AWS INSTITUTE

Cloud data governance and best practices for public healthcare cloud adoption 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.

Alvarez & Marsal

Alvarez & Marsal

Alvarez & Marsal ("A&M") is a global consulting firm that offers a broad range of professional services including Operational & Financial Restructuring, Transaction Advisory, Performance Improvement, Valuations, and Disputes & Investigation Services.

Companies, investors, and government entities around the world turn to A&M for leadership, action, and results. Clients select us for our deep expertise and ability to create and deliver practical, rather than theoretical solutions to their unique problems in addition to our objectivity.

The Privacy & Data Compliance Services team at A&M advises and supports leading global and multi-national companies with all aspects of their privacy and data compliance requirements. We work closely with clients to develop and implement award-winning global privacy and data protection frameworks, and manage cross-border data transfer risk, privacy-by-design solutions, and complex data protection impact assessment remediation.

Disclaimer: *Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.*

Table of contents

1. Executive summary

The COVID-19 pandemic has accelerated the adoption of the cloud as a quicker and more cost-effective way of providing healthcare services. Cloud technology has enabled faster innovation without the need for large investments in IT infrastructure and reduced the costs of providing healthcare services. Many cloud service providers operate a pay-as-you-go model, allowing users flexibility to pay only for the resources they need, and offer a wide range of services including infrastructure-as-a-service (laaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS).

Cloud service providers have demonstrated their value to healthcare agencies enabling them to collect and process vast amounts of data, quickly develop and scale applications, and reduce the time required to react to a healthcare crisis and coordinate a nationwide response.

In recent years, countries in the Asia Pacific region have drawn up Cloud First Policies and digitalisation strategies involving cloud in the public healthcare sector. Despite this, cloud adoption across public healthcare in the Asia Pacific region remains low and fragmented, particularly in developing countries. Lack of funding, low understanding of data governance, uncertainty on standards required for cloud adoption, and increasing complexity of data protection laws have contributed to slower levels of cloud adoption[1].

Greater coordination across healthcare stakeholder groups is required to avoid piecemeal implementation of digital health initiatives.

Key recommendations

1. **Align cloud-first strategies with data classification**

- Healthcare authorities should take the lead in aligning cloud-first strategies with existing data classification frameworks to provide greater transparency on types of data that can be moved to the cloud.
- Data classification for healthcare should take a risk-based approach for datasets requiring more robust controls in place. Granular examples and guidance should be illustrated to clearly indicate which cloud model or service provider would be appropriate based on the level of risk involved.
- Support data classification efforts with a risk management framework to healthcare providers on risk factors when adopting the cloud.

2. **Simplify cloud procurement for public healthcare and enable better data exchange**

- Simplify access to cloud services to encourage greater adoption by healthcare agencies. This can be achieved through the creation of panel lists and recognising internationally-accepted cloud accreditations. Alternatives include entering into agreements with cloud service providers at a whole-of-government level to provide better value and management of cloud services.
- Develop clear rules on data sharing and secondary use of data within the healthcare sector to allow greater information exchange and access to medical services and research.

3. **Consider alternatives to data localisation**

- Avoid implementing broad data residency requirements to healthcare data that restrict access to healthcare services and technology. At an international level, there are multiple valid and effective ways to establish security and control over data.
- Alternatives include allowing public sector data to be located offshore, subject to certain requirements, or “whitelisting” countries that provide a sufficient degree of protection for that data.
- Make requirements accountability-based rather than jurisdiction-based to promote free-flow of data across borders. This will ensure that the data owner is responsible for meeting requirements, regardless of where the data is physically stored.

Conclusion

To realise cloud-first strategies, greater coordination across multiple stakeholders in the healthcare sector is needed to develop a good foundation of policies, regulations, and support initiatives. This will in turn increase confidence in cloud services and ease cloud adoption for public healthcare.

Key stakeholders include national policymakers and industry-level public sector agencies to draft the right policies for public healthcare data governance and to implement the data governance framework across the sector. With the right policies and tools, public sector healthcare agencies will be able to unlock the full potential of the cloud to achieve better healthcare outcomes.

[1] *Access Health International and AWS Institute, Overcoming Barriers to Cloud Adoption in Public Healthcare in Asia Pacific.*

2. Introduction

Cloud adoption in the healthcare sector has increased in the last few years. Many governments in the Asia Pacific region are demonstrating a desire to take advantage of cloud services across the public sector. Australia, New Zealand, Singapore, India, Japan, Philippines, and South Korea have adopted “Cloud First Policies” or developed digital health strategies with a cloud component. A Cloud First Policy is part of an overall strategic plan by the government or authority to encourage the use of cloud-based technology. It sets out advantages of using the cloud and ongoing initiatives by the government to promote the use of cloud.

A Cloud First Policy is often the first step governments take to promote the use of the cloud in the public sector. This indicates a willingness by countries in Asia Pacific to seed more cloud initiatives in the region. However, more work needs to be done at national and international levels to avoid fragmented implementation of the cloud in the public healthcare sector, such as increasing trust in cloud services and promoting cloud adoption amongst public healthcare providers.

Many cloud service providers offer a range of compliance and data management tools that can assist with cloud adoption and onboarding. However, countries in the Asia Pacific region are at different stages of their cloud journey. Based on a study conducted by ACCESS International[2], some of the key barriers to cloud adoption in healthcare include insufficient understanding of cloud technology and misconceptions about the privacy and security of cloud-based data, and shortage of technical expertise to effectively implement cloud technology in an evolving regulatory landscape.

The aim of this whitepaper is to understand best practices and frameworks used by countries that have been successful in cloud adoption and provide suggestions on how to approach key challenges as countries in the Asia Pacific region move forward with their cloud journey. Themes explored in this whitepaper are the development of frameworks and policies that offer public healthcare greater access to cloud services, while still providing value and control over data in the cloud.

We began our research by first understanding the current state of cloud adoption, and studying the various cloud frameworks and initiatives by government bodies, with particular emphasis on public sector healthcare in the Asia Pacific region (with reference to countries outside Asia Pacific where relevant). We reviewed available cloud regulations, standards and guidelines to understand the requirements expected from cloud service providers and how those requirements would be implemented. As part of the process, we analysed best practices that have worked for more mature countries and compiled them into a series of recommendations that may serve as a useful reference for countries embarking on their cloud adoption journey.

[2] *Access Health International and AWS Institute, Overcoming Barriers to Cloud Adoption in Public Healthcare in Asia Pacific.*

3. Aligning cloud-first strategies with data classification

What is data classification?

Data classification establishes a set of guiding rules that govern the extent to which data can be accessed, shared, or otherwise used across different environments. It is a key component of good data management and governance. Data classification involves categorising data into different tiers and defining the types of data that would fall in each tier. It establishes security measures, data handling restrictions, and data sharing and access protocols based on the level of sensitivity or impact involved.

Most governments have a version of data classification in place for public sector data. Countries in the Asia Pacific region have adopted different methodologies of data classification for public sector data, often categorised into between three to six tiers based on either sensitivity or impact[3].

Aligning cloud adoption strategies to the data classification framework

When drafting cloud adoption guidelines, public authorities typically focus on information security and governance based on internationally recognised standards such as ISO 27001:2013 or Health Level 7 (HL7), specific to the healthcare industry. However, there has been less discussion on alignment with established public sector data classification frameworks to distinguish between state secret or official information related to national security (usually prohibited from disclosure under official secrets acts or similar legislation) and information that may be owned by a public sector body but may not fall under these categorisations.

To enable greater data use and access to that data by different healthcare providers in the public healthcare ecosystem, countries should avoid classifying healthcare data under highly restricted categories, such as SECRET or TOP SECRET. Restrictive classifications of healthcare data may lead to inadvertent data localisation, which may restrict access to medical services available abroad. Good examples that take a risk-based approach to data classification include the United Kingdom (UK) National Health Service Health and Social Care Cloud Risk Framework[4], and the Singapore Multi-Tier Cloud Security Standard (MTCS)[5]. Classifying health data at a lower level provides greater flexibility but allows stricter requirements to be implemented based on the degree of risk involved.

For example, the UK has three tiers of data classification: OFFICIAL, SECRET and TOP SECRET. The UK classifies up to 90 percent of its public sector data as OFFICIAL, including business, most policy development, legal advice, personal data contracts, statistics, case files and administrative data[6]. This has allowed the UK government to use a wider variety of products and services available on the market, provided appropriate security controls are met.

Greater alignment would be highly beneficial to healthcare providers wishing to adopt cloud services as it would help them understand how different types of data should be treated, and what security and control measures need to be applied to that data.

[3] *As an example, the Republic of Philippines has recently amended their Cloud First Policy to provide clearer instructions on policy coverage, data classification, and data security, as well as its policy on sovereignty, residency, and ownership. Department of Information and Communications Technology, Department Circular 2020-010, Amendments to Department Circular 2017-002 Re: Prescribing the Philippine Government's Cloud First Policy (June 2020), p.9-11.* *https://dict.gov.ph/wp-content/uploads/2020/06/Department_Circular_No_10_Amendments_to_DC_No_2017_002_re_Prescribing.pdf*

[4] *NHS Digital, Health and Social Care Cloud Risk Framework,.* *https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services/cloud-risk-framework*

[5] *IMDA, MTCS Certification Scheme,.* *https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Compliance-and-Certification*

[6] *UK Cabinet Office, Government Security Classifications (May 2018),.* *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf*

Case Callout

UK NHS Health and Social Care Cloud Risk Framework (Data Classification)

The UK National Health Service (NHS) has developed a Health and Social Care Cloud Risk Framework that is specifically targeted to health and social care organisations to help them assess, and take a risk-based approach to, managing data in the cloud.

The framework covers the following considerations as part of its risk model: types of data, scale of data and persistence of data, risk appetite and risk analysis and management. Each of the data types are mapped back to the Government Security Classification Policy that leverages existing general public sector classifications of OFFICAL, SECRET and TOP-SECRET to ensure alignment. It is important to note that in this example, all healthcare data has been labelled as OFFICIAL or OFFICIAL-SENSITIVE, permitting use of accredited cloud services[7].

Type of data	Description	Example	Government security classification
Publicly available information	Statistical material that is intended for public distribution	The number of diabetics in Sheffield, or location information for health-care providers	No mapping/ UNCLASSIFIED
Aggregate data	Summarised and anonymised data, but which is not suitable for public distribution	Summarised records of activity of a particular hospital	OFFICIAL
Personal data	Information about an identified individual	A person's address details and NHS Number	OFFICIAL-SENSITIVE
Pseudonymised data	Sensitive personal data that has been subject to de-identification and/or other privacy-enhancing techniques, in line with the Information Commissioner's Office Anonymisation Code of Practice	Hospital Episode Statistics (HES) data set	OFFICIAL-SENSITIVE

Extracted from the NHS Health and Social Care Cloud Risk Framework[8]

The following are some considerations when classifying healthcare data:

- What outcome needs to be achieved?
- What are the security goals for the intended data?
- What are the dimensions of risk involved – is it based on data type, volume or length of time it is kept?
- What requirements or functionality would help public sector agencies meet required legal or security obligations?
- What available services or products would be able to meet requirements? If so, are additional requirements necessary to meet the data classification tier?
- What is the impact of the data classification on data use and disclosure?

Supplementing data classification with a risk framework

Data classification can be further supported by the development of a risk management framework that would provide additional guidance to healthcare providers on the level of risk involved in a project and the requirements that would need to be met proportionate to the risks. The risk level identified in the risk framework will not change the original data classification assigned to healthcare data.

[7] *Under the Government Security Classifications (May 2018), OFFICIAL information can be managed through accredited service offerings through the G-Cloud programme. Service offerings will be accredited through the UK G-Cloud Information Assurance Requirements and Guidance.*

[8] *NHS Digital, Health and Social Care Cloud Risk Framework, Dimensions that Affect Risk,. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services/cloud-risk-framework/dimensions-that-affect-risk*

Case Callout

UK NHS Health and Social Care Cloud Risk Framework (Risk Framework)

The NHS also considers other dimensions of risk, such as scale of data based on the number of records affected, and volume and the persistency of data (whether data is permanently held in the system for long-term use, for a temporary period of time, or is transient). The NHS allows a degree of risk appetite to be considered. A risk framework tool is provided that assigns a Risk Impact Score value which maps to five different risk profile Levels.

Based on the level of risk presented, the use of public cloud is permitted, subject to acquiring the necessary levels of approval by the respective stakeholder groups in the NHS. For risk profiles Class IV and V (see table below), a balancing exercise is conducted to understand if the benefits of using public cloud would be justified, and recommendations can be provided to address available risks.

Risk Profile Level	Governance expectation
Class I	All organisations are expected to be comfortable operating services at this level.
Class II	Whilst there may be some concerns over public perception and lock-in, most organisations are expected to be comfortable operating services at this level.
Class III	At this level, risks associated with impact of breach become more significant, and the use of services at this level therefore requires specific risk management across all risk classes, and requiring approval by Chief Information Officer (CIO)/Caldicott Guardian level.
Class IV	At this level, it is likely to become more difficult to justify that the benefits of the use of public cloud outweigh the risks. However, this case may still be made, requiring approval by CIO/Caldicott Guardian, and would be required to be made visible to the organisation's board. Specific advice and guidance may be provided by NHS Digital on request.
Class V	Operating services at this level would require board-level organisational commitment, following specific advice and guidance from NHS Digital.

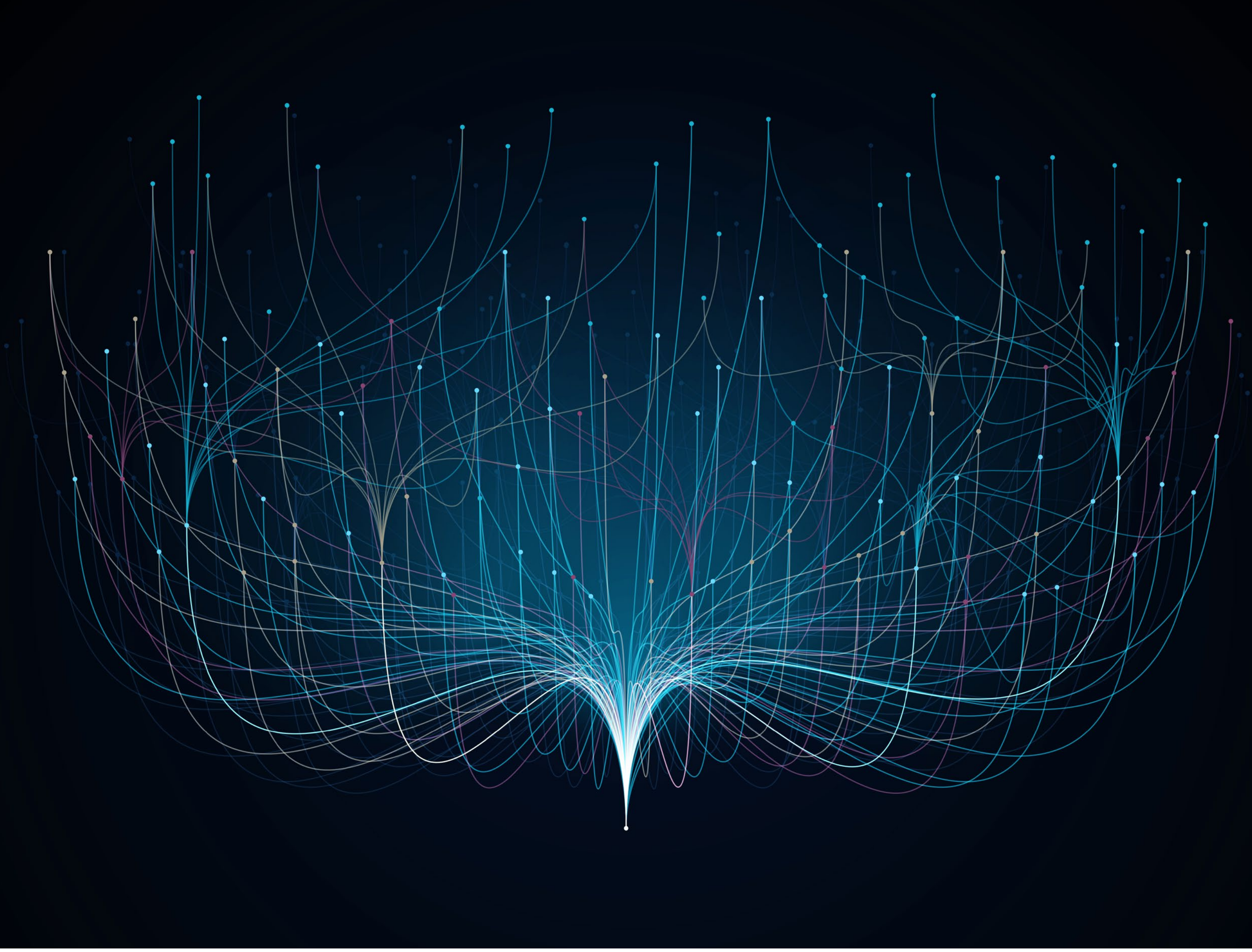
Source: NHS Health and Social Care Cloud Risk Framework[9]

The NHS Cloud Framework forms a coherent step-by-step model that requires healthcare providers to consider the types of data involved, the dimensions of risk that may affect the data and finally, provide guidance on risk levels and requirements to use cloud services. This has enabled the UK NHS to use the cloud as part of its healthcare initiatives.

When developing a risk framework, information technology requirements should be kept neutral to provide access and flexibility to a greater pool of providers. The higher the risk, the greater the requirements that should be in place to meet stricter industry requirements. Larger-scale, sensitive government projects processing large volumes of data may require approval and agreement across different government agencies, possibly requiring higher-level clearance and specific bespoke arrangements.

For complex cloud projects, a phased approach to cloud adoption may be beneficial. This could focus initially on lower-level and lower-risk cloud migration to monitor effectiveness and risk levels, and then use experience gained to work around challenges associated with higher-level and higher-risk data classifications.

[9] *NHS Digital, Health and Social Care Cloud Risk Framework, Risk analysis and management,. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services/cloud-risk-framework/risk-framework*



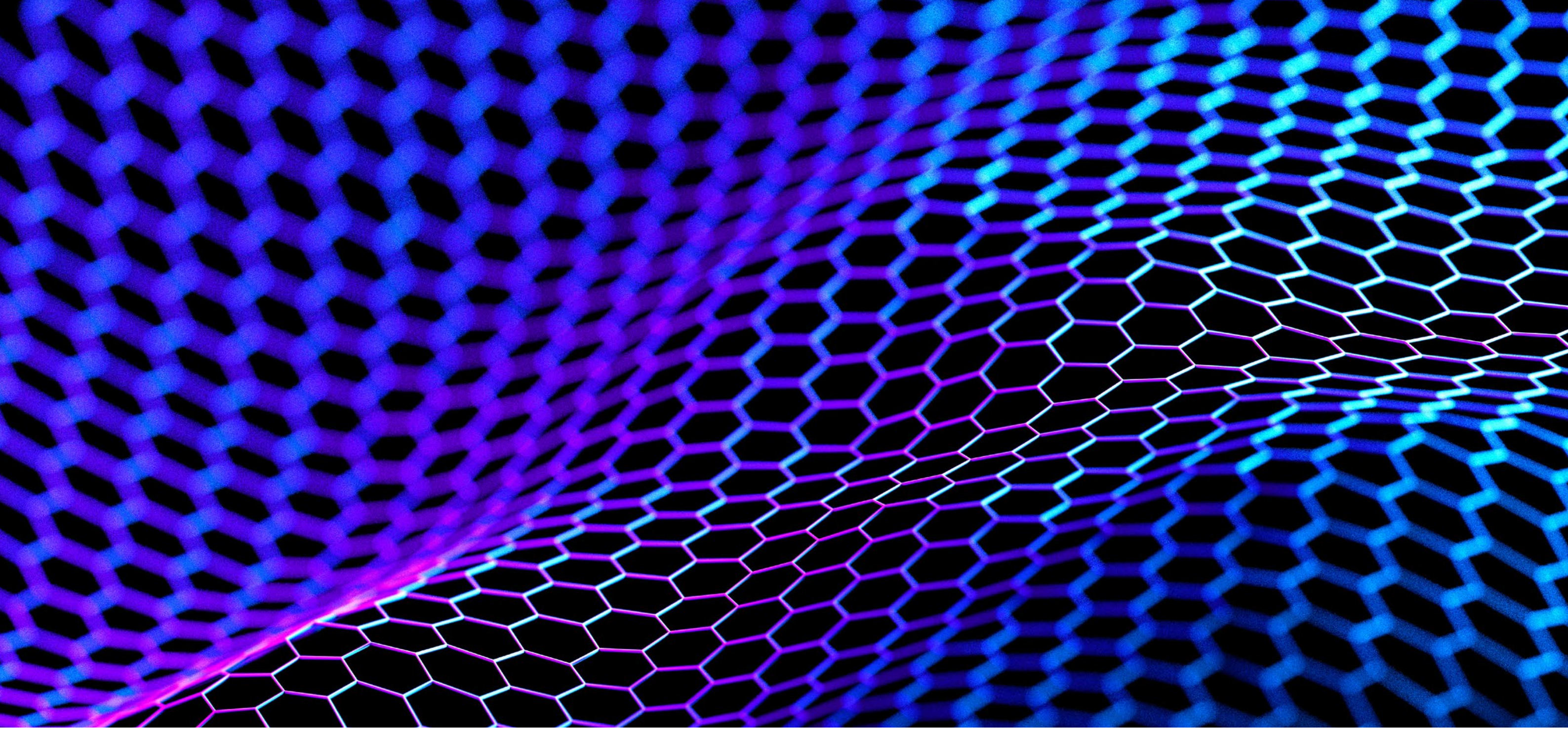
Key takeaways

Align cloud adoption strategies to the data classification framework

- When classifying healthcare data, policymakers should carefully consider data classification tiers and balance the benefits of appropriate data security against the interests of greater public health.
- An overly conservative approach to data classification for healthcare data could restrict data from being hosted in available cloud environments, and limit sharing with third-party providers, requiring increased investment in infrastructure and ongoing maintenance, and indirectly increasing the cost of public healthcare.
- The alignment of cloud requirements or standards against types of data that can be processed in a cloud, which in turn are mapped to specific requirements (e.g. certification required) would provide greater guidance and clarity to healthcare agencies when selecting cloud vendors.

Supplement data classification with a risk framework

- A risk framework that considers different dimensions of risk would provide greater assistance on the factors that need to be considered. Some dimensions of risk include type and sensitivity of data, volume of data, and persistence of data (how long the data is kept).
- For each data classification category, determine the minimum level of requirements needed to process that data and any conditions for using cloud services. This can require meeting security requirements, certification requirements, or approval requirements by relevant stakeholders.



4. Developing a framework to ease cloud adoption and facilitate data exchange

Leveraging the power of the cloud for public healthcare

Cloud adoption in the public sector can be improved by providing the right tools and support from a central level (initiatives led by government or healthcare authorities) to establish clear requirements for cloud adoption and to ease the cloud procurement process. Lack of coordination may result in negotiating cloud contracts on a case-by-case basis, duplicating efforts to onboard the same provider and multiple risk assessments against the same cloud provider for different projects.

Clear rules on data sharing and secondary use of data (in the cloud or otherwise) are needed to provide greater guidance on the limits of data sharing, and conditions required to process the data. Health data processing has advanced significantly. We now have an increasing number of players involved in processing the same patient's data from the doctor to pharmacist, medical device manufacturers, testing facilities, research organisations and patient aftercare.

Cloud technical skills and awareness of cloud technology should be improved to allow healthcare providers to set up the cloud in a way that meets their compliance needs.

Simplify procurement requirements for cloud services

Streamlining the procurement requirements for cloud services through a framework of interconnecting requirements would significantly improve cloud adoption in public healthcare. Based on a study of best practices adopted by countries in the Asia Pacific region, effective cloud services procurement processes include:

- **Recognised certifications and accreditations:** This can take the form of internationally recognised or approved standards, certifications or accreditations across a number of desired areas, including information management, data governance, availability, expected service levels, and security[10].

  There are a number of internationally accepted standards that are independently validated by third-party organisations such as the International Organization for Standardization (ISO) and the Cloud Security Alliance. Specific to healthcare, the United States (US) requires compliance with its Health Insurance Portability and Accountability Act (HIPAA), which sets baseline standards that need to be in place for the protection of health information.

[10] *There are a number of generally recognised industry standards used in practice, including the ISO/IEC 27001: 2013 and Health Level Seven (HL7) Healthcare Privacy and Security Classification System (HCS) which provide guidance and recommendations for data owners to assess the data they hold and the level of protection that should be assigned to it.*

Case Callout

US HIPAA

The US HIPAA requires covered entities (designated healthcare providers) to put in place technical, physical, and administrative safeguards for protected health information (PHI). HIPAA was further supplemented by the Privacy Rule and the Security Rule, which established national standards for the protection of health information[11].

HIPAA does not expressly prohibit storage or processing of PHI outside of the US but instead mandates meeting required security and privacy requirements. HIPAA permits the use of cloud services to store and process PHI provided HIPAA requirements are met .

HIPAA certifications for products and services help healthcare providers understand if a particular product can meet a particular industry standard when selecting an appropriate service provider. As a result, we have seen a number of HIPAA-compliant services that allow both the public and private sectors to use available services that comply with requirements.

Public-sector agencies should consider adopting existing standards and adding supplementary requirements where necessary rather than developing a completely new set of national standards. This will allow cloud service providers to demonstrate their ability to meet requirements and reduce duplication of audits, onboarding time and costs. Services may be independently assessed by appointed third parties or a specific department of the government ministry.

- **Creation of public sector or industry-specific panels:** An accredited panel list of cloud service providers helps reduce administrative burden and duplication by public sector agencies. Service providers can be pre-screened centrally to ensure they meet minimum requirements, reducing the lead time to contract providers who are part of the panel. This process can be further enhanced by the creation of industry-specific panel lists specifically for healthcare.

Case Callout

Australia's Cloud Marketplace

The Australian Digital Transformation Agency (DTA) has established a Cloud Marketplace where buyers and sellers can provide various services to the Australian government. The new Cloud Marketplace embraces digitalisation and promotes cloud adoption in line with its Secure Cloud Strategy to use public cloud services as the default[15].

The Cloud Marketplace includes more than 300 providers consisting of small-to-medium enterprises (SME), start-up companies and global providers. Cloud offerings are grouped into two categories, cloud consulting professional services and cloud services that include information and communication technology (ICT) capabilities. A list of recognised cloud service providers can be found through the Australian Tender platform[16], serving as a panel list for government agencies to choose from if they wish to use cloud services.

To apply for the marketplace, sellers would need to apply to be admitted to the panel list and undergo an evaluation by the Australian DTA. The panel list is composed of evaluated sellers that are able to offer pre-approved services and products to the Australian government[17].

- **A set of pre-negotiated terms with major service provides:** We have recently seen whole-of-government contracts entered into between cloud service providers and governments. Government agencies, including healthcare service providers, would benefit from a set of pre-negotiated terms with major cloud service providers. Pre-negotiated terms would enable governments to reuse existing contractual templates and services without the need to re-negotiate the entirety of the terms for each individual initiative.
- Consolidated whole-of-government arrangements have recently increased in popularity as they provide greater bargaining power and control in negotiations with cloud service providers. Such arrangements would provide governments with one main point of contact with service providers to ensure alignment of terms and services across a wider part of the public sector. Some examples of countries with arrangements in place include Australia, New Zealand, Singapore, the United Kingdom and Malaysia.

[11] *US Department of Health and Human Services (HHS), The HIPAA Privacy Rule,. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html*

[12] *HHS.gov, Guidance on HIPAA and Cloud Computing,. https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html*

[13] *Australia's Digital Transformation Agency, DTA launches new Cloud Marketplace,. https://www.dta.gov.au/news/dta-launches-new-cloud-marketplace*

[14] *Australia's Digital Transformation Agency, DTA launches new Cloud Marketplace,. https://www.dta.gov.au/news/dta-launches-new-cloud-marketplace*

[15] *Digital Transformation Agency, Secure Cloud Strategy, updated 2021 (p.13)*

[16] *Australian Government, Aus Tender,. https://www.tenders.gov.au/Son/Show/7b3c8f4e-4638-452d-8b3d-6f2f41ece41d*

[17] *Australian Government, Buy ICT,. https://www.buyict.gov.au/sp?id=seller_getting_started*

Case Callout

UK's One Government Cloud Strategy

The United Kingdom, as part of its One Government Cloud Strategy, has developed Cross-Departmental Memorandums of Understanding (MoU) with selected cloud service providers[18]. The MoU aims to maximize the value of government spending with cloud service providers by setting out special terms and pricing for cloud products and services that will be available to all public sector organisations.

The benefit of such an arrangement is that the cloud provider will view the government as a single customer with multiple points of purchase and consumption, enabling the government to receive larger discounts based on their spending commitments. As part of the MoU arrangement, the parties will agree to baseline commercial, technical, security and legal principles which will be applicable across the services.

Establishing a robust cloud adoption framework at a central government or industry level will remove some of the administrative and technical burdens on healthcare providers and provide greater access to cloud services.

Establish clear rules on data sharing and any secondary use of data

As part of overall healthcare data governance, it is important to establish data-sharing rules and requirements between different stakeholder groups in the healthcare network. Healthcare agencies are responsible for the configuration and compliance setup of that data within the cloud and should be provided clear guidance on the extent to which patient data can be used and shared within the public sector ecosystem.

The primary purpose for using and sharing health data is often clear—to provide treatment to the patient. However, as healthcare environments become more complex, with multiple parties processing the same patient's data, the lines between primary and secondary uses of data may become blurred. This may make it difficult for the data user to determine if patient consent is required to collect and use that data, and who in the healthcare chain is responsible for providing the appropriate notices and obtaining that patient's consent.

According to a whitepaper published by the National University of Singapore and Precision Public Health Asia Society[19], a data-sharing framework requires collaboration between multiple stakeholders and requires the creation of (i) a data-sharing strategy, (ii) technical and technological capacity, (iii) regulatory and legal capacity, and (iv) an approach to operationalising data sharing.

While this is still an emerging area, key components of health data-sharing frameworks include:

- Providing transparency to the individual about the use of data and any secondary uses of that data
- Ensuring there are clear processes and procedures in place to request and access data
- Requiring approvals for ethical data use through an independent board or appointed committee
- Setting clear requirements and standards for the de-identification of data
- Ensuring data quality and availability standards are met
- Developing interoperability standards to enable quality data exchange between public and private health systems
- Establishing security requirements to facilitate the secure exchange of data to other members within the public healthcare ecosystem

When developing a data-sharing framework, there is a need to understand common types of data used in public health and research, the extent of data sharing taking place today and the wider goals and aims of future digital health initiatives. Data users would benefit from clear rules around types of data sharing that would be permitted, and any associated limitations to ensure that the respective environments and systems are appropriately configured in line with the data-sharing framework.

Privacy considerations around appropriate use and transparency requirements should also be taken into account as part of this process. Transparency, trust and responsible data sharing are keywords often used when promoting secondary use of healthcare data. A large part of this involves being upfront with patients about how their data will be used and giving them a choice.

From an operational perspective, consent management and privacy notification requirements may be managed through centralised key systems and processes (e.g. eHealth record repositories which are the main collection points of patient data). Access rights can be granted to individual providers on a need-to-know basis, and privacy notices and consent can then be collected centrally. This will allow patients to manage their data in one place rather than through a confusing network of individual health providers. Organisations will also be able to better manage user requests when individuals exercise their rights over their data.

[18] *Gov.uk, Cross-Departmental Memorandums of Understanding,. https://www.gov.uk/guidance/cross-departmental-memorandums-of-understanding*

[19] *National University of Singapore and Precision Public Health Asia Society, Whitepaper on Responsible Data Sharing in Health and Healthcare*

Most cloud service providers offer a suite of compliance tools that map back to existing best practice requirements that may be utilised to manage the data in accordance with the data-sharing framework. Requirements from health data-sharing frameworks can be shared with cloud service providers to provide technical assistance on implementing the appropriate back-end functionality and controls needed to manage that data within the cloud environment.

Increase awareness of cloud technology and functionality

Healthcare providers are ultimately responsible for the data entered into the cloud. Therefore, it is important that each party using the cloud understands how to use data management tools and configure the appropriate settings in the cloud.

For example, a cloud service provider would provide the functionality to manage patient consent in an app or platform, but it is ultimately up to the cloud user (i.e. healthcare provider) to set their own consent management policies and collect patient consent in line with industry guidelines and regulatory requirements.

When working with cloud service providers, healthcare providers should understand the Shared Responsibility Model[20] and their own role in managing access, security, data handling, and configuration of the cloud service to achieve the desired outcome. The roles and responsibilities of each party may change, depending on the type of cloud service used (i.e. SaaS, PaaS and IaaS), and it is critical that these are clearly set out in contracts and business process documentation to ensure that any gaps are appropriately handled by an assigned party.

Healthcare authorities should encourage education programmes on cloud skills from a compliance and security perspective. Cloud courses and training will increase awareness of cloud benefits and how to utilise the cloud to increase efficiency or drive innovation.

The following is an example of how good cloud adoption and data-sharing frameworks enable greater and faster healthcare innovation.

Case Callout

Genomics England

Genomics England (GEL), wholly owned by the UK Department of Health and Social Care, recently worked in partnership with the GenOMICC consortium to analyse whole genome sequences of 20,000 people who have been severely affected by COVID-19 and compare them to 15,000 other genomes from people who were mildly affected or had no symptoms[21]. This success closely followed GEL's previous project to sequence 100,000 genomes from NHS patients and families with rare diseases and common cancers to identify disease-causing regions of the genome.

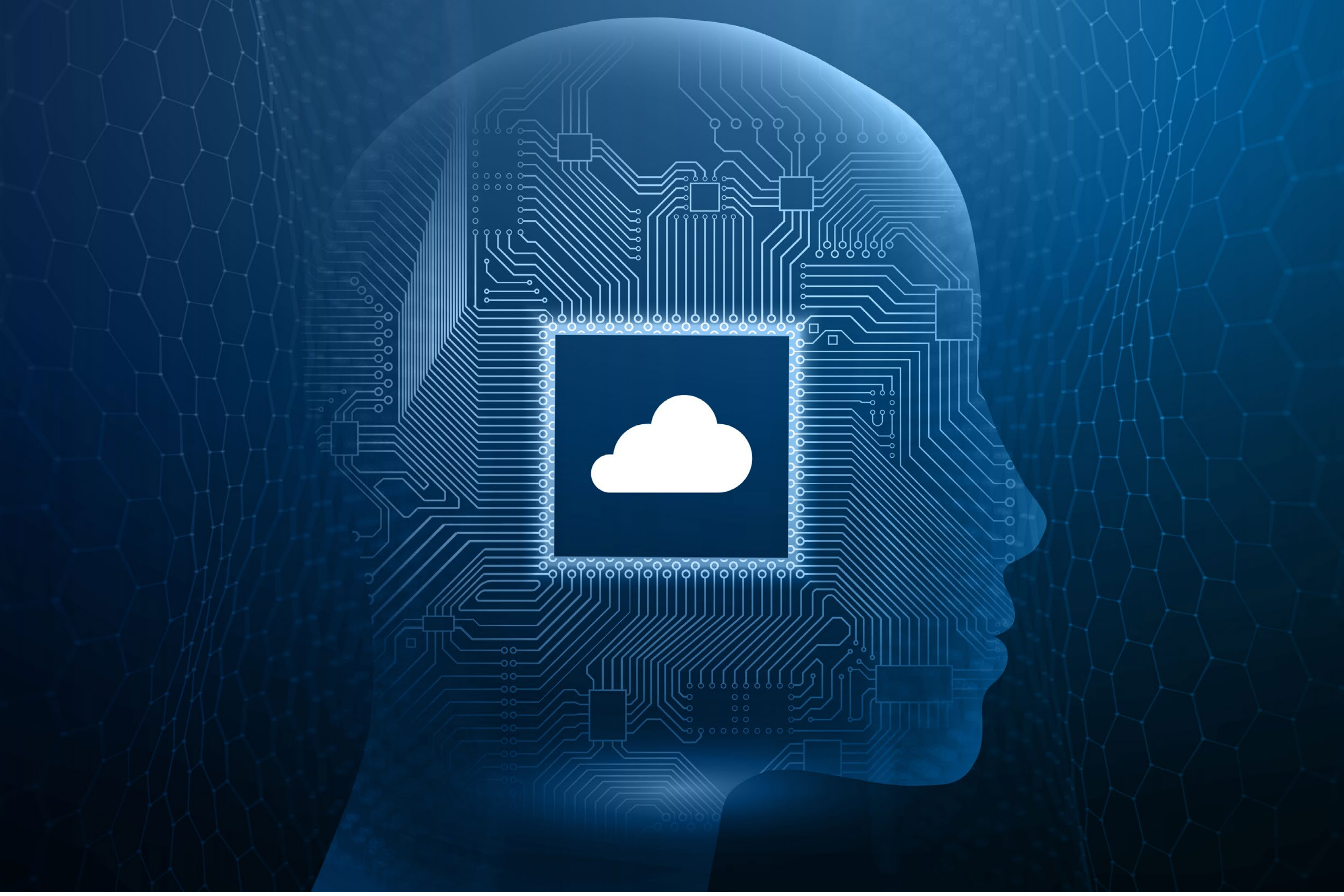
GEL partnered with AWS and Lifebit to create a trusted research environment that allowed researchers to utilise advanced cloud computing tools to deliver data-driven healthcare and glean better insights from genomic research. AWS tools provided researchers with reliable, comprehensive and privacy-compliant access to these datasets and made data more accessible to the medical community[22]. Through secure collaboration and analysis, this initiative will inform better cancer diagnosis, drive drug development, and enable precision medicine.

The project involved migrating petabytes of genomic data from on-premise research environments to AWS, and enabled the processing of large-scale datasets on a pay-as-you-go basis. This was ideal for academic and government-funded research because it allowed for flexibility to accommodate fluctuations in grant funding.

[20] *A Shared Responsibility Model sets out the roles and responsibilities between the cloud service provider and cloud. This may include security, compliance and risks.*

[21] *Genomics England, COVID-19 study,. https://www.genomicsengland.co.uk/initiatives/covid-19*

[22] *AWS, Genomics England Develops Genomic and Health Information Platform on AWS to Turn Science into Healthcare,. https://aws.amazon.com/solutions/case-studies/genomics-england/*



Key takeaways

Simplify the procurement process by streamlining requirements for cloud adoption

- Develop clear certification and accreditation mechanisms using internationally accepted standards. Requirements can be independently validated by a designated third-party.
- Create a panel list of cloud service providers (or a marketplace where government agencies can select and purchase cloud services) to simplify the procurement process.
- Consider pre-negotiated terms with major service providers to streamline agreement of contractual terms for better value during the negotiation process. This will allow agencies to re-use cloud services and products that have been onboarded, and reduce administrative duplication.

Establish clear rules on data sharing and any secondary use of data

- Establish clear rules to govern data sharing amongst different healthcare providers to ensure controls and compliance requirements are set up adequately in the cloud (or other) environments.
- Address privacy and transparency requirements to make sure individuals understand how their data will be used and are provided a choice.
- Cloud users will need to work with cloud service providers to translate data sharing requirements into technical controls to manage data in the cloud.

Increase awareness of cloud technology and functionality of cloud users

- Cloud users should understand the Shared Responsibility Model and the roles and responsibilities of each party over the data.
- Cloud users should be provided additional training on cloud technology and functionality to ensure that they can appropriately configure the cloud to their requirements.

5. Tackling common challenges of data localisation

Balancing between data localisation and greater access to medical health

Cloud services enable data to be used faster and shared more readily across borders. Healthcare authorities and policymakers should carefully balance the benefits of cross-border data sharing for greater access to medical services against security and localisation requirements.

Requiring data to be hosted and processed locally can result in loss of certain cloud benefits, including the ability to scale quickly and dynamically, provide high levels of service, and cost-effectiveness. Strict localisation may also impair both business and government continuity plans, resulting in critical government functions and institutions not being able to operate during a national emergency, such as war[23] or major natural disasters. Data localisation also may stifle innovation and research opportunities due to the requirement to have infrastructure located onshore and increase overall infrastructure costs.

Barriers to free flow of data should be tackled at multiple levels. This section attempts to provide best practice recommendations at a policy level as well as some approaches that healthcare providers may consider in the interim.

Tackling data localisation at a national and international level

A number of jurisdictions have begun to explore offshore options that provide them with a sufficient degree of assurance that the data will be kept secure at a satisfactory level:

- The **Philippines** have amended their data sovereignty and data residency requirements in their Cloud First Policy to state that all data owned by the Philippine government located in the cloud, regardless of location, shall be governed by Philippine laws, policies, rules and regulations. The Philippines lifted residency restrictions on government data stored or processed in the cloud with the exception of certain data classification categories involving sensitive government data.

- **Singapore** permits data transfers of healthcare data under the Singapore Personal Data Protection Act 2012 (PDPA), Personal Data Protection Regulations (PDPR) and Advisory Guidelines for the Healthcare Sector. Data transfer of healthcare data is permitted if the recipient of personal data is bound by legally enforceable obligations to provide the transferred personal data a standard of protection comparable to the PDPA.

- The **UK NHS** permits personal confidential data to be hosted in countries that provide an adequate level of protection for personal data. NHS and social care providers may use cloud computing services to host NHS data within the UK, the European Economic Area (EEA), or a country deemed adequate by the UK..

Based on our research, we have seen practices and recommendations capable of achieving a pragmatic balance between data residency and data exchange:

- Create carve outs and exemptions. Governments should work with public sector healthcare agencies to take a risk-based data classification approach and carefully balance the trade offs and benefits of more accessible public healthcare against security and control of the data. Imposing data localisation on healthcare data should be avoided as it would impose extremely strict requirements which would have an adverse impact on costs and risk losing the benefits of data exchange.

  If alternatives do not provide a sufficient standard of assurance and data localisation is required, possible exceptions for offshore processing of healthcare data should be identified, with clear requirements specified for instances when data can be sent offshore. The ultimate goal is to establish a sufficiently robust health data sharing and transfer framework based on the level of risk involved rather than relying on data localisation.

[23] *Amazon, AWS employees help secure vital data so the Ukrainian government, education, and banking institutions can continue to serve Ukrainian people,. https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future*

Case Callout

UAE Health Data Exceptions

The United Arab Emirates (UAE), through Ministerial Resolution 51/2021, has created exceptions to Article 13 of the Health Data Law[24] which permit specific types of health data to be processed offshore, including when the patient provides their consent or where it is used for:

- Scientific research
- Insurance claims and management
- Medical samples sent abroad
- Processing by medical devices
- Pharmacovigilance activities
- Providing remote health services

The exceptions clarify the types of data that can be transferred, as well as the conditions required to transfer the data.

- **Increase participation in certification frameworks that allow data transfers to occur between member countries.** There are a number of data transfer frameworks that allow for the free flow of data between member states. These include EU adequacy decisions for non-EU countries deemed to provide an adequate level of protection, and the Cross-Border Privacy Rules (CBPR) endorsed by the Asia Pacific Economic Cooperation (APEC). Recent developments indicate the formation of a Global CBPR Forum[25], which seeks to include non-APEC members and to enhance interoperability across different data protection and privacy frameworks.

- **Create whitelists of countries where data transfer would be permitted.** Whitelisted countries may be those assessed to have equivalent or higher standards of data protection, or where certain international cooperation agreements or digital trade agreements allow transfers of data between two or more countries[26]. Many of these agreements typically promote the free flow of data between countries. Some countries have actively prohibited data localisation as being detrimental to free trade.

Interim measures for public healthcare providers

Without the appropriate support and tools at a national and industry level, it may be challenging for individual healthcare providers to attempt cross-border data transfers if there are strict requirements on localisation. While we await further developments on cross-border data sharing, healthcare providers may consider some of the following when carrying out cross-border cloud initiatives:

- **Conduct a risk assessment before transferring data abroad.** Begin with an assessment of relevant laws on data privacy and regulations published by healthcare authorities on transferring data abroad to identify if there are any exceptions that allow data transfer. If there are exceptions, perform a privacy and security assessment to identify necessary compliance controls to transfer the data in accordance with requirements.

- **Consider utilising privacy enhancing technologies to de-identify data.** There are technological tools that can be used to de-identify patient personal data to reduce risks to the individual if the data is misused. Most health research today is conducted on de-identified or partially de-identified data. This can be achieved through basic de-identification techniques, such as data redaction and aggregation, or through more technical means such as hashing.

  Recent technological breakthroughs in this space include multi-party computing, homomorphic encryption and federated learning. These technologies permit machine learning or analysis of the data without privacy loss. Some of these new solutions allow data processing within their existing environments and a variety of cryptography techniques can be applied to this process to ensure that a certain outcome is achieved without requiring data sharing between parties. This may allow data analytics to be performed without data leaving the environment.

- **Seek advice and assistance from your healthcare regulator.** Initiate discussions with local health regulators where data localisation restrictions may impede effectiveness and speed of healthcare services. Healthcare authorities may offer alternative workarounds that meet requirements. In some circumstances, regulatory approval can be obtained to permit the cross-border data transfer, however this may take time as it will be subject to regulatory scrutiny.

[24] *AUAE Cabinet, Health Data Law (Arabic),. https://laws.uaecabinet.ae/ar/materials/law/1209*

[25] *US Department of Commerce, Statement on the Establishment of the Global CBPR Forum,. https://www.commerce.gov/news/press-releases/2022/04/statement-commerce-secretary-raimondo-establishment-global-cross-border*

[26] *An example of this is the Australia-Singapore Digital Economy Agreement that allow cross-border data flows between Australia and Singapore for business purposes, including in the financial sector. Businesses will not be required to build data storage centres as a condition of conducting business.*

Key takeaways

Tackle data localisation at a national/international level

- Avoid implementing broad data residency requirements for healthcare data that restrict access to healthcare services and technology. If data must be localised, exemptions for offshore processing of healthcare data should be clearly identified and permitted, subject to clear requirements.
- Increase participation in certification frameworks that promote data transfers between member countries that meet requirements or consider whitelists of countries to which data transfer would be permitted.

Interim measures for public healthcare providers

- Conduct a risk assessment before transferring data. To identify any exceptions that would permit the data transfer, healthcare providers should carefully assess relevant privacy laws and regulations, and perform privacy and security assessments.
- Consider utilising privacy enhancing technologies to de-identify data and reduce risks arising from transfers. Certain privacy enhancing technologies allow data analytics to be carried out on the data without requiring data sharing or data leaving the environment.
- Seek advice and assistance from your local healthcare regulator to discuss potential solutions and workarounds. Consider if regulatory approval may be required to permit cross-border data transfers where other options have been exhausted.

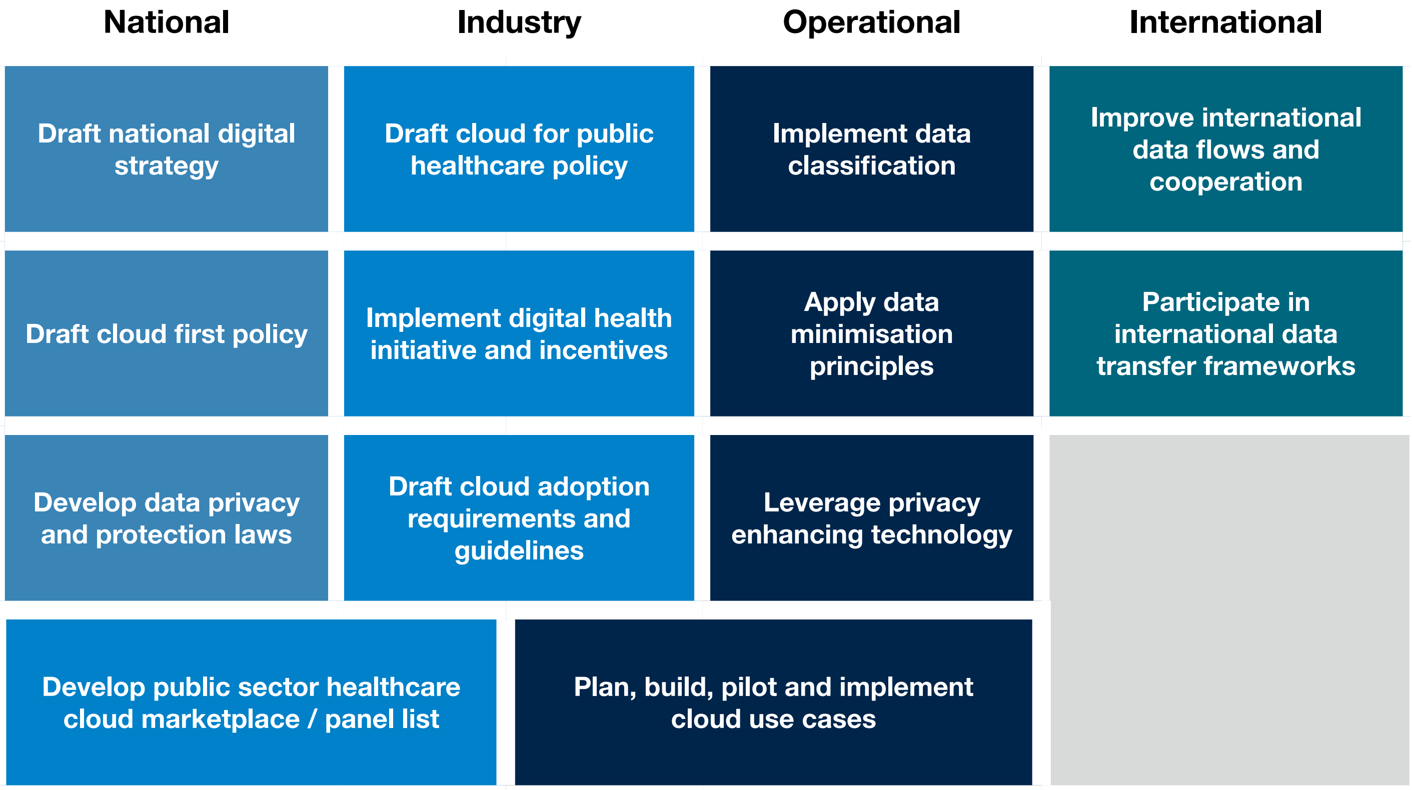
6. Conclusion

The cloud has the potential to improve healthcare outcomes by allowing greater and faster health innovation, reduce waiting time and lower healthcare costs. Improving the rate of cloud adoption in healthcare requires collaboration and coordination across multiple stakeholder groups from policymakers, healthcare authorities and healthcare providers in the public and private sector.

Developing countries beginning their cloud journey could benefit from the development of a roadmap towards cloud adoption to coordinate multiple stakeholder groups and avoid fragmented implementation of cloud initiatives.

At a national level, cloud adoption should be driven by an overarching national digital strategy and Cloud First Policy. Healthcare authorities should be empowered to initiate and implement digital health projects and be provided incentives for cloud adoption. Platforms or panel lists of cloud service providers should be established to simplify the selection and onboarding process for healthcare organisations.

At an operational level, healthcare providers need to work with healthcare authorities to plan, build and pilot cloud use cases. Pain points and challenges that are barriers to cloud adoption should be raised and discussed in a common forum. In parallel, countries should consider data flows at an international level and utilise international mechanisms that meet requirements and allow data sharing between trusted countries.



National	Industry	Operational	International
Draft national digital strategy	Draft cloud for public healthcare policy	Implement data classification	Improve international data flows and cooperation
Draft cloud first policy	Implement digital health initiative and incentives	Apply data minimisation principles	Participate in international data transfer frameworks
Develop data privacy and protection laws	Draft cloud adoption requirements and guidelines	Leverage privacy enhancing technology	
Develop public sector healthcare cloud marketplace / panel list		Plan, build, pilot and implement cloud use cases	

Illustrative Cloud Adoption Roadmap

A coordinated cloud adoption strategy with different sections of government collaborating on an overarching plan can result in tangible benefits and outcomes, including more coordinated infrastructure and cost savings. An example of a cloud adoption strategy with different sections of the government working in parallel towards an overarching plan can be seen below.

Case Callout

Singapore Cloud Strategy

In late 2018, as part of its Smart Nation Strategy, the Singapore government adopted a Cloud First Policy and announced a five-year plan to migrate most of its Information and Communications Technology (ICT) systems from on-premises infrastructure to commercial cloud platforms to accelerate service delivery and improve services for citizens and businesses[27]. The initiative aimed to homogenise the onboarding of multiple government agencies to the cloud, including workload administration, account and billing management, secure access, and compliance with governance policies.

It established a five-year roadmap to improve the onboarding process and is transitioning from Government on Commercial Cloud (GCC) 1.0 to GCC 2.0, which will be used as a whole-of-government platform along with the Singapore Government Tech Stack for modern app development by the government.

The Singapore government is currently migrating less sensitive government Information and ICT systems onto the commercial cloud, to allow the use of leading-edge private sector capabilities to develop digital services. A small number of very sensitive and critical systems will remain hosted within government infrastructure, even as the global norm is increasingly for ICT systems to be cloud base[28]. According to the roadmap on their website for 2023 and beyond[29], Singapore targets hosting 70 percent of eligible government systems on the commercial cloud.

In parallel, the Infocomm Media Development Authority (IMDA) launched the MTCS (Multi-Tier Cloud Security Standard) which is mapped to the Ministry of Health's (MOH) Healthcare IT Security Policy & Standards (HITSecP). Vendors who successfully qualify for the MTCS certifications are published on the IMDA website and healthcare providers can easily select cloud service providers that possess the necessary MTCS certification[30].

The MTCS is developed based on the Singapore Standard SS 584 Specification for multi-tiered cloud computing security and ties back to internationally recognised ISO 27001 standards. The MTCS certification is undertaken by accredited certification bodies and is valid for three years subject to annual audit.

The following MTCS Levels have been mapped to the MOH's HITSecP. This has helped bring further clarity to public healthcare providers on which type of cloud can be used based on the different levels of MTCS certification[31].

MTCS Levels	Application/System Types	Data
L3	Clinical and patient administrative support systems	Patient electronic, medical and health records, including diagnosis, medication prescriptions, billing and admissions, patient-generated health information
L2	IT enterprise support and administration systems	Operational data including employee information, medication inventory and purchase management
L1	Public information systems	Publicly available information including informational websites, clinical standards and terminology systems, medical practitioners' registries

Source: IMDA's MTCS SS factsheet[32]

[27] *Singapore Government Developer Portal,. https://www.developer.tech.gov.sg/products/categories/infrastructure-and-hosting/government-on-commercial-cloud/overview.html#:~:text=What%20is%20GCC%3F,Amazon%2C%20Microsoft%2C%20and%20Google*

[28] *CODEX: Re-engineering the Government's Digital Infrastructure (smartnation.gov.sg), commercial-cloud-factsheet.pdf (smartnation.gov.sg)*

[29] *Smart Nation Singapore, Digital Government,. https://www.smartnation.gov.sg/about-smart-nation/digital-government#the-progress-so-far*

[30] *Singapore IMDA, Compliance and Certification,. https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Compliance-and-Certification*

[31] *Singapore IMDA, 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*

[32] *IMDA MTCS SS Factsheet,. https://www.imda.gov.sg/-/media/Imda/Files/Industry-Development/Infrastructure/mtcs/MTCS-FactSheet-May-2016-FINAL.pdf*

Underpinning this framework, Singapore has established clear laws and regulations on data protection and privacy through the PDPA which covers healthcare data. Singapore has also actively participated in data transfer certification frameworks that promote cross-border data flows, such as the APEC CBPR[34].

As a result, Singapore is one of the most advanced countries in the region for healthcare cloud adoption.

[34]. IMDA, APEC Cross Border Privacy Rules (CBPR) System, https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification

7. Acknowledgements

Amazon Web Services

Project Advisors

Agne Makauskaite
Head of Public Policy for Regulated Industries, APJ

Annabel Lee
Director, Digital Policy (APJ) and ASEAN Affairs

Andrew Wiltshire
Healthcare Policy Lead, APJ

Nicola Murphy
International Government Health, AWS

Monique Viengkhou
APJ Lead, AWS Institute

Alvarez & Marsal

Privacy & Data Compliance Services

Robert Grosvenor
Managing Director

Matthew Negus
Senior Director

Nicole Chee
Senior Manager

Hassan El-Rashidy
Associate

February 2023

ABOUT AMAZON WEB SERVICES

For over 15 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud offering. AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 200 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 96 Availability Zones within 30 geographic regions, with announced plans for 15 more Availability Zones and five more AWS Regions in Australia, Canada, Israel, New Zealand, and Thailand. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs.

To learn more about AWS, visit **aws.amazon.com**

ABOUT ALVAREZ & MARSAL

Companies, investors and government entities around the world turn to Alvarez & Marsal (A&M) for leadership, action and results. Privately held since its founding in 1983, A&M is a leading global professional services firm that provides advisory, business performance improvement and turnaround management services. When conventional approaches are not enough to create transformation and drive change, clients seek our deep expertise and ability to deliver practical solutions to their unique problems.

With over 7,000 people across five continents, we deliver tangible results for corporates, boards, private equity firms, law firms and government agencies facing complex challenges. Our senior leaders, and their teams, leverage A&M's restructuring heritage to help companies act decisively, catapult growth and accelerate results. We are experienced operators, world-class consultants, former regulators and industry authorities with a shared commitment to telling clients what's really needed for turning change into a strategic business asset, managing risk and unlocking value at every stage of growth.

To learn more, visit: **AlvarezandMarsal.com**

A & M | AWS INSTITUTE