monique Viengkhou**,  
APJ Lead, AWS Institute

## ACCESS Health International

### PROJECT LEADS

#### Singapore

**Simeen Mirza**, Senior Strategy Consultant

**Sejal Mistry**, Regional Director

#### India

**Dr. Anuradha Katyal**, Technical Specialist & Research Lead

**Prashanthi Krishnakumar**, Program Manager

#### Philippines

**Miggy Marasigan**, Program Manager

### TECHNICAL EXPERTS

**Dr. Pankaj Gupta**, Management Consultant in Healthcare

**Jabin Pathan**, Digital Health Specialist

**Dr. Ramachandran Balaji**, Digital Health Strategy Expert

**Dr. Arundhathy Mamidi**, Health Systems Transformation Consultant

**Krishan Bhardwaj**, Digital Health Expert

### KEY CONTRIBUTORS

#### Singapore

**Adrienne Mendenhall**, Head of Business Development

**A Vigneswari**, Junior Consultant

**Tanya Sharma, Gauri Saxena, Afiya Dikshit Syed, Avanti Balaji**, Interns

#### India

**Girish Bommakanti**, Director, Operations & Strategy

**Sireesha Perabathina**, Consultant

**Komal Malhotra**, Program Manager

**Sushma Dsouza**, Research Associate

#### Philippines

**Abegale Escolano**, Program Associate

**Ramer Karlo Buot**, Program Associate

#### Malaysia

**Nasir Ismail**, Senior Consultant

#### Vietnam

**Hoang Phuong Nhung Vo**, Research Analyst

## 7. Endnotes

- <sup>1</sup> Amazon Web Services, Inc. (2017). Moderna Therapeutics Delivers mRNA Drugs Faster, at Lower Cost Using AWS. <https://aws.amazon.com/solutions/case-studies/moderna-therapeutics/>.
- <sup>2</sup> Dcruz, N. (2021, July 20). How Cloud Computing helped accelerate the COVID-19 vaccination. Great Learning. <https://www.mygreatlearning.com/blog/how-cloud-computing-helped-accelerate-the-covid-19-vaccination/#Benefits%20cloud%20computing>.
- <sup>3</sup> Alawadhi, N. (2021, June 29). Salesforce Cloud helping deliver vaccines to billions the world over: exec. Business Standard. [https://www.business-standard.com/article/companies/salesforce-cloud-helping-deliver-vaccines-to-billions-the-world-over-exec-121062901514\\_1.html](https://www.business-standard.com/article/companies/salesforce-cloud-helping-deliver-vaccines-to-billions-the-world-over-exec-121062901514_1.html).
- <sup>4</sup> New Zealand Government. (2021, December 16). Why government organisations use public cloud services. <https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/about/why/>.
- <sup>5</sup> Donnelly, C. (2018, January 22). NHS Digital declares the public cloud a safe place to store patient data. ComputerWeekly.com. <https://www.computerweekly.com/news/252433531/NHS-Digital-declares-the-public-cloud-a-safe-place-to-store-patient-data>.
- <sup>6</sup> Asia Cloud Computing Association. (2020, May 28). The Cloud Readiness Index (CRI) 2020 by the Asia Cloud Computing Association (ACCA). Slideshare.net. <https://www.slideshare.net/accacloud/the-cloud-readiness-index-cri-2020-by-the-asia-cloud-computing-association-acca>.
- <sup>7</sup> Raghavan, A., et al. (2021, January 5). Public Health Innovation through Cloud Adoption: A Comparative Analysis of Drivers and Barriers in Japan, South Korea, and Singapore. International Journal of Environmental Research and Public Health 2021 (18), pp. 334. <https://doi.org/10.3390/ijerph18010334>.
- <sup>8</sup> ACCESS Health Interviews.
- <sup>9</sup> Mace, S. (2021, January 29). Report: Healthcare Most Targeted Industry for Cyber-Crime In 2020. Health Leaders. <https://www.healthleadersmedia.com/technology/report-healthcare-most-targeted-industry-cyber-crime-2020>.
- <sup>10</sup> Iversen, H. K. (2020, June 2). Scaling Your Data Storage in the Cloud. Forbes. <https://www.forbes.com/sites/forbestechcouncil/2020/06/02/scaling-your-data-storage-in-the-cloud/?sh=747ea6564f1c>.
- <sup>11</sup> Ranger, S. (2018, December 13). What is cloud computing? Everything you need to know about the cloud explained. ZDNet. <https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/>.
- <sup>12</sup> FinSMEs Ltd. (2021, March 31). 7 Benefits of Cloud Computing for Remote Working. <https://www.finsmes.com/2021/03/7-benefits-of-cloud-computing-for-remote-working.html>.
- <sup>13</sup> Turco, K. (2021, June 24). 4 Ways Cloud Computing Can Save Your Company Money. Technology Advice. <https://technologyadvice.com/blog/information-technology/4-ways-cloud-computing-can-save-money/>.
- <sup>14</sup> Kwo, L. (2021, July 1). Contributed: Top 10 Use Cases for AI in Healthcare. Mobihealthnews.com. <https://www.mobihealthnews.com/news/contributed-top-10-use-cases-ai-healthcare>.
- <sup>15</sup> Ribeiro, J. (2021, March 16). 5 key benefits of the relation between AI and the Cloud. Towards Data Science. <https://towardsdatascience.com/5-key-benefits-of-the-relation-between-ai-and-the-cloud-611315d192d4>.
- <sup>16</sup> Development Asia. (2021, June 23). Why Cloud Computing Is a Key Enabler for Digital Government. <https://development.asia/explainer/why-cloud-computing-key-enabler-digital-government>.
- <sup>17</sup> Jones, M. (2021). 9 Key Benefits of Cloud Computing in Healthcare. Cox Blue. <https://www.coxblue.com/9-key-benefits-of-cloud-computing-in-healthcare/>.
- <sup>18</sup> New Zealand Government. (2021, December 16). Why government organisations use public cloud services. <https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/about/why/>.
- <sup>19</sup> Donnelly, C. (2018, January 22). NHS Digital declares the public cloud a safe place to store patient data. ComputerWeekly.com. <https://www.computerweekly.com/news/252433531/NHS-Digital-declares-the-public-cloud-a-safe-place-to-store-patient-data>.
- <sup>20</sup> McDonald, D. D. (2013, December 13). Scoping Out the 'Total Cost of Standardization' in Federal Financial Reporting. Squarespace. <https://static1.squarespace.com/static/52f8e871e4b060243dd758d6/t/5786898a09e1c4bfec4d3ba6/1386966957743/ScopingOuttheTotalCostofStandardizationinFederalFinancialReporting.pdf>.
- <sup>21</sup> NHS Digital. (2021, March 12). Public cloud first. <https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-architecture/principles/public-cloud-first>.
- <sup>22</sup> New Zealand Government. (2021, November 16). How to adopt public cloud services. <https://dns.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/about/how/>.

- <sup>23</sup> HIPAA Journal. (n.d.). What is the HITECH Act?. <https://www.hipaajournal.com/what-is-the-hitech-act/>.
- <sup>24</sup> Kim, S. J. & Bae, S. (2021, August 17). Korean Policies of Cybersecurity and Data Resilience. Carnegie Endowment for International Peace. <https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164>.
- <sup>25</sup> The Infocomm Development Authority of Singapore. (2016, May 4). Singapore Maps Cloud Security Standards to Private Healthcare Sector, Exploring Data Certification Framework. <https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Media-Releases/2016/singapore-maps-cloud-security-standards-to-private-healthcare-sector-exploring-data-certification-framework>.
- <sup>26</sup> Moritz Lehne et al. (2019, August 20). Why digital medicine depends on interoperability. *NPJ Digital Medicine*, 2019 (2), 79. <https://doi.org/10.1038/s41746-019-0158-1>.
- <sup>27</sup> Government Technology Agency. (2019, June 7). 3 new ways to partner with GovTech. <https://www.tech.gov.sg/media/technews/3-new-ways-to-partner-with-govtech>.
- <sup>28</sup> APAC News Network. (2021, March 27). Amazon's AWS extending 'Activate' Program to the Social Entrepreneurship startups. <https://apacnewsnetwork.com/2021/03/amazons-aws-extending-activate-program-to-the-social-entrepreneurship-startups/>.
- <sup>29</sup> LaFrenz, C. (2021, September 10). Digital health accelerator targets 25 high-growth companies. *The Australian Financial Review*. <https://www.afr.com/companies/healthcare-and-fitness/andhealth-opens-applications-for-its-flagship-digital-health-program-20210909-p58q7x>.
- <sup>30</sup> New Zealand Government. (2021, November 16). Cloud services. <https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/>.
- <sup>31</sup> Jenkins, S. (2020, July 28). ACSC launches guidance to support safe adoption of cloud services. *The Mandarin*. <https://www.themandarin.com.au/136490-acsc-launches-guidance-to-support-safe-adoption-of-cloud-services/>.
- <sup>32</sup> IRAP. (2020, November). Policy and Procedures. Australian Cyber Security Center. <https://www.cyber.gov.au/sites/default/files/2020-12/IRAP%20Policy%20and%20Procedures.pdf>.
- <sup>33</sup> New Zealand Government. (2021, August 4). Cloud services. Archives New Zealand. <https://archives.govt.nz/manage-information/how-to-manage-your-information/digital/cloud-services>
- <sup>34</sup> Principles for Digital Development. (n.d.). Homepage. <https://digitalprinciples.org/>.
- <sup>35</sup> African Alliance Digital. (n.d.). Digital Health Leadership Program. <https://www.africanalliance.digital/programs-digital-health-leadership-program>.
- <sup>36</sup> Economic Planning Unit, Prime Minister's Department. (2021). Malaysia Digital Economy Blueprint. Malaysia: Economic Planning Unit, Prime Minister's Department. <https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf>.
- <sup>37</sup> Johnston, M. (2019, July 2). Thailand transforms healthcare through Microsoft and AI. *Channel Asia*. <https://www.channelasia.tech/article/663471/thailand-transforms-healthcare-through-microsoft-ai/>
- <sup>38</sup> Charlebois, K., et al. (2016, October 18). The Adoption of Cloud Computing in the Field of Genomics Research: The Influence of Ethical and Legal Issues. *PLoS ONE*, 11 (10). <https://doi.org/10.1371/journal.pone.0164347>.
- <sup>39</sup> AWS healthcare. (2021, July 8). Cloud computing proves key enabler for improved health outcomes. *Healthcare IT News*. <https://www.healthcareitnews.com/news/emea/cloud-computing-proves-key-enabler-improved-health-outcomes>.
- <sup>40</sup> Langmead, B., & Nellore, A. (2018, January 30). Cloud computing as a platform for genomic data analysis and collaboration. *Nature Review Genetics* 19 (4), pg 208-219. doi: 10.1038/nrg.2017.113.
- <sup>41</sup> Asian Development Bank. (2021, September). The Republic of Korea's Coronavirus Disease Pandemic Response and Health System Preparedness. Philippines: Asian Development Bank. <https://www.adb.org/sites/default/files/publication/730201/republic-korea-coronavirus-disease-pandemic-response.pdf>
- <sup>42</sup> Budd, J., et al. (2020). Digital technologies in the public-health response to COVID-19. *Nat Med*, 26 (2020), pg. 1183-1192. <https://doi.org/10.1038/s41591-020-1011-4>.
- <sup>43</sup> Siwicki, B. (2021, November 2). AWS physician expert talks new use cases for telehealth, machine learning, cloud. *Healthcare IT News*. <https://www.healthcareitnews.com/news/aws-physician-expert-talks-new-use-cases-telehealth-machine-learning-cloud>.
- <sup>44</sup> Loh, D. (2020, December 22). Telehealth services rush to relieve ASEAN hospitals' COVID burden. *Nikkei Asia*. <https://asia.nikkei.com/Spotlight/Coronavirus/Telehealth-services-rush-to-relieve-ASEAN-hospitals-COVID-burden>.
- <sup>45</sup> Dudley, J. T., et al. (2010, August 6). Translational bioinformatics in the cloud: an affordable alternative. *Genom Medicine*, 2 (2010), 51. <https://doi.org/10.1186/gm172>.
- <sup>46</sup> Precedence Research. (2020, November 20). Benefits of Cloud Computing for Healthcare. *Channel Asia*. <https://www.channelasia.tech/mediareleases/136310/benefits-of-cloud-computing-for-healthcare/>.

- <sup>47</sup> Amazon Web Services, Inc. (2022). Cloud Computing for Defense. <https://aws.amazon.com/government-education/defense/>.
- <sup>48</sup> Chin, L. V. (2018, July 12). Clinerion and the Precision Medicine-HIS Development Group of Korea University Medical Center Collaborate on Patient-data-driven Solutions for Precision Medicine. Cision PRWeb. <https://www.prweb.com/releases/2018/07/prweb15616573.htm>.
- <sup>49</sup> Raghavan, A., et al. (2021, January 5). Public Health Innovation through Cloud Adoption: A Comparative Analysis of Drivers and Barriers in Japan, South Korea, and Singapore. *International Journal of Environmental Research and Public Health*, 18 (1), p. 334 <https://www.mdpi.com/1660-4601/18/1/334>.
- <sup>50</sup> Robinson, E. (2018, April 27). Apollo Hospitals adopts Microsoft Cloud and AI to improve healthcare. *Technology Record*. <https://www.technologyrecord.com/Article/apollo-hospitals-adopts-microsoft-cloud-and-ai-to-improve-healthcare-68992>.
- <sup>51</sup> Macias, F. & Thomas, G. (2011). *Cloud Computing Advantages in the Public Sector*. United States: Cisco. [https://www.cisco.com/c/dam/en\\_us/solutions/industries/docs/c11-687784\\_cloud\\_omputing\\_wp.pdf](https://www.cisco.com/c/dam/en_us/solutions/industries/docs/c11-687784_cloud_omputing_wp.pdf).
- <sup>52</sup> Salesforce. (2022). Cloud adoption in government: Salesforce drives DCSI service innovation to improve the lives of people with disabilities. <https://www.salesforce.com/ap/customer-success-stories/dcsi/>
- <sup>53</sup> D'hondt, C., et al. (2021). *The cloud imperative in healthcare*. United States: Accenture. [https://www.accenture.com/\\_acnmedia/PDF-145/Accenture-Health-Content-Cloud-Imperative-in-Healthcare.pdf](https://www.accenture.com/_acnmedia/PDF-145/Accenture-Health-Content-Cloud-Imperative-in-Healthcare.pdf).
- <sup>54</sup> Kamani, V. (2019, October 2). 5 Ways Cloud Computing Is Impacting Healthcare. *Health IT Outcomes*. <https://www.healthitoutcomes.com/doc/ways-cloud-computing-is-impacting-healthcare-0001>.
- <sup>55</sup> Dhilawala, A. (2019, March 5). 9 Key Benefits of Cloud Computing in Healthcare. *Galen Data*. <https://www.galendata.com/9-benefits-cloud-computing-healthcare/>.
- <sup>56</sup> Wainstein, L. (2018, June 26). *Cloud-Based Telehealth Defined: Advantages, Applications, and Security*. Arizona Telemedicine Program. <https://telemedicine.arizona.edu/blog/cloud-based-telehealth-defined-advantages-applications-and-security>.
- <sup>57</sup> Krishman, S. (2017, November). *Telemedicine: Decreasing Barriers and Increasing Access to Healthcare*. *Altarum*, 22 (2017). <https://www.healthcarevaluehub.org/advocate-resources/publications/telemedicine-decreasing-barriers-and-increasing-access-healthcare>.
- <sup>58</sup> Collaborate Healthcare P. C. (2022). *Collaborate Health Cloud*. Collaborate247.com. <https://collaborate247.com/>.
- <sup>59</sup> Ponnappalli, S. (n.d.). 7 Examples of Telehealth Used Effectively. *Beam Health*. <https://beam.health/7-examples-of-telehealth-used-effectively/>.
- <sup>60</sup> Integrated Health Information Systems Pte Ltd. (2021). *Smart Health Video Consultation*. IHIS. <https://www.ihis.com.sg/vc>.
- <sup>61</sup> Passemaid, A. (2020, April 9). *Helping contact centers respond rapidly to customer concerns about COVID-19*. Google Cloud. <https://cloud.google.com/blog/products/ai-machine-learning/support-for-contact-centers-during-covid-19>.
- <sup>62</sup> Google Cloud. (n.d.). *Provide secure, continuous patient care*. <https://cloud.google.com/solutions/healthcare-life-sciences/patient-experience>.



**ACCESS**  
health international

| **AWS INSTITUTE**